# ESCUELA DE COMUNICACIÓN Y TECNOLOGÍAS LIBRES PARA LA Defensa Común del Territorio

## ÍNDICE



## OBJETIVO

El objetivo de la Escuela Común es brindar herramientas para que las comunidades y organizaciones produzcan y almacenen de manera segura, material multimedia que documente el impacto ambiental y social de los proyectos que amenazan sus territorios.

espora.org

Centro de Autonomía Digital

# AGENDA

ESCUELA DE COMUNICACIÓN Y TECNOLOGÍAS LIBRES PARA LA Defensa Común del Territorio

| EN LÍNEA (agosto) | | Sesion 1 (10 agosto) | Sesion 2 (17 agosto) | Sesion 3 (24 agosto) | Sesion 4 (31 agosto) |
|---|---|---|---|---|---|
| | INTRODUCCIÓN<br>Sábados 3 pm UTC | Presentación Escuela Común - Entrega de Herramienta de Diagnóstico | Devolución de Diagnóstico por grupos - Plenaria | Politizar la Tecnología: Comunicación Comunitaria y el uso de las herramientas digitales | Sesión de preparación e información logística |

| PRESENCIAL (septiembre) | HORARIO | LUGAR | JUEVES 19 | VIERNES 20 | SÁBADO 21 | DOMINGO 22 | LUNES 23 | MARTES 24 |
|---|---|---|---|---|---|---|---|---|
| | 7:30 a 9:00 | Comedor | Llegadas a Quito<br>Viaje a Unión Base<br>Dormir en Unión Base | Desayuno | Desayuno | Desayuno | Desayuno | Desayuno |
| | 9:00 - 11:00 | DOCUMENTACIÓN (Salón 1) Nota: se dividen en grupos: Documentación (en azul) y servidores (en morado) | | Ceremonia de bienvenida<br>puesta en comun. Acuerdos de convivencia | Cefo y lanceros digitales: Campañas y casos con desenlace favorable | Descanso<br>paseo a Coto Cocha | Revisar lista de tomas/guion<br>Preparando Equipos, cuidados (medidas de seguridad) | Salir a grabar (Napo) |
| | | SERVIDORES (Salón 2) | | | ¿Qué implica tener una servidorcita propia en nuestra organización? | | Instalación de Servicios | Qué hacer cuando nada funcione? |
| | 11:00 a 11:30 | Libre | | Refrigerio | Refrigerio | | Refrigerio | Refrigerio |
| | 11:30 - 13:30 | DOCUMENTACION (Salón 1) | | Contexto General Consulta Libre Previa e Informada (Cefo) | Casos de éxito (preguntas y respuestas) Planeación y análisis de riesgo | | preprando equipos y fuentes (satélites, drone, camaras trampa, grabar en directo) | Regreso de grabar en Napo |
| | | SERVIDORES (Salón 2 o repartidos dentro de la Wlan) | | Software Libre, por qué y para qué (labo) | Primeros pasos de un CisAdmin, Vitualización, Bash y SSH | | Explicacion de lo que hace Red Abya Yala | Cómo levantar nuevos servicios |
| | 13:30 a 15:30 | COMEDOR | | Comida/Almuerzo | Comida/Almuerzo | | Comida/Almuerzo | Comida/Almuerzo |
| | 15:00 - 17:00 | General (Salón 1) | | Documentación<br>¿Qué es un servidor? Ejercicio demostrativo de un Nodo AbyaYala en funcionamiento | ProofMode (Guardian Project) | | Archivo (Inés Witness) | Archivo (Inés Witness) |
| | 17:00 a 17:30 | Libre | | Refrigerio | Refrigerio | | Refrigerio | Refrigerio |
| | 17:30 - 19:00 | General (Salón 1) | | Documentacion<br>Colocación Máquinas / recomendaciones mínimas de cuidados y seguridad fisica | Taller de Seguridad Digital (labo) | Libre en Puyo<br>Cena en Puyo | OSINT: WITNESS | Taller de uso y administración de Nextcloud (Labo) |
| | 19:00 a 20:00 | Comedor | | Cena | Cena | | Cena | Cena |
| | 20:30 en adelante | Hotel en Quito | | | | | | |
| | | | | películas | salida | | películas | convivio compartencia |

| | MIÉRCOLES 25 | JUEVES 26 | VIERNES 27 | SABADO 28 | DOMINGO 29 |
|---|---|---|---|---|---|
| PRESENCIAL (septiembre) | Desayuno | Desayuno | Desayuno | Desayuno | Desayuno |
| | descargar material/organizar | Cierre protocolar de Escuela. Entrega de certificados | 9:00 AM Salida de Unión Base a Quito | 9:30 AM Diálogos en la Casa de la Cultura | Vuelos de regreso |
| | Ejercicios Prácticos de BASH | | | | |
| | Refrigerio | Refrigerio | | | |
| | Editar | Visionado material y plataformas | | | |
| | Proyección acompañamiento y soporte. Cómo nos vamos a vincular? | | | | |
| | Comida/Almuerzo | Comida/Almuerzo | | | |
| | Archivo (Inés Witness) | Comida/Almuerzo | Comida/Almuerzo hotel en Quito | Comida/Almuerzo | |
| | Refrigerio | Refrigerio | 17:00 horas Inauguración de los Diálogos en al Auditorio de la Conaie | Diálogos Clausura en la Casa de la Cultura | |
| | Taller de creación de páginas web (Sutty) | Paseo a orquideario en Puyo<br>Cena de cierre en Puyo | | | |
| | Cena | | | Cena de despedida en Quito | |
| | | | Cena | | |

| | | Sesion 1 5 de octubre | Sesion 2 12 de octubre | Sesion 3 19 de octubre | Sesion 4 26 de octubre | Sesion 5 2 de noviembre | Sesion 6 9 de noviembre | Sesion 7 16 de noviembre | Sesión 8 23 de noviembre |
|---|---|---|---|---|---|---|---|---|---|
| EN LÍNEA (octubre) | | Herramientas jurídicas para la defensa del territorio (Cefo) | OSINT y sus uso en la defensa del territorio (Witness) | Archivo: Creación de categorías y colecciones (Witness) | TICs y su impacto en el medio ambiente (Colnodo) | Presentación de Red de Servidoras Autónomas (Nodo Abyayala) | Uso del Video para la defensa Medio Ambiental (Witness) | Herramientas de monitoreo con software y hardware libre (Colnodo) | Actividad Cierre Escuela |
| | TUTORÍAS | | | | | | | | |
| | DOCUMENTACIÓN | | | | | | - Reuniones de seguimiento general cada 15 días - Se generará chat o foro para dar seguimiento a los procesos. - Del proceso se generará una plataforma web con recursos que facilitarán la creación de servicios y plataformas web | | |
| | SERVIDORES | Segunda Semana de Octubre | Cuarta Semana de Octubre | segunda semana de noviembre | cuarta semana de noviembre | | | | |

# RESUMEN DEL TRABAJO EN PROGRESO SOBRE LOS ACUERDOS DE CONVIVENCIA

Cuidar la privacidad de las personas y espacio personal

Valores de Respeto

Real interés en lo que dice el otre

Tenerse tolerancia entre todos los participantes, cada uno proviene posiblemente de una cultura diferente

No juzgar. Preguntar, profundizar.

SER MÁS COOPERATIVO Y COLABORATIVO EN MOMENTOS QUE SEA NECESARIO PARA LA COLECTIVIDAD

Respetar cómo cada quien quiere/pide ser llamade/nombrade

Respetar los tiempos de descanso.

Respeto de pronombres

Evitar cualquier comentario o acción racista

Respetar los tiempos acordados para cada actividad.

Repartir las tareas de cuidados y limpieza: rotar, activar, que no queden siempre en las mismas personas

SI HAY PROBLEMAS DE RED, AVISAR A NICO

SI HAY PROBLEMAS DE SALUD o inconveniencia, AVISAR A FABBY

Repartir las tareas de cuidados y limpieza: rotar, activar, que no queden siempre en las mismas personas

RESPETAR LOS TIEMPOS EN EL USO DE LA PALABRA

Evitar actitudes de índole patriarcal

Evitar generar residuos plásticos, recoger nuestra basura

SI VAS A SALIR, AVISALE A ORI!!!

# RESUMEN DEL TRABAJO EN PROGRESO SOBRE LOS ACUERDOS DE CONVIVENCIA

Respeto a la cosmovisión de cada compañerx y sus pueblos

Valores de Solidaridad

Tener en cuenta que no hablamos todes de la misma manera, estar atentes a la necesidad de precisar, aclarar algo que no se comprendió

Paciencia.
No todes tenemos los mismos tiempos y conocimientos.

TOMAR LAS COSAS CON CALMA PARA NO CAER EN MALENTENDIDOS.

Compartir la comida, materiales, elementos.

Compartir labores para mantener el orden y la limpieza del lugar.

No todas las personas hablan tu mismo dialecto. Estar dispuestes a explicar y a comprender.

Evitar generar residuos plásticos, recoger nuestra basura

Compartir labores para mantener el orden y la limpieza del lugar.

Establecer momentos para uso de los dispositivos celulares para poder estar presentes durante los talleres

Cuidar el lugar al que vamos y respetar sus costumbres y culturas.

CUIDADO CON SALIR DE NOCHE A LA SELVA. INCLUSO LA GENTE DE ALLÁ SE GUARDA PORQUE SI NO "ALGO TE COME"

Cuidar el orden y la limpieza del lugar siendo responsables de dejarlo como lo encontramos o mejor

Impedir el acoso.

# RESUMEN DEL TRABAJO EN PROGRESO SOBRE LOS ACUERDOS DE CONVIVENCIA

AMABILIDAD Y CORDIALIDAD EN EL TRATO

practicar respeto solidaridad, puntualidad, atención a las clases

Evitar actitudes de índole patriarcal

Cuidar la privacidad de las personas y espacio personal

Escucha Activa

Respetar los límites que ponen las otras personas, estar atentes a los límites que necesitamos (o a pedir ayuda al respecto)

Ayudar con material extra para los procesos de aprendizaje en convivencia

No dar nada por sentado.
No todo el mundo tiene las mismas discusiones respecto a la convivencia. podemos dar espacio a todes para comprender y crecer

Seguridad Digital: Consentimiento de uso de imagen en fotografías
Al compartir imágenes en redes hacerlo después de la Escuela

Grabaciones de audio y video: Seguridad y consentimiento para grabar un caso
o un tema determinado que compartan lxs compañerxs durante la Escuela.

QUIZAS PONER UNA HORA EN LA NOCHE LUEGO DE LA CUAL HACER SILENCIO

Protocolo de acción frente a situaciones de acoso a las compañeras que implique hablar con
la persona que realizo la acción, Establecer medidas para no repetir la situación
y establecer formas de acompañamiento a quien sufrió el acoso.

SI VAS A SALIR, AVISALE A ORI! !!!

# INFORMACIÓN


Unión Base, comunidad anfitriona

Union Base, en la provincia de Pastaza (900 msnm) se localiza en la frontera entre Los Andes y la Amazonía Ecuatoriana. Es la base de la Confederación de Nacionalidades Amazónicas del Ecuador (CONFENIAE)

De Pastaza son originarias 11 diferentes nacionalidades de las 15 existentes en Ecuador.
Ecuador se conforma además de 18 pueblos indígenas no amazónicos.


Río Puyo

Se llama Unión Base, porque dos ríos que nacen más arriba en los Andes, se unen; el río Puyo y el río Pastaza, juntos se sumarán al caudal del río Marañon en Perú, que a su vez será un gran tributario al gigante río Amazonas ya en Brasil.


Río Pastaza

Varios pueblos de las diferentes nacionalidades en Ecuador, se incorporaron hasta recientes fechas al país, finalizado el periodo colonial, siendo el último, el pueblo Shuar Arutam,
Existen al menos 2 pueblos No Contactados.

# DOCUMENTACIÓN

## ÍNDICE



# EXPERIENCIAS SOBRE LA RESISTENCIA DE LOS PUEBLOS Y NACIONALIDADES DESDE LA COMUNICACIÓN DIGITAL Y SU REPRESENTACIÓN

**Andrés Tapia, Lanceros Digitales**

## Amazonía

**11 nacionalidades amazónicas pertenecientes a 23 organizaciones en las 6 provincias amazónicas: Kichwa, Shuar, Achuar, Sapara, Shiwiar, Waorani, Andwa, Quijos, Siona, Siekopai, Aí Kofán.**

- **Existe una enorme brecha digital entre las comunidades indígenas (-10% amazonia)**
- **Necesidad de implementar estrategias de TIC en comunidades indígenas**
- **873 Infocentros en el país, 189 en las 6 provincias amazónicas: Morona Santiago 45, Orellana 36, Sucumbíos 31, Napo 28, Zamora Chinchipe 26 y Pastaza 23**



**Fuente:** MINTEL (2020).

## La Resistencia de los pueblos y nacionalidades desde la comunicación digital (experiencia de los Lanceros Digitales)

**¿Cómo representan los medios a los pueblos y nacionalidades en la Resistencia Ambiental?**
**Espacio de reflexión**

## Un puente entre la comunicación ancestral y las tecnologías de comunicación modernas: Lanceros y Tuntwitteros

A un "click" de distancia, los neo "uwishin" (sabios) y los "kakaram" (guerreros) digitales, hacen de las redes sociales su nuevo campo de batalla:

Los primeros, en "twitter" con sus "tsentsak" (flechas invisibles) enfrentan y cuestionan el poder, mientras que los segundos en "Facebook", postean, transmiten en vivo (streaming), publican fotos, suben videos, comparten (share), dan "likes" a favor de la vida y en contra del extractivismo.

Ahora los "Smartphone" reemplazan al "tuntui" (instrumento de percusión) y la "lanza" (nanki). La guerra (mesét) virtual en el alto amazonas, más presente como en los tiempos de nuestros abuelos

## Tejidos de comunicación desde lo digital

- Jóvenes comunicadores comunitarios de las organizaciones de base
- Reportería desde territorio para alimentar el canal de información oficial
- Cobertura de asambleas, congresos y eventos de comunidades y organizaciones
- Articulación a la línea editorial, gráfica y política del movimiento indígena

*La tecnología y la comunicación responden a un proyecto político: movilización y lucha en defensa de nuestros territorios*


**Articulación en la estructura organizativa**


## EJES DE TRABAJO

- **FORMACIÓN**

**Certificación técnica de 100 comunicadores comunitarios en Sucumbios Pastaza Napo**

- **ALIANZAS DE COMUNICACIÓN**

**Aprobación de las políticas de acción afirmativa y democratización del espectro radioeléctrico 34% frecuencias para medios comunitarios**

- **PRODUCCIÓN RADIAL Y AUDIOVISUAL**

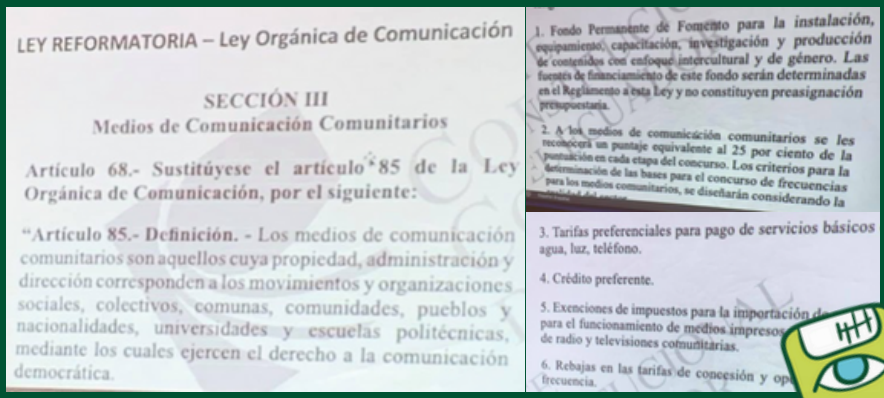
Radio y Revista La Voz de la CONFENIAE (recuperación tras 20 años)

- **COMUNICACIÓN POLÍTICA**

Posicionamiento del canal oficial de difusión de las nacionalidades — Comunicación Confeniae

## Reformas a la Ley de Comunicación

- Democratización del espectro radioeléctrico con 34% de frecuencias para medios comunitarios en la Ley Orgánica de Comunicación LOC aprobada por la Asamblea Nacional del Ecuador 2019
- Aprobación de las políticas de acción afirmativa dentro de la Ley de Comunicación
- Concurso de frecuencias de radio y televisión (licencia 2 radios comunitarias)


LEY REFORMATORIA – Ley Orgánica de Comunicación

SECCIÓN III
Medios de Comunicación Comunitarios

Artículo 68.- Sustitúyese el artículo 85 de la Ley Orgánica de Comunicación, por el siguiente:

"Artículo 85.- Definición. - Los medios de comunicación comunitarios son aquellos cuya propiedad, administración y dirección corresponden a los movimientos y organizaciones sociales, colectivos, comunas, comunidades, pueblos y nacionalidades, universidades y escuelas politécnicas, mediante los cuales ejercen el derecho a la comunicación democrática.

1. Fondo Permanente de Fomento para la instalación, equipamiento, capacitación, investigación y producción de contenidos con enfoque intercultural y de género. Las fuentes de financiamiento de este fondo serán determinadas en el Reglamento a esta Ley y no constituyen preasignación presupuestaria.

2. A los medios de comunicación comunitarios se les reconocerá un puntaje equivalente al 25 por ciento de la puntuación en cada etapa del concurso. Los criterios para la determinación de las bases para el concurso de frecuencias para los medios comunitarios, se diseñarán considerando la

3. Tarifas preferenciales para pago de servicios básicos agua, luz, teléfono.

4. Crédito preferente.

5. Exenciones de impuestos para la importación de para el funcionamiento de medios impresos de radio y televisiones comunitarias.

6. Rebajas en las tarifas de concesión y op frecuencia.

## Comunicando nuestras propias voces y narrativa




TRIPLE PANDEMIA
COVID19
EXTRACTIVISMO
MARGINACIÓN HISTÓRICA
ESTALLIDOS SOCIALES

## Periodismo de investigación


## CAMPAÑA

#ConfeniaeResiste

#7DePastaza

#FuerzaShuarArutam #ResistenciaWaorani #LaLuchaVaPorqueVa

#ResultadosYa #PiatúaResiste #ElParoSigue

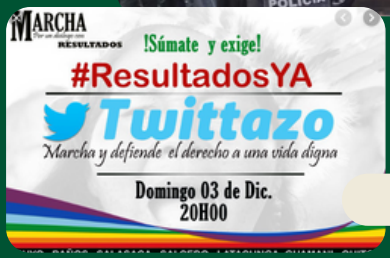
## RESULTADOS

- Unidad de las nacionalidades amazónicas
- Liberación e indulto presidencial perseguidos políticos
- Liberación líder Shuar Agustín Wachapa
- Restitución Educación Bilingüe
- Sentencia histórica prohíbe explotación petrolera
- Sentencia histórica en defensa del río piatúa
- Contexto de surgimiento del paro nacional
- Ruptura del cerco mediático durante el paro nacional


#ConfeniaeResiste

#ConfeniaeResiste






#ResultadosYa

#FuerzaShuarArutam


## #FuerzaShuarArutam



## #ParoNacionalEC #ElParoSigue

- Tendencia nacional en redes sociales durante 10 días
- 40 millones de interacciones en redes sociales durante 10 días

- Posicionamiento de los canales oficiales de comunicación del Movimiento Indígena
- Confeniae 10 a 140K seguidores – FB y 5 a 60K
- Conaie 20 a 300K seguidores – FB y 10 a 120K – X

# LA VIDA, EL ANÁLISIS Y LA SEGURIDAD DE LOS DATOS

**Armando Gómez, Laboratorio Popular de Medios Libres**

## Introducción a la vida y gestión de los datos.

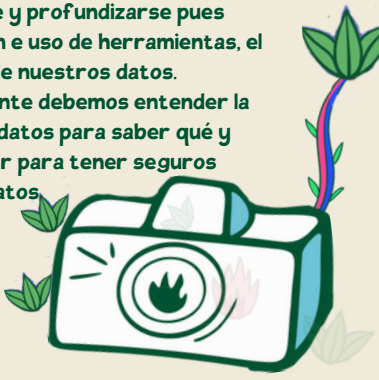
¿Qué es un dato? Es información traducida, procesada o almacenada por una computadora. Un dato describe una acción, es una representación simbólica de un atributo o variable cuantitativa o cualitativa. Los datos describen hechos empíricos, sucesos y entidades.

Un dato digital como un texto, una imagen, un video o un registro, son conjuntos de datos agrupados en archivos.

Los datos para su mejor uso deben de tener un ciclo de vida, donde se incluye su creación, recolección, archivado y cuidado de esos datos. Entender todo el proceso que lo lleva de ser un simple dato a ser parte de una conjunto de ellos, que en su procesamiento los hace coherentes e útiles. Es importante tener en cuenta esa evolución de la vida de los datos en dos sentidos relevantes. En el papel de la comunicación estratégica de nuestras comunidades y de la administración de esos archivos y servicios digitales.

Por un lado es recibir o recabar los datos, clasificarlos y limpiarlos para crear bases de datos almacenadas en la nube de la internet o en nuestros equipos y dispositivos de cómputo como los SERVIDORES. Después de esos primeros procesos los datos tienen un mejor uso y métodos de análisis métrico y forense, o para su incidencia mediática o jurídica en un soporte digital seguro y que permita la privacidad y la autonomía digital.

En el transcurso que va de ser registrado un dato, por ejemplo cuando es tomada una imagen por una cámara fotográfica, o un audio en alguna grabadora o teléfono móvil, o al hacer una hoja de calculo (tabla excel) para capturar las acciones y después pasarlas a un dispositivo para su edición de esa imagen, ese audio, este texto o esa hoja de calculo para almacenarla en alguna lugar o quizá subirla a alguna red para poder compartirla o publicarla. Conservarla para poder darle un uso, buscano guardar aspectos básicos de un dato ahora convertidos en archivos digitales. Este ciclo debe conocerse, practicarse y profundizarse pues permite con e uso de herramientas, el mejor uso de nuestros datos. Principalmente debemos entender la ruta de los datos para saber qué y dónde cuidar para tener seguros nuestros datos.



Vamos también a conocer algunos de los riesgos, amenazas y vulnerabilidades, mientras conocemos algunas de las buenas prácticas de seguridad para esos datos en nuestros dispositivos y en el internet.

La vida de los datos consta de seis etapas para su análisis: Va desde Planificar para decidir qué tipo de datos se tienen o se necesitan, cómo se gestionarán y quiénes serán responsables de ellos. Capturar que implica el recopilar o reunir datos de varias fuentes distintas. El Gestionar que es cuidar y brindar mantenimiento a los datos. Esto incluye determinar cómo y dónde se almacenan y las herramientas utilizadas para hacerlo. El cuarto paso es Analizar y es utiilizar los datos para resolver problemas, tomar decisiones y respaldar los objetivos estratégicos de nuestra comunicación. De los últimos pasos está el Archivar para mantener almacenados los datos relevantes para acervo cerrado o abierto a corto, mediano o largo plazo. Otro punto que siempre se toma en cuenta en el plano de la seguridad es el nivel de Privacidad así como la posible destrucción o depuración de los archivos que elimina o preserva de manera planificada los datos almacenados y todas las copias compartidas.

## Cuidados en internet ante riesgos, amenazas y vulnerabilidades.

El mundo conectado y el Internet de las Cosas (IoT por sus siglas en inglés).

La inter conectividad es la capacidad de conectar a la red de internet cada vez un mayor número de dispositivos y máquinas con cada vez mayores velocidades de respuesta y reacción. Esa red global ha crecido rápidamente y a la par lo ha hecho las amenazas, riesgos y vulnerabilidades en esas redes globales.

No hay nada seguro en internet, podemos tener buenas prácticas para reducir el riesgo, ayudado por algunas herramientas de revisión y monitoreo, como una actualización constante de los equipos y las capacidades técnicas de usuarixs y administradorxs. Conozcamos tres términos de seguridad fundamentales:

**Riesgo:** Cualquier hecho que pueda afectar la confidencialidad, integridad o disponibilidad de un activo.
**Amenaza:** Cualquier circunstancia o evento que pueda afectar negativamente a los activos. Las amenazas son circunstancias o eventos que pueden tener un impacto negativo en los activos. Existen muchos tipos diferentes de amenazas, pero generalmente se clasifican en dos categorías: intencionales e involuntarias.
**Vulnerabilidad:** Son debilidades que pueden ser aprovechadas por las amenazas. Existen diversas vulnerabilidades, pero se pueden clasificar en dos categorías: técnicas y humanas.

Los Archivos digitales protegen diversos tipos de activos. Algunos ejemplos podrían incluir:

- Activos digitales como datos personales de miembros o registros financieros.
- Sistemas de información que procesan datos, como redes o software.
- Activos físicos que pueden incluir instalaciones, equipos o suministros.
- Activos intangibles como la reputación de la marca o la propiedad intelectual.

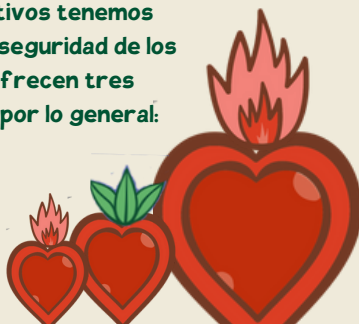
Independientemente de su tipo, es crucial que cada activo sea clasificado y contabilizado. Determinar sus factores puede variar, pero evaluar cuán sensible e importante es un activo generalmente requieren conocer la siguiente información:

1. Lo que tienes (qué tipo de activo o archivo es)
2. Dónde se encuentra ubicado
3. Quién es el propietario y quién tiene acceso a ese archivo.
4. Cuál es su nivel de importancia para la organización.

El esquema de clasificación más común consta de cuatro niveles: restringido, confidencial, solo interno y público.

**Restringido** es el nivel más alto. Esta categoría está reservada a activos muy sensibles, como la información que solo se proporciona a quienes necesitan conocerla.
El nivel **confidencial** se refiere a los activos cuya divulgación puede provocar un impacto negativo significativo en una organización.
El nivel **solo interno** describe activos disponibles para el personal de una empresa y socios comerciales.
**Público** es el nivel más bajo de clasificación. Estos activos no tienen consecuencias negativas para la organización si se divulgan.

Aparte de las buenas prácticas en nuestros dispositivos tenemos que pensar en la seguridad de los servidores que ofrecen tres tipos de servicio por lo general:



1. Software como servicio (SaaS) correo electronico Riseup o Gmail.
2. Plataforma como servicio (PaaS) Soporte para aplicaciones Google App Engine, Hostings
3. Infraestructura como servicio (IaaS) Servidores, Machine Learning, Google Cloud , Microsoft Azure

Seguridad en la nube

Migrar aplicaciones e infraestructura a la nube puede facilitar el funcionamiento de un servicio en línea. Sin embargo, también puede complicar la tarea de mantener los datos privados y seguros. La seguridad en la nube es un campo en crecimiento dentro de la ciberseguridad, que se enfoca específicamente en la protección de datos, aplicaciones e infraestructuras en la nube.

En un modelo tradicional, las organizaciones tenían toda su infraestructura de TI en sus instalaciones. La protección de esos sistemas recaía por completo en el equipo de seguridad interno de ese entorno. No obstante, estas responsabilidades no están tan claramente definidas cuando parte o todo el entorno operativo se encuentra en la nube. Acá una lista de recomendaciones para asumir la supervisión de seguridad de nuestros sistemas.

- Crea un perfil actual de las operaciones de seguridad y describe las necesidades específicas de tu organización.
- Realiza una evaluación de riesgos para identificar cuáles de tus operaciones actuales cumplen con los estándares regulatorios y de seguridad.
- Analiza y prioriza las vulnerabilidades existentes en las operaciones de seguridad que ponen en riesgo los activos a cuidar.
- Implementa un plan de acción para alcanzar las metas y objetivos de tu organización.

Para ayudarnos a conocer experiencias previas de cómo manejar la seguridad en una organización, existen los marcos o protocolos de seguridad como el Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST) que incluye estándares, pautas y prácticas recomendadas para gestionar riesgos para la ciberseguridad.

En estos marcos o protocolos encontramos respuestas, por ejemplo revisamos un marco de seguridad ante un ataque donde se recomienda tener una ruta trazada bajo los siguientes parámetros:

- Identificar: Desarrollar una comprensión de todo el sistema para gestionar los riesgos de ciberseguridad para sistemas, personas, activos, datos y capacidades.

- **Proteger:** Implementar acciones apropiadas para garantizar la prestación de servicios y la preservación de los archivos.

- **Detectar:** Desarrollar actividades apropiadas para identificar la causa de un evento de ciberseguridad.

- **Responder:** Desarrollar actividades apropiadas para tomar medidas con respecto a un incidente detectado.

- **Recuperar:** Actividades apropiadas para mantener planes de resiliencia y restaurar cualquier capacidad o servicio que se vio afectado debido a un incidente.

La **privacidad de la información** se refiere a la protección contra el acceso y la difusión no autorizados de datos.

La **seguridad de la información** se refiere a la práctica de mantener los datos, en todas sus formas, alejados de usuarios no autorizados.

## ¿Por qué es importante la privacidad en la seguridad?

La importancia de la privacidad en la seguridad de los datos comenzó a ganar mucha atención a finales de la década de 1990.

En ese momento, las empresas tecnológicas pasaron repentinamente de procesar los datos de las personas a almacenarlos y utilizarlos con fines comerciales. Por ejemplo, si una persona buscaba un producto en línea, las empresas almacenaban y compartían información sobre el historial de búsqueda de ese usuario con otras organizaciones. Esto permitía a las compañías ofrecer experiencias de compra personalizadas de forma gratuita.

## Regulaciones importantes sobre privacidad

Las empresas deben cumplir con ciertas leyes para operar. Como recordarás, las regulaciones son normas establecidas por un gobierno u otra autoridad para controlar la forma en que se realiza algo. En particular, las regulaciones de privacidad existen para proteger a los usuarios de que su información sea recopilada, utilizada o divulgada sin su consentimiento. Además, estas regulaciones suelen describir las medidas de seguridad que deben implementarse para mantener la información privada protegida de amenazas.

Tres de las regulaciones de la industria más influyentes que todo profesional de la seguridad debe conocer son:

- Reglamento General de Protección de Datos (RGPD)
- Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI-DSS)
- Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA)

Reglamento General de Protección de Datos (RGPD) es un conjunto de normas y regulaciones desarrollado por la Unión Europea (UE) que otorga a los propietarios de los datos el control total sobre su información personal. Según el RGPD, se considera información personal el nombre, la dirección, el número de teléfono, la información financiera e información médica de una persona, entre otras.
El cumplimiento de las normas suele ser un proceso continuo que implica auditorías y evaluaciones de seguridad:

- Una auditoría de seguridad es una revisión de los controles de seguridad, políticas y procedimientos de una organización frente a un conjunto de expectativas.
- Una evaluación de seguridad es una revisión para determinar la resistencia de las actuales medidas de seguridad frente a las amenazas.


- Una evaluación de seguridad es una revisión para determinar la resistencia de las actuales medidas de seguridad frente a las amenazas.

    - Una evaluación de seguridad es una revisión para determinar la resistencia de las actuales medidas de seguridad frente a las amenazas.

### ¿Qué es un escáner de vulnerabilidades?

Un escáner de vulnerabilidades es uno o varios softwares que comparan automáticamente las vulnerabilidades y exposiciones conocidas con las tecnologías de la red. En general, estas herramientas analizan los sistemas para encontrar configuraciones erróneas o fallas de programación. Las herramientas de escaneo se utilizan para analizar cada una de las cinco superficies de ataque de la red.

1. Capa perimetral, como los sistemas de autenticación que validan el acceso del usuario.
2. Capa de red, que se compone de tecnologías como firewalls de red y otros.
3. Capa de punto de conexión (endpoint), que describe los dispositivos en una red, como computadoras portátiles yde escritorio o servidores.
4. Capa de aplicación, que involucra el software con el que interactúan los usuarios.

5. Capa de datos, que incluye cualquier información almacenada, en tránsito o en uso.

## La importancia de las actualizaciones

Es posible que en algún momento te hayas preguntado: "¿Por qué mis dispositivos necesitan actualizaciones constantemente?"
Para los consumidores, las actualizaciones proporcionan mejoras en el rendimiento y la estabilidad, ¡e incluso nuevas características! Pero desde el punto de vista de la seguridad, sirven para un propósito específico.

## Software al final de su vida útil

A veces, las actualizaciones no están disponibles para cierto tipo de software conocido como software al final de su vida útil (End-of-Life, o EOL). Todo software tiene un ciclo de vida. Comienza cuando se produce y termina cuando se lanza una versión más nueva.

## Agentes de amenaza

Un agente de amenaza es cualquier persona o grupo que plantea un riesgo para la seguridad. Esta definición a grandes rasgos abarca a personas tanto dentro como fuera de una organización. También incluye a personas que intencionalmente representan una amenaza y quienes ponen en riesgo los activos por accidente.

Por lo general, los agentes de amenaza se dividen en cinco categorías según sus motivaciones:

- Los Mercenarios digitales refiere a las personas contratadas por los grupos de poder que representan una amenaza porque podrían beneficiarse de la información filtrada.
- Los Actores estatales son agencias de inteligencia del gobierno.
- Los Grupos criminales son grupos organizados de personas que ganan dinero mediante actividades delictivas.
- Las amenazas internas pueden ser cualquier persona que tenga o haya tenido acceso autorizado a los recursos de una organización.

## Tácticas de ingeniería social

Los ataques de ingeniería social son muy comunes entre los agentes de amenazas. Esto se debe a que, a menudo, es más fácil engañar a las personas para que les proporcionen acceso, información o dinero que explotar una vulnerabilidad de software o red.
La suplantación de identidad (o phishing) es el uso de comunicaciones digitales para engañar a las personas de manera que revelen datos confidenciales o instalen software malicioso en sus equipos.

## MALWARE Cosas Malas

El Malware es un software diseñado para dañar dispositivos o redes. Desde su primera aparición en computadoras personales hace décadas, se desarrolló una gran cantidad de cepas de malware
Un virus es un código malicioso escrito para interferir con las operaciones informáticas y causar daños a los datos y al software. Para poder propagarse y causar daños, este tipo de malware debe ser instalado por el usuario a quien el ataque apunta.

Un gusano es un software malicioso que se puede duplicar y propagar por sí mismo a través de sistemas. De manera similar a los virus, un gusano debe ser instalado por el usuario a quien está dirigido el ataque, y también se puede propagar mediante tácticas como el correo electrónico malicioso. Dada la capacidad que tiene un gusano de propagarse por sí solo, los ataques a veces están dirigidos a dispositivos, unidades o archivos que tienen acceso compartido a través de una red.

Un troyano, también llamado caballo de Troya, es un software malicioso (malware) que se parece a un archivo o programa legítimo.

El software respaldado por publicidad, o adware, es un tipo de software legítimo que a veces se utiliza para mostrar publicidad digital en las aplicaciones.

Al igual que el adware, el spyware es un tipo de software malicioso que se usa para recabar y vender información sin consentimiento.

Otro tipo es el scareware. Esta clase de software malicioso emplea tácticas para asustar a los usuarios con el fin de que infecten su propio dispositivo.

El software malicioso sin archivos (o malware sin archivos) no necesita que el usuario lo instale porque utiliza programas legítimos que ya están instalados para infectar una computadora.

Un rootkit es un software malicioso que proporciona acceso administrativo y remoto a una computadora.

El ransomware es un ataque en el que los agentes de amenaza cifran los datos de una organización y exigen un pago (rescate) para restablecer el acceso a ellos.

VirusTotal es un servicio que permite a cualquier persona analizar archivos, dominios, URL y direcciones IP sospechosos en busca de contenido malicioso.

Nota: Los datos subidos a VirusTotal se compartirán públicamente con toda la comunidad de VirusTotal. Es necesario tener cuidado al enviar información y asegurarse de no subir información personal.

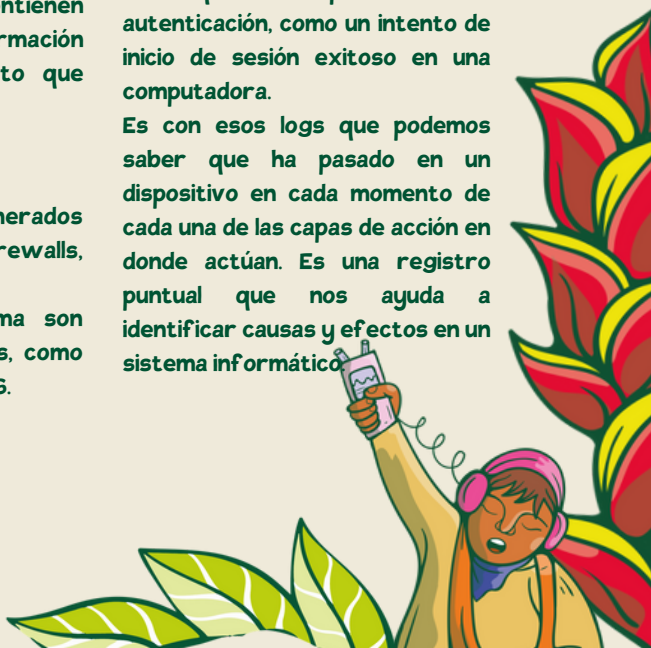
Así un responsable de la seguridad de un centro de datos puede recurrir a las siguientes herramientas para organizar, compartir ese organigrama, tener planes periódicos de seguridad y rutas de acción ante brechas de seguridad.

**Manual de estrategias:** Guía que proporciona detalles sobre cualquier acción operativa de un servicio y un servidor. Permite sucesiones, auditorias y una comprensión sencilla por terceros.
**Plan de continuidad:** Documento que describe los procedimientos para mantener las operaciones digitales durante y después de una interrupción significativa. Respaldos.
**Plan de respuesta a incidentes:** Documento que describe los procedimientos a seguir en cada paso de la respuesta a un incidente.

Un elemento importante a tomar en cuenta para la seguridad de un servidor o un centro de datos son los **Registros**. Las fuentes de datos, como los dispositivos, generan información en forma de eventos, **registros** (o logs) que recopilan los eventos que se producen dentro de los sistemas de una organización. Estos registros contienen entradas, y cada una detalla la información correspondiente a un único evento que ocurrió en un dispositivo o sistema.

## Tipos de registros

**Red:** Los registros de red son generados por dispositivos de red, como firewalls, routers o switches.
**Sistema:** Los registros de sistema son generados por sistemas operativos, como Chrome OS, Windows, Linux o macOS.
**Aplicación:** Los registros de aplicación son generados por aplicaciones de software y contienen información relacionada con los eventos que ocurren dentro de la aplicación, como una aplicación en un teléfono inteligente.
**Seguridad:** Los registros de seguridad son generados por varios dispositivos o sistemas, como el software antivirus y los sistemas de detección de intrusiones. Estos contienen información relacionada con la seguridad, como la eliminación de archivos.
**Autenticación:** Los registros de autenticación se generan cada vez que se produce una autenticación, como un intento de inicio de sesión exitoso en una computadora.
Es con esos logs que podemos saber que ha pasado en un dispositivo en cada momento de cada una de las capas de acción en donde actúan. Es una registro puntual que nos ayuda a identificar causas y efectos en un sistema informático.



## Tipos de registros

**El cifrado asimétrico** se basa en el uso de un par de claves: una pública, para cifrar los datos, y una privada, para descifrarlos. La clave privada solo se comparte con los usuarios con acceso autorizado.

Por ejemplo, los sitios web suelen emplear el cifrado asimétrico para proteger pequeños bloques de datos que son importantes, como nombres de usuario y contraseñas durante el proceso de inicio de sesión. Una vez que alguien obtiene acceso, el resto de su sesión en el sitio web suele cambiar al cifrado simétrico debido a su mayor rapidez.

**Las funciones hash** son algoritmos que producen un código que no se puede descifrar. Las funciones hash convierten la información en un valor único que luego puede utilizarse para determinar su integridad.

**Cómo funciona el inicio de sesión único (SSO)**

El inicio de sesión único (SSO) funciona automatizando el establecimiento de confianza entre un usuario y una empresa proveedora de servicios

**La autenticación de múltiples factores, o multifactor, (MFA)** requiere que un usuario verifique su identidad de dos o más formas para acceder a un sistema o red. En cierto sentido, la MFA es similar al uso de un cajero automático.

**El principio de mínimo privilegio,** según el cual a un usuario solo se le otorga el nivel mínimo de acceso y autorización requerido para completar una tarea o función.

**La segregación de funciones,** que es el principio según el cual no se debe conceder a los usuarios niveles de autorización que les permitan hacer un uso indebido de un sistema.

**La inteligencia de fuentes abiertas** (OSINT) es la recopilación y análisis de información procedente de fuentes de acceso público para generar inteligencia utilizable. La OSINT también se puede utilizar como método para recopilar información relacionada con agentes de amenaza, amenazas, vulnerabilidades y más.

# INTRODUCCIÓN A LA VIDA Y GESTIÓN DE LOS DATOS.

1. ¿Estás al tanto de las prácticas básicas de seguridad cibernética? ¿Conoces las medidas básicas para proteger tus dispositivos y datos personales? ¿Qué herramientas y cuidados digitales conoces?
2. ¿Comprendes los riesgos de la ingeniería social? La ingeniería social es una táctica común utilizada por los atacantes para engañar a las personas y obtener información confidencial. ¿Eres consciente de cómo identificar y evitar estas trampas de ingeniera social?
3. ¿Utilizas contraseñas seguras? Las contraseñas son la primera línea de defensa. ¿Sabes cómo crear contraseñas fuertes? ¿tienen una contraseña distinta para cada servicio? ¿sabes guardar tus contraseñas de manera segura? ¿la cambias frecuentemente?
4. ¿Actualizas regularmente tus dispositivos y aplicaciones? Las actualizaciones de seguridad suelen corregir vulnerabilidades conocidas. ¿Te aseguras de mantener tus sistemas actualizados en tu computadora o teléfono? ¿actualizas las aplicaciones y softwares que ocupas?
5. ¿Eres consciente de los riesgos de las redes Wi-Fi públicas? Las redes Wi-Fi abiertas pueden ser inseguras. ¿Te conectas a internet de forma segura?, ¿Tomas precauciones al conectarte a redes públicas?, ¿confiás en la red a la que te conectas?
6. ¿Realizas copias de seguridad de tus datos? Las copias de seguridad son esenciales para proteger tus archivos en caso de pérdida o ataque. ¿Haces copias de seguridad regularmente? ¿Como guardas y desechas tus archivos?
7. ¿Sabes cómo reconocer correos electrónicos de phishing? Los correos electrónicos de phishing intentan engañarte para que reveles información personal. ¿Puedes identificar señales de advertencia en correos electrónicos sospechosos?
8. ¿Conoces los riesgos de hacer click en enlaces desconocidos? Los enlaces maliciosos pueden llevar a sitios web peligrosos que realicen tareas no permitidas. ¿Eres cauteloso al hacer click en enlaces en mensajes de redes sociales? ¿como verificas la información que te envían?
9. ¿Estás al tanto de las amenazas de malware o virus informático? El malware puede dañar tus dispositivos y robar información. ¿Tienes instalado algún antivirus, evitas descargar archivos sospechosos? Sabes que aplicaciones malignas pueden atacar tus dispositivos? ¿ocupas alguna medida de revisión y limpieza?
10. ¿Proteges tu privacidad en las redes sociales? Las redes sociales pueden exponer información personal. ¿Configuras adecuadamente tus opciones de privacidad? ¿Quién sabe de ti, por qué y para qué? ¿cómo te pone en riesgo esa información?

WITNESS
MÍRALO GRÁBALO CÁMBIALO

# GUÍA DE VIDEO COMO EVIDENCIA
# ¿CÓMO GRABAR VIOLACIONES AMBIENTALES?

1

Las pruebas visuales, como videos y fotos, pueden utilizarse para denunciar violaciones ambientales o delitos relacionados. Para ello, es necesario utilizarlas con eficacia.

## Comprender lo que se necesita grabar

Las pruebas son información presentada al público para demostrar o refutar un hecho. En este caso, el público puede incluir a la prensa, las empresas, el gobierno y los tribunales. Por eso primero debes identificar la razón por la que quieres recolectar estas evidencias, por ejemplo: Para impedir que la empresa minera contamine el río.

Después contesten ¿cómo utilizarán la documentación para defender los derechos humanos y salvaguardar los bienes comunes naturales? Por ejemplo: Para demostrar al gobierno, a lxs accionistas de la empresa, y a los tribunales cómo la empresa minera está destruyendo los ríos para que se cancelen las concesiones de la empresa.

También es importante que identifiques qué violación se va a documentar, hay que decidir qué información se va a presentar. Algunos ejemplos de violaciones medioambientales son: invasión de tierras indígenas, minería ilegal, tala de árboles, contaminación de ríos, pesca o caza ilegales, construcción de presas, apropiación de tierras para el desarrollo inmobiliario, entre otras.

2

## Organizar los roles dentro del equipo

Si es posible y seguro grabar la violación, lo ideal es organizar un equipo y dividir las tareas en etapas, teniendo en cuenta quién tomará las decisiones, quién saldrá a grabar, quién organizará el material recogido, quién lo analizará y quién lo presentará.

## 3 PRESTEN ATENCIÓN A CADA PASO

**Hagan una lista de tareas para cada etapa de la recolección de pruebas:**

- Antes de grabar, comprueben la seguridad del lugar donde se recogerán las pruebas. Es importante asegurarse de que el entorno es seguro para grabar y de que nadie del equipo esté en peligro.
- Hagan un plan de recolección, organizando qué delitos hay que probar y qué hay que grabar o fotografiar para exponer cada uno de ellos. Consulta cómo hacerlo en wit.to/PlanRecoleccion
- Antes de grabar, comprueben el equipo y carguen las baterías. Si es posible, lleven baterías y tarjetas de memoria de repuesto. Comprueben que la fecha y la hora de la cámara están ajustadas correctamente.
- Durante la grabación, vuelvan a comprobar la seguridad y graben sólo las violaciones más relevantes. Siempre que sea posible, pidan a una persona que les monitoree mientras estén haciendo la documentación en terreno.
- Al entrevistar o grabar a personas víctimas, asegúrate de que hay autorización e informa a la persona o personas del motivo de la grabación. Consulta más sobre consentimiento informado en wit.to/consentimiento
- Después de grabar, descarga las imágenes de tu cámara o teléfono móvil en un lugar seguro.

## 4 ENCUADRES Y EQUIPO

Cuando hagan fotos y videos, tengan en cuenta algunas cuestiones técnicas:

Graben planos abiertos, medios y primeros planos relevantes. Tomen una vista panorámica de la escena y giren la cámara 360 grados, si es posible.

# 4 ENCUADRES Y EQUIPO

**Panorámica**

**Plano abierto**

**Plano medio**

**Plano detalle (close up)**

**Entrevistas**

Para las entrevistas, ajusten la altura de la cámara al nivel de los ojos de la persona entrevistada. Cuando graben en horizontal, utilicen la regla de los tercios para situar a la persona en la imagen.

Si es posible, consideren apoyarse utilizando imágenes de satélite y de drones que puedan ayudar a contar una historia más amplia y mostrar la extensión geográfica de las violaciones causadas.

## 5 PRESERVA EL MATERIAL RECOLECTADO

Tomen medidas para evitar perder accidentalmente archivos. Para eso es esencial una buena organización. Hay que tener cuidado al transferir y organizar el material:

- Conserven los nombres originales de los archivos y nombren claramente las carpetas en su equipo de cómputo, incluyendo la fecha y el lugar/tema, sin espacios ni caracteres especiales como @#$%&*:"' <>?/\~|,.
- Hagan copias de los archivos en distintos dispositivos y plataformas, como un disco duro externo y una plataforma de almacenamiento en la nube, por ejemplo.
- Al editar videos, exporten una copia de alta resolución para su preservación, además de las copias de acceso.

Estas son algunas de las precauciones que pueden garantizar el acceso a tus archivos.

Importante:
No utilicen las redes sociales para "conservar" tus videos o fotos.

## ¡HORA DE LA ACCIÓN! 6

Por fin ha llegado el momento de pasar a la acción. Es el momento de presentar claramente todas las pruebas que se han recopilado. En esta fase, decidirás cuál es la mejor manera de presentar la información y si debe omitirse algún dato para proteger la privacidad y la seguridad de las personas implicadas. Por último, no olvides dar crédito a las organizaciones y personas que han participado en el trabajo.

Recuerda siempre que el objetivo es informar y provocar un cambio real.

Para más información sobre cómo grabar violaciones ambientales, consulta la Guía de video cómo evidencia para la defensa ambiental en wit.to/DefensaMedioambiental

WITNESS
MÍRALO GRÁBALO CÁMBIALO

# GUÍA: UN ENFOQUE COMUNITARIO DE LA VERIFICACIÓN VISUAL PARA FORTALECER LA VERDAD

Esta guía de verificación visual comunitaria propone un enfoque colaborativo de la verificación utilizando materiales de fuentes abiertas. Incluye herramientas y procesos para verificar la exactitud, veracidad y credibilidad de los contenidos visuales de fuentes abiertas, especialmente en situaciones en las que las fuentes oficiales de información pueden no estar disponibles o ser poco fiables.

Cada paso de este proceso está dedicado a un aspecto fundamental de la verificación:

1. Evaluación de la fuente: comprender de dónde procede el video
2. Evaluación del contenido: comprender lo que nos está diciendo el video
3. Geolocalización: determinar dónde tuvo lugar el suceso
4. Cronolocalización: determinar cuándo se grabó un video o se tomó una fotografía
5. Archivo de datos verificados: almacenar los datos para su uso futuro, incluidos el análisis y la presentación
6. Distribución/informes: saber cuál es la mejor manera de compartir información y con quién

Consulta la guía completa en wit.to/verificacion-comunitaria

es.witness.org
@witness_es
witnessespanol
witness_es

# FORMATO PARA LLENAR

| OBJETIVO | SITUACIÓN ACTUAL | METAS |
| --- | --- | --- |
| | | |
| | | |
| | | |

# FORMATO PARA LLENAR

| OBJETIVO | SITUACIÓN ACTUAL | METAS |
| --- | --- | --- |
| | | |
| | | |
| | | |
| | | |

# EJEMPLO DE JÚBA WAJIIN

## Resumen del caso

En 2011, la comunidad indígena me'phaa (tlapaneca) de San Miguel El Progreso (o la comunidad Júba Wajiín), supo que el gobierno mexicano autorizó a dos empresas, Hochschild (Perú) y Zalamera (México), a comenzar la etapa de explotación para una operación minera a cielo abierto. Conocido como el proyecto Corazón de Tinieblas, esta operación abarcaría el 80% de la tierra Júba Wajiín, sin embargo, el gobierno mexicano otorgó a las empresas estas concesiones mineras sin consultar a la comunidad. Como respuesta, la comunidad Júba Wajiín decidió oponerse a la minería en esa región.

Como la Ley de Minería de México no reconoce el derecho de las comunidades indígenas a la consulta, en 2014, Tlachinollan y la comunidad Júba Wajiín presentaron un requerimiento solicitando que la Corte Suprema de México determine si la Ley de Minería era constitucional y compatible con las obligaciones internacionales de derechos humanos del país. México es signatario de varios instrumentos de derechos humanos, incluyendo el Convenio 169 de la Organización Internacional del Trabajo (OIT) que establece que los pueblos indígenas tienen derecho a ser consultados sobre actividades que afectan sus medios de subsistencia, tales como las concesiones mineras.

En 2018, una jueza federal establece que el gobierno mexicano tiene la obligación constitucional de respetar el derecho a su territorio de los pueblos indígenas lo cual implica que las empresas mineras no pueden continuar operando en territorio de Júba Wajiín. Las empresas se desisten de las concesiones, por lo cual la Suprema Corte establece se queda sin materia para seguir analizando el caso. Ello implicó un triunfo para Júba Wajiín, aunque no se llegó a lograr la declaración de inconstitucionalidad de la Ley Minera en México.

# EJEMPLO FORMATO JUBA WAJIIN

| | OBJETIVO | SITUACIÓN ACTUAL | METAS |
|---|---|---|---|
| ARCHIVO | Lograr tener sus archivos en control y manos de la comunidad | Tienen archivos pero sobre todo en casas y en organizaciones que les han apoyado como el Centro de Derechos Humanos de la Montaña Tlachinollan. | Juntar en el disco duro de la comunidad toda la información, acordar previamente el formato para organizar el material |
| MULTIMEDIA: PRODUCCIÓN O DIFUSIÓN JURÍDICO | Obtener una sentencia favorable que declarara inconstitucional la Ley Minera por contravenir la Constitución y el Artículo 169 OIT. | Se está llevando a cabo un video sobre el derecho a la consulta y el reconocimiento del ser indígena a través de mostrar cuestiones como la lengua, prácticas culturales, políticas y rituales. Además. se utilizan videos cortos como parte de la campaña pública de comunicación. | Terminar de grabar las imágenes y edición del video |
| INFORMACIÓN DE FUENTES ABIERTAS (OSINT) | Reunir información adicional sobre el estado de las concesiones y las acciones de las empresas. | Solicitud de acceso a la información para solicitar las concesiones en proceso. | Obtener información sobre las acciones de las empresas |
| SEGURIDAD | Completar un análisis de riesgo a fin de contar con planes de acción | Se tiene recopilada información relevante para el análisis de riesgo | Contar con el plan de acción avalado por la comunidad |