

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

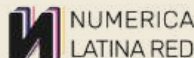
ÍNDICE

Objetivo
Agenda
Acuerdos de convivencia
Información
Documentación
Servidores
Archivo
Perfiles de waykis /
amikiur



OBJETIVO

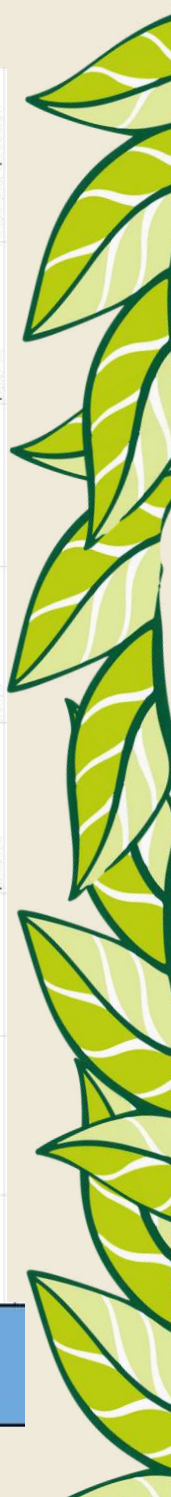
El objetivo de la Escuela Común es brindar herramientas para que las comunidades y organizaciones produzcan y almacenen de manera segura, material multimedia que documente el impacto ambiental y social de los proyectos que amenazan sus territorios.





AGENDA

EN LINEA (agosto)	Session 1 (10 agosto)		Session 2 (17 agosto)		Session 3 (24 agosto)		Session 4 (31 agosto)	
	INTRODUCCIÓN Sábados 3 pm UTC	LUGAR	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)	7:30 a 9:00	Comedor	Ceremonia de bienvenida		Desayuno		Desayuno	
	9:00 - 11:00	DOCUMENTACIÓN (Salón 1) Nota: se dividen en grupos y se dividen (en azul) y sesiones (en naranja)	puesta en comun. Acuerdos de convivencia		Café y lanceros digitales: Compañías y casos con desempeño favorable		Revisar lista de tomas/guion Preparar equipos, cuidados (medidas de seguridad)	
		SERVIDORES (Salón 2)					Instalación de Servicios	
	11:00 a 11:30	Libre	Refrigerio		Refrigerio		Refrigerio	
	11:30 - 13:30	DOCUMENTACIÓN (Salón 1)	Contexto General Consulta Libre Previa e Informada (Café)		Casos de éxito (preguntas respuestas) y análisis de riesgo		preparando equipos y fuentes (satélites, drone, camaras trampa, grabar en directo)	
		SERVIDORES (Salón 2 o repáridos dentro de la WiAn)			Primeros pasos de un CisAdmin, Virtualización, Bash y SSH		Explicación de lo que hace Red Abya Yala	
	13:30 a 15:30	COMEDOR	Software Libre, por qué y para qué (labo)		Comida/Almuerzo		Comida/Almuerzo	
	15:00 - 17:00	General (Salón 1)	Documentación		ProofMode (Guardian Project)		Archivo (Inés Witness)	
					¿Qué es un servidor? Ejercicio demostrativo de un Nodo AbyaYala en funcionamiento		Refrigerio	
	17:00 a 17:30	Libre	Documentación		Taller de Seguridad Digital (labo)		Refrigerio	
	17:30 - 19:00	General (Salón 1)	Colocación Máquinas / recomendaciones mínimas de cuidados y seguridad física		Cena		OSINT: WITNESS	
					Cena		Taller de uso y administración de Nextcloud (Labo)	
	19:00 a 20:00	Comedor						
	20:30 en adelante	Hotel en Quito	películas		salida		películas	
							convivio compartencia	





PRESENCIAL (septiembre)	MÉRCOLES 25	JUEVES 26	VIERNES 27	SABADO 28	DOMINGO 29
	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	Visiónado material y plataformas			
	Proyección acompañamiento y soporte. Cómo nos vamos a vincular?				
	Comida/Almuerzo	Comida/Almuerzo	Comida/Almuerzo hotel en Quito	Comida/Almuerzo	
	Archivo (Inés Witness)	Comida/Almuerzo			
	Refrigerio	Refrigerio	17:00 horas Inauguración de los Diálogos en el Auditorio de la Conale	Diálogos Clausura en la Casa de la Cultura	
Taller de creación de páginas web (Suty)	Paseo a orquideario en Puyo				
	Cena de cierre en Puyo				
	Cena		Cena	Cena de despedida en Quito	



EN LÍNEA (octubre)	DOCUMENTACIÓN		TUTORÍAS		SERVIDORES	
	DOCUMENTACIÓN		TUTORÍAS		SERVIDORES	
	DOCUMENTACIÓN		TUTORÍAS		SERVIDORES	
	Sesión 15 de octubre	Herramientas jurídicas para la defensa del territorio (Celso)	Sesión 212 de octubre	OSINT y uso en la defensa del territorio (Witness)	Sesión 319 de octubre	Archivo: Creación de categorías y colecciones (Witness)
	Sesión 16 de octubre	OSINT y uso en la defensa del territorio (Witness)	Sesión 213 de octubre	OSINT y uso en la defensa del territorio (Witness)	Sesión 320 de octubre	OSINT y uso en la defensa del territorio (Witness)
	Sesión 17 de octubre	OSINT y uso en la defensa del territorio (Witness)	Sesión 214 de octubre	OSINT y uso en la defensa del territorio (Witness)	Sesión 321 de octubre	OSINT y uso en la defensa del territorio (Witness)
	Sesión 18 de octubre	OSINT y uso en la defensa del territorio (Witness)	Sesión 215 de octubre	OSINT y uso en la defensa del territorio (Witness)	Sesión 322 de octubre	OSINT y uso en la defensa del territorio (Witness)
	Sesión 19 de octubre	OSINT y uso en la defensa del territorio (Witness)	Sesión 216 de octubre	OSINT y uso en la defensa del territorio (Witness)	Sesión 323 de octubre	OSINT y uso en la defensa del territorio (Witness)
	Sesión 6 de noviembre	Uso del Video para la defensa Medio Ambiental (Witness)	Sesión 52 de noviembre	Presentación de Red de Servidores Autónomos (Nodo Abyayala)	Sesión 716 de noviembre	Herramientas de monitoreo con software y hardware libre (Colnodo)
	Sesión 7 de noviembre	Uso del Video para la defensa Medio Ambiental (Witness)	Sesión 53 de noviembre	Presentación de Red de Servidores Autónomos (Nodo Abyayala)	Sesión 717 de noviembre	Herramientas de monitoreo con software y hardware libre (Colnodo)
	Sesión 8 de noviembre	Uso del Video para la defensa Medio Ambiental (Witness)	Sesión 54 de noviembre	Presentación de Red de Servidores Autónomos (Nodo Abyayala)	Sesión 718 de noviembre	Herramientas de monitoreo con software y hardware libre (Colnodo)
	Sesión 9 de noviembre	Uso del Video para la defensa Medio Ambiental (Witness)	Sesión 55 de noviembre	Presentación de Red de Servidores Autónomos (Nodo Abyayala)	Sesión 719 de noviembre	Herramientas de monitoreo con software y hardware libre (Colnodo)
	Sesión 10 de noviembre	Uso del Video para la defensa Medio Ambiental (Witness)	Sesión 56 de noviembre	Presentación de Red de Servidores Autónomos (Nodo Abyayala)	Sesión 720 de noviembre	Herramientas de monitoreo con software y hardware libre (Colnodo)
- 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						

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 otro

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

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

No juzgar.
Preguntar,
profundizar.

Respetar cómo cada
quien quiere/pide ser
llamado/nombrado

Respeto de
pronombres

Respetar los
tiempos de
descanso.

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

RESPECTAR
LOS
TIEMPOS EN
EL USO DE
LA
PALABRA

Evitar
actitudes de
índole
patriarcal

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

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 todos de
la misma manera, estar
atentos a la necesidad
de precisar, aclarar
algo que no se
comprendió

**TOMAR LAS
COSAS CON
CALMA PARA NO
CAER EN
MALENTENDIDOS.**

Paciencia.
No todos tenemos
los mismos
tiempos y
conocimientos.

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 dispuestos 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

Ayudar con
material extra
para los procesos
de aprendizaje en
convivencia

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

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

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

o un tema determinado que
compartan lxs compañerxs
durante la Escuela.

Protocolo de acción frente a situaciones de
acoso a las compañeras que implique hablar
con
la persona que realizó 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.

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 Marañón en Perú, que a su vez



Río Puyo

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
- La vida, el análisis y la seguridad de los datos
- Cómo grabar violaciones ambientales
- Formato para llenar



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

Andrés Tapia, Lancers Digitales

Amazonía

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



Situación de Conectividad a Internet y Otros Medios de Comunicación de los Pueblos Indígenas

Amazonia Ecuatoriana, Peruana, Colombiana, Región Trópico Húmedo de México

- 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, Sucumbios 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 Tuntwittereros

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 REFORMATIVA – 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 conexión y operación de frecuencias.

🔥 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 Agustin 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

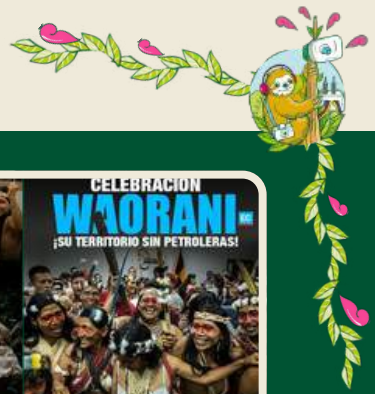


#ResultadosYa



#FuerzaShuar Arutam





#FuerzaShuar Arutam



#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, buscamos guardar aspectos básicos de un dato ahora convertidos en archivos digitales. Este ciclo debe conocerse, practicarse y profundizarse pues permite con el 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 utilizar 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 usuarios y administradores. 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 electrónico 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. Aquí 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 recordará, 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 y de 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.

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.



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.



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, auditorías 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.

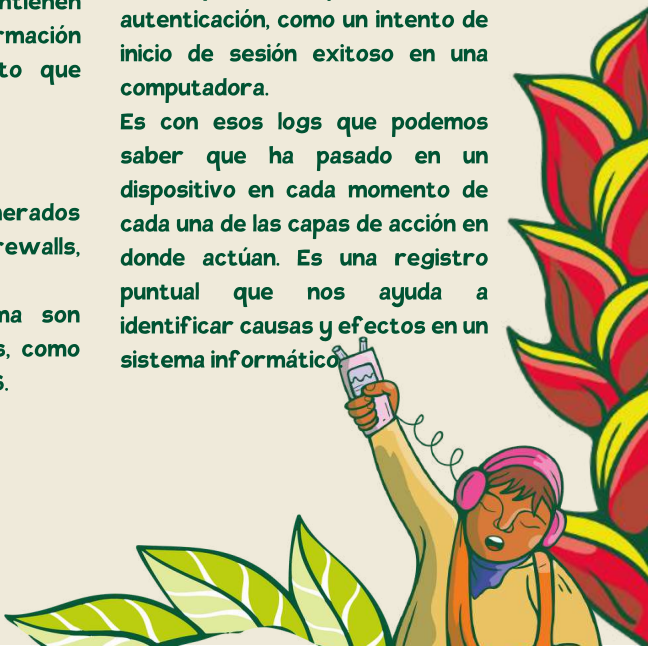
Sistema: Los registros de sistema son generados por sistemas operativos, como Chrome OS, Windows, Linux o macOS.

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 ingeniería 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?



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

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

 es.witness.org

 [@witness_es](https://twitter.com/@witness_es)

 [witnessespanol](https://www.facebook.com/witnessespanol)

 [witness_es](https://www.instagram.com/witness_es)

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



bitly

FORMATO PARA LLENAR

METAS

SITUACIÓN ACTUAL

OBJETIVO





METAS

FORMATO PARA LLENAR

SITUACIÓN ACTUAL

OBJETIVO



EJEMPLO DE JÚBA WAJIIN

Resumen del caso

En 2011, la comunidad indígena me'phaa (tlapaneca) de San Miguel El Progreso (o la comunidad Júba Wajiin), 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 Wajiin, sin embargo, el gobierno mexicano otorgó a las empresas estas concesiones mineras sin consultar a la comunidad. Como respuesta, la comunidad Júba Wajiin 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 Wajiin 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 Wajiin. 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 Wajiin, aunque no se llegó a lograr la declaración de inconstitucionalidad de la Ley Minera en México.



VIDEO 1

Suprema Corte de
Justicia de la Nación



VIDEO 2

Aliadxs y medixs
(1 minuto)



VIDEO 3

Comunidades
(40 minutos)

EJEMPLO FORMATO JUBA WAJIIN

OBJETIVO

Lograr tener sus archivos en control y manos de la comunidad

ARCHIVO

MULTIMEDIA:

PRODUCCIÓN O

DIFUSIÓN

JURÍDICO

Obtener una sentencia favorable que declare la inconstitucional la Ley Minera por contravenir la Constitución y el Artículo 169 OIT.

SITUACIÓN ACTUAL

Tienen archivos pero sobre todo en casas y en organizaciones que les han apoyado como el Centro de Derechos Humanos de la Montaña Tlachinollan.

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.

METAS

Juntar en el disco duro de la comunidad toda la información, acordar previamente el formato para organizar el material

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

SERVIDORES

ÍNDICE

- Sabor a libertad: El Software Libre y la construcción colectiva del conocimiento
- Resumen de "La Era del Capitalismo de la Vigilancia" de Shoshana Zuboff
- IA y crisis climática: las grandes tecnológicas escogen España para instalar sus gigantescos centros de datos
- ¿Qué hacemos con nuestra huella de carbono digital?: asumiendo el coste ecológico de nuestros datos.
- Distribúyase
- ¡Queremos redes libres!
- ¿Por qué hicimos Servidores Autónomos Replicables?
- Comic: Mamá ¿Por qué hay una pequeña nube en casa?



SERVIDORES



Sabor a libertad: El Software Libre y la construcción colectiva del conocimiento

Imagina un mundo en el que todo el software es como la comida que te sirve tu abuela: hecha en casa, con ingredientes frescos, siguiendo recetas abiertas y compartidas por generaciones. Ese es el mundo del software libre, una filosofía y un movimiento que surgió hace más de cuatro décadas y que hoy impulsa otra forma de hacer tecnología. En contraste, tenemos el software propietario, que es más como la comida rápida de McDonald's: rápida, conveniente, pero con recetas secretas que solo conoce la empresa.

@copyleft

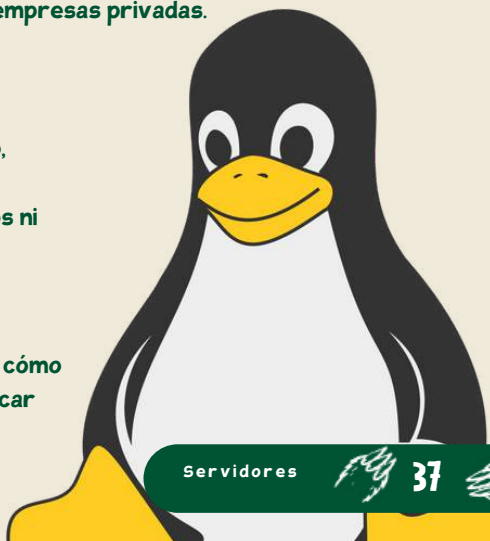
Un Poco de Historia

El concepto de software libre se originó a principios de la década de 1980 con Richard Stallman, un programador y activista que creía que el software debería ser libre, no solo en términos de costo, sino también en cuanto a libertad. Fundó el Proyecto GNU y la Free Software Foundation, estableciendo las cuatro libertades esenciales del software libre: la libertad de usar el software, estudiarlo, modificarlo y compartirlo. Con el tiempo, esta idea se expandió y el software libre se convirtió en un movimiento global. Surgieron sistemas operativos como GNU/Linux. A través de los años, el software libre ha demostrado ser una alternativa sólida, segura y ética frente al software propietario. La evolución de GNU/Linux y otros proyectos de software libre ilustra cómo el desarrollo colaborativo y abierto puede superar incluso a las soluciones ofrecidas por las grandes empresas privadas.

¿Qué es el Software Libre?

Este tipo de software es abierto: cualquiera puede ver cómo está hecho, modificarlo según sus necesidades y compartirlo con otros. No hay secretos ni ingredientes ocultos.

El software propietario puede ser conveniente y rápido, pero no sabes exactamente qué ingredientes usan o cómo se prepara. Además, no puedes modificar





la receta no compartirla. Solo puedes consumirlo tal y como lo ofrecen. Al igual que con la comida rápida, donde puedes encontrar ingredientes desconocidos, en el software propietario puedes estar expuesto a herramientas de monitoreo que las grandes empresas tecnológicas utilizan para vigilar y monetizar tu comportamiento, sin que tengas acceso completo a lo que el software realmente hace.

¿Quién Hace el Software Libre?

El software libre es creado por comunidades de personas de todo el mundo que creen en la colaboración y el apoyo mutuo. Imagina a un grupo de vecinos que se reúnen para hacer una gran comida comunitaria, cada quien aportando lo que sabe y tiene. Este es el espíritu detrás de proyectos como GNU/Linux, LibreOffice y Firefox, entre otros. Miles de programadores y entusiastas colaboran para mejorarlos constantemente.

En cambio, el software propietario es desarrollado por grandes empresas como Microsoft, Apple o Adobe. Es como si esas empresas fueran los chefs de un restaurante que guarda celosamente sus recetas. Ellos controlan lo que puedes y no puedes hacer con su software. Si bien ofrecen ciertos beneficios, la mayoría de las veces estas empresas no permiten que los usuarios vean o modifiquen el código del programa.

Costos para las Personas Usuarías

Una de las mayores ventajas del software libre es que, en la mayoría de los casos, es gratuito. Puedes descargarlo, instalarlo y usarlo sin pagar nada. Es como recibir la comida de la abuela sin costo, ya que es el resultado del trabajo compartido y solidario de una comunidad. En cambio, el software propietario, como las hamburguesas de McDonald's, puede parecer barato al principio, pero con el tiempo, los costos se acumulan. Debes pagar por licencias, actualizaciones y, a veces, incluso por soporte técnico.

Soporte y Comunidad

Cuando utilizas software libre, no estás solo. Detrás de cada programa hay comunidades de usuarios y desarrolladores que están dispuestos a ayudar. Los foros de discusión, listas de correos y grupos en línea están llenos de personas que, de forma voluntaria, comparten soluciones y mejoras.



Seguridad: Más Allá de la Comida Rápida

El software libre es conocido por ser más seguro. Como el "recetario" es abierto y accesible, muchas personas pueden revisar y mejorar la seguridad del software. Si alguien encuentra un problema, lo soluciona rápidamente y lo comparte con todos.

Por el contrario, en el mundo del software propietario, solo la empresa sabe cómo está hecho el programa. Si hay un problema de seguridad, dependes de ellos para solucionarlo. Este 2024, Microsoft sufrió un grave problema en un paquete de actualización de Windows, generando fallos alrededor del planeta especialmente en la industria aeronáutica. Esto sería menos probable en un entorno de software libre, donde la revisión continua por parte de la comunidad reduce la posibilidad de problemas críticos.

La Nube: Software Libre en Acción

Gran parte de los servicios que usamos en línea, como ver videos, enviar correos o hacer búsquedas, dependen de servidores en la "nube". Lo que no muchos saben es que la gran mayoría de estos servidores funcionan con software libre. El 90% de la infraestructura en la nube, incluyendo la de gigantes como Amazon Web Services (AWS), Google Cloud Platform (GCP) y Microsoft Azure, utiliza Linux como sistema operativo. Esto sucede simplemente porque el software libre al ser adoptado (y adaptado) ampliamente, su desarrollo alcanza mayores niveles que otros softwares privativos.



El Conocimiento Humano y el Software Libre

Desde el inicio de los tiempos, el conocimiento humano ha crecido y evolucionado a través de la colaboración y el intercambio libre de ideas. Un ejemplo notable de esta colaboración es el desarrollo del maíz, uno de los cultivos más importantes del mundo. Hace miles de años, los pueblos originarios de América Central y del Sur tomaron una planta silvestre llamada teocintle y, a través de generaciones de selección y mejora, la transformaron en lo que hoy conocemos como maíz. Este proceso no se hizo de forma aislada ni por una sola persona; fue el resultado de comunidades que compartieron sus conocimientos, experimentaron y mejoraron el cultivo de manera colectiva.



La evolución del maíz es un claro ejemplo de cómo el conocimiento compartido puede mejorar y beneficiar a todos. Así como los agricultores ancestrales compartieron sus técnicas y semillas para mejorar el maíz, hoy en día los desarrolladores y usuarios de software libre comparten su código y conocimientos para mejorar las herramientas digitales que todos usamos. Este proceso de evolución abierta y colaborativa ha permitido que el software libre prospere y se adapte rápidamente a las necesidades cambiantes de la sociedad.

Wikipedia, por ejemplo, es una enciclopedia colaborativa y libre que demuestra cómo el conocimiento compartido puede crecer exponencialmente. Cualquier persona puede editar artículos, corregir errores y añadir nueva información, lo que permite que el conocimiento colectivo se perfeccione constantemente.

El software libre no solo representa una opción más económica, segura y ética, sino que también encarna la idea de compartir y construir conocimiento colectivamente.

Resumen de "La Era del Capitalismo de la Vigilancia" de Shoshana Zuboff

Shoshana Zuboff, en su libro "La era del capitalismo de la vigilancia: La lucha por un futuro humano frente a las nuevas fronteras del poder", presenta un análisis profundo de cómo las grandes empresas tecnológicas han desarrollado un nuevo tipo de capitalismo basado en la recolección masiva de datos personales y su uso para influir en el comportamiento humano.



¿Qué es el Capitalismo de Vigilancia?

El capitalismo de vigilancia es un modelo económico que surgió con las grandes empresas de tecnología, como Google, Facebook, Amazon y Microsoft, que se basa en la extracción, análisis y comercialización de datos personales. Estas empresas "venden" predicciones sobre el comportamiento de las personas a través de la recolección de datos masivos que obtienen a partir de la actividad en línea de los usuarios, como búsquedas en internet, interacciones en redes sociales o uso de aplicaciones móviles. Estas predicciones son utilizadas por anunciantes y otras compañías para dirigir campañas publicitarias de manera precisa, influyendo en lo que las personas compran, piensan e incluso cómo actúan (La era del capitalismo de la vigilancia, p. 8).



La Materia Prima: Los Datos Personales

En el capitalismo de vigilancia, los datos personales se han convertido en la materia prima más valiosa. Cada acción que una persona realiza en internet, desde búsquedas en Google hasta los movimientos del cursor del ratón, es recolectada y analizada. Estos datos, que a menudo las personas entregan sin darse cuenta o por conveniencia, son utilizados para crear perfiles detallados que permiten a las empresas predecir comportamientos futuros (La era del capitalismo de la vigilancia, pp. 94-95). Más allá del ámbito digital, la proliferación de dispositivos "inteligentes" en los hogares también ejemplifica esta extracción continua de la experiencia humana. Esta invasión del espacio privado amplía la capacidad de las empresas para conocer cada detalle de nuestra vida cotidiana y monetizar esta información.

La Pérdida de la Autonomía Humana

Zuboff argumenta que el capitalismo de vigilancia no solo recolecta datos, sino que también utiliza esos datos para manipular el comportamiento. Esto se hace a través de herramientas de persuasión, como las notificaciones personalizadas o los algoritmos de recomendación, que guían a los usuarios hacia ciertos comportamientos o decisiones sin que ellos se den cuenta (La era del capitalismo de la vigilancia, p. 295). Por ejemplo, plataformas como YouTube y TikTok utilizan algoritmos avanzados para mantener a los usuarios enganchados el mayor tiempo posible. Este tipo de manipulación erosiona la libertad individual y convierte a las personas en objetos controlados por fuerzas que no comprenden completamente.

La Asimetría del Conocimiento

Un concepto fundamental que introduce Zuboff es el de "asimetría del conocimiento", que describe la desigualdad entre lo que las empresas de tecnología saben sobre las personas y lo que las personas saben sobre estas empresas (La era del capitalismo de la vigilancia, p. 131).

Mientras las corporaciones tecnológicas tienen acceso a enormes cantidades de datos sobre cada aspecto de nuestras vidas, los usuarios suelen ser ignorantes de cómo se recopilan, analizan y utilizan esos datos. Este fenómeno quedó en evidencia nuevamente en 2021 cuando Apple introdujo cambios en su política de privacidad que obligaron a las aplicaciones a pedir permiso explícito a los usuarios para rastrear su actividad en otras aplicaciones y sitios web. Facebook y otras compañías protestaron vehementemente contra esta medida, ya que afectaba directamente su modelo de negocio basado en la recolección de datos.

El Peligro para la Democracia

Según Zuboff, el capitalismo de vigilancia no solo afecta a los individuos, sino que también representa un peligro para la democracia. La capacidad de manipular a grandes grupos de personas puede ser utilizada para influir en elecciones, fomentar la polarización y desestabilizar sociedades (La era del capitalismo de la vigilancia, pp. 371-373).

Un ejemplo destacado es el escándalo de Cambridge Analytica en 2018, donde se reveló cómo los datos recolectados de millones de usuarios de Facebook fueron utilizados para influir en elecciones en varios países, incluyendo el referéndum del Brexit y las elecciones presidenciales de Estados Unidos en 2016.

La Expansión del Capitalismo de Vigilancia Más Allá del Ámbito Digital

El capitalismo de vigilancia no se limita solo a las empresas tecnológicas y al ámbito digital; su lógica ha permeado también la producción y operación de empresas de otros sectores. Empresas de retail, fabricantes de automóviles, aseguradoras y bancos han comenzado a adoptar prácticas similares de recolección y análisis de datos. (La era del capitalismo de la vigilancia, p. 451). Zuboff llama a la acción y advierte que es necesario un esfuerzo colectivo para resistir el capitalismo de vigilancia y proteger un futuro en el que los seres humanos no sean tratados como meros recursos de datos.



IA y crisis climática: las grandes tecnológicas escogen España para instalar sus gigantescos centros de datos

Resumen del artículo publicado en Diario El Salto por Pablo Jiménez Arandia.
Consulta la versión completa en: <https://www.elsaltodiario.com/inteligencia-artificial/meta-centro-datos-agua-sequia>

El boom de la IA ha disparado las necesidades de computación de los centros de datos y su consumo de agua. Mientras las resistencias a estos complejos crecen por el mundo, las grandes tecnológicas buscan nuevas regiones para instalarlos. España entre ellos.

"Mi interés por esto viene porque ya lo he vivido", dice Aurora Gómez mientras pasea por el parque Madrid Río, junto al río Manzanares. Gómez, activista por los derechos digitales y medioambientales, recuerda un momento concreto de su infancia al hablar del proyecto que el gigante de internet Meta —antes Facebook— está a punto de construir en Talavera de la Reina, provincia de Toledo."



Fotografía: Terrenos donde la compañía Meta planea construir su nuevo centro de datos, en las inmediaciones de Talavera de la Reina (Toledo).

Cuando tenía 15 años, Gómez escuchó las primeras noticias sobre los planes para construir un aeropuerto al lado de su pueblo natal, Ballesteros de Calatrava. Corría la segunda mitad de la década de 1990 y el Gobierno de Castilla-La Mancha de entonces decidió expropiar a su abuelo unas tierras agrícolas muy fértiles. Su familia fue a juicio y ganó. Pero para entonces el aeropuerto de Ciudad Real, hoy un elefante blanco en manos privadas del que no despegan aviones, ya estaba en pie.



Igual que ocurrió en su momento con este aeropuerto fantasma el Gobierno castellano-manchego ha declarado el proyecto planeado por Meta para construir un enorme centro de datos en Talavera de la Reina como de “singular interés” para la región. Una figura legal que facilita los trámites que la compañía estadounidense ha de cumplir para levantar el que será su cuarto centro de este tipo en Europa, el más grande hasta la fecha.

El aspecto exterior de los centros de datos puede variar mucho. Pero en su interior hay pocas sorpresas: hileras de servidores colocados unos encima de otros funcionando día y noche. Una especie de granja de la era digital que almacena y procesa datos para que todo tipo de aplicaciones online puedan funcionar. En estos lugares, la nube se hace física.

En los últimos años las preocupaciones sobre el coste medioambiental de estas infraestructuras han ido en aumento. Sobre todo al hablar de los centros más grandes, conocidos en inglés como hyperscale. Países como Irlanda, Países Bajos o Singapur han aplicado recientemente diferentes tipos de moratorias a su construcción.

Diversas investigaciones señalan en los últimos meses un incremento sostenido de la demanda de agua de gigantes de internet como Google o Microsoft por el auge de la IA

La Comisión Europea ha puesto también su foco en este tipo de complejos con su nueva directiva de eficiencia energética, que pronto obligará a los propietarios de centros con una capacidad mínima instalada de 500 kW a informar sobre su gasto energético.





Pero la electricidad no es la única preocupación que rodea a estas infraestructuras. Los racks de servidores que se almacenan en los centros de datos necesitan sistemas de refrigeración que eviten un calentamiento excesivo de los equipos. A pesar de que las soluciones técnicas varían entre instalaciones, hoy es habitual el uso de tuberías con agua fría para mantener a los servidores a una temperatura constante.

Agua, ¿pero cuánta?

Saber cuánta agua consume un centro de datos no es sencillo. Hasta ahora, las grandes compañías tecnológicas han evitado en muchos casos ofrecer números precisos. En otros, los datos revelados han resultado poco útiles: en Países Bajos, en 2021, en plena sequía nacional, una investigación periodística reveló que un centro de Microsoft consumía cuatro veces más agua que la que había anunciado la empresa.

El actual boom de la inteligencia artificial (IA) está escalando este problema a otro nivel. Los productos de IA generativa, como los chatbots o las aplicaciones para crear artificialmente contenidos, precisan de capacidades de computación nunca vistas hasta la fecha.

[...]

Como en otras regiones españolas, la falta de lluvias y el aumento de las temperaturas ha provocado en los últimos años periodos de sequía recurrentes en la cuenca del Tajo, que riega el territorio donde Meta instalará su nuevo centro de datos. Aunque estas tierras no viven una situación tan límite como otras zonas del país, en el último lustro las autoridades de la región han activado varias veces planes de acción especiales contra la sequía.

Miguel Ángel Hernández, de Ecologistas en Acción, señala que los cálculos sobre la disponibilidad de agua se han hecho en un "escenario promedio", teniendo en cuenta tanto las épocas de sequía como las de abundancia de los últimos años. "Pero resulta que vamos hacia un escenario en el que cada vez hay menos recursos disponibles en la cuenca del Tajo. Y en el que las situaciones de crisis, por episodios de altas temperaturas o baja precipitación, son cada vez más graves", analiza Hernández.

Las dudas mostradas por algunas voces no impidieron que el gobierno regional tramitase oficialmente en marzo pasado la evaluación de impacto ambiental del proyecto, al considerar el consumo previsto de agua por la empresa dueña de Facebook, Instagram y Whatsapp como “adecuado” para la zona.

Buscando un trozo de tierra en el sur

Susan Schaap vive en Zeewolde, una pequeña localidad en Países Bajos. Schaap recuerda que la primera vez que oyó hablar del centro de datos que Meta planeaba instalar en su pueblo fue durante una videollamada organizada por el ayuntamiento. En la reunión, hecha online por culpa del covid-19, había unas 50 personas, entre concejales y vecinos. En ella se les informó que el complejo proyectado ocuparía una enorme parcela de terreno hasta entonces dedicada a la agricultura.

Para cuando Schaap y sus vecinos se enteraron de esos detalles, los enviados de la compañía estadounidense llevaban meses negociando con las autoridades locales.

“Si vamos a pagar por esto, como ciudadano tengo algo que decir”, argumenta esta comercial de profesión, reconvertida a activista, que lideró hace un par de años el movimiento vecinal contra el proyecto de Zeewolde, finalmente cancelado por la empresa. Resistencias similares se han dado también en países como Chile, Irlanda, México y Singapur, entre otros.

En un contexto de creciente oposición en los países del centro y norte de Europa, las big tech están girando cada vez más su mirada más hacia el sur del continente. En una tendencia similar a la que se está viviendo al otro lado del Atlántico, donde los países latinoamericanos están acogiendo cada vez más infraestructuras de este tipo.

“(El almacenamiento y procesamiento de datos) es un problema para todas las grandes tecnológicas, todas están buscando dónde construir”, explica un antiguo ingeniero de Meta especializado en el diseño de centros de datos, que trabajó en la compañía seis años y prefiere mantener su anonimato.



Esta fuente apunta que a día de hoy dar con regiones “receptivas para su construcción” es “el factor fundamental” que mueve a estas compañías a decidirse por una u otra ubicación. A ello se añaden factores propios de cada empresa como las necesidades de conectividad, de energía y un gobierno estable, explica.

“¿Cuántos centros son asumibles?”

En una soleada mañana de enero, desde la granja de Luis Miguel Pinero se ve al fondo la Sierra de Gredos nevada. Justo detrás de esta cadena montañosa al norte de Talavera de la Reina nace el río Alberche, que abastece de agua al área donde se instalará el centro de Meta. Este río afluente del Tajo también riega los terrenos de cultivo de Pinero, un agricultor de barba canosa y manos curtidas por el trabajo en el campo.

Apoyado en un tablón de madera en su granja, Pinero explica cómo en los últimos años en la zona han sufrido varias restricciones en el suministro de agua. Periodos en los que el caudal suministrado por el Alberche no era suficiente, que se solucionaron con el desvío de agua proveniente de otro caudal, el del Tajo, mucho más contaminado. “A mi esa agua no me sirve”, apunta este pequeño productor de tomates ecológicos y otras hortalizas.

A diferencia de lo que está ocurriendo en otras latitudes, hoy en Talavera de la Reina y sus alrededores prácticamente no existe contestación ciudadana al gran centro de datos de Meta. Pinero, que si se muestra escéptico sobre los beneficios del proyecto para la población local, cree que tanto los políticos de la región como la empresa se han encargado de apartar del debate público los posibles efectos negativos del proyecto.

“La gente está esperanzada porque va a traer puestos de trabajo. ¿Este tipo de proyectos se supone que va a traer eso, no?”, se pregunta Pinero. Con una tasa de paro del 24%, un descenso continuado de la población en las últimas décadas y un abandono sostenido de las instituciones, en esta comarca muchos ven la inversión de Meta como una posible salvación.



Pero otras voces creen que es el momento de replantearse la construcción de proyectos tan demandantes en recursos. "A pesar de que la empresa alega eficiencia, proyectos como este tienen consumos muy elevados", explica Begoña Valero, técnica de conservación de la ONG SEO Birdlife.

Valero argumenta que es urgente una mayor toma de conciencia ciudadana sobre la huella medioambiental de los productos y servicios digitales. "Hay que trasladarle a la sociedad que todo esto, que parece tan etéreo, tiene una parte física. Que detrás de estas tecnologías están estas infraestructuras". Y añade que "el consumo de datos no va a dejar de disminuir". "¿Cuántos centros de datos son asumibles? A lo mejor hay que racionalizar el uso de estas herramientas", reflexiona.

Aurora Gómez, hace unos meses creó como contestación al centro de Meta en Talavera la asociación Tu nube seca mi río, reclama hablar también de la amenaza a nuestra "soberanía tecnológica" que, valora, supone que estos grandes complejos pertenezcan a un puñado de actores privados, capaces de imponer una narrativa asociada al "progreso" social y económico de la zona — igual que ocurrió hace 25 años con el aeropuerto que construyeron sobre los terrenos de su familia, rememora—. "Escogen territorios despoblados y envejecidos, donde la contestación sea nula", asegura Gómez. "Cuando una zona ya está despoblada es cuando puede aparecer una invasión del territorio. Y ahí ya da igual", remacha.

¿Qué hacemos con nuestra huella de carbono digital?:
asumiendo el coste ecológico de nuestros datos.

Publicado en Tu Nube Seca Mi Río,
consulta el artículo completo en:



¡Viva la soberanía digital!





El otro día asesoramos a un pódcast de la BBC hablando de nuestro tema #Agua y #CentrosDeDatos. Y la periodista hizo «la pregunta»: ¿Cómo podemos reducir el consumo de agua de nuestros datos? Y nos recorrió un escalofrío por la espalda: ¿De verdad vamos a volver a caer en la individualización de la culpa en otra actividad contaminante?

La trampa de individualizar la culpa

¿Qué es esto de la #IndividualizaciónDeLaCulpa? Pues es poner el foco de atención en los comportamientos individuales en vez de los elementos estructurales o fijarla en los verdaderos responsables.

Esto es lo que nos pasó con la Huella de Carbono.

La Huella de Carbono es un concepto inventado por la British Petroleum para desviar la atención de su responsabilidad del Cambio Climático a las personas individuales.

Así, la gente pensaría que su problema serían sus comportamientos individuales (ej. cogen el coche para ir al trabajo), en vez de centrarse la responsabilidad de las petroleras y grandes corporaciones.

¿La culpa del cambio climático es de un trabajador precario del extraradio de una ciudad que coge su coche para ir a trabajar a la otra punta de la ciudad? ¿O es de la petroleras que venden el petróleo y presionan a los gobiernos para crear sociedades coche-céntricas que hacen inviable trabajar a 15 minutos andando de tu casa?

Pues lo mismo nos pasa con los Centros de Datos.

Nuestro rol como consumidores digitales en el gasto de datos

Claro que podemos tomar medidas individuales para reducir el consumo de datos. Pero nuestra «culpa» del consumo de agua y energía de los centros de datos se circunscribe al rol de consumidores. Y por supuesto que no es culpa, sino responsabilidad. Cuando cambiamos el concepto moral de la culpa, al de responsabilidad nos permite dejar atrás las emociones paralizantes y pasar a la acción.

Es desde el rol de «productor» donde están las verdaderas responsabilidades y mayores capacidades de acción.



Es decir, hay que mirar hacia Musk Zuckemberg, Sam Altman... y todos estos Bros de Silicon Valley. Ellos tienen la capacidad de elegir tecnologías menos depredadoras con el medio ambiente, no acumular esa cantidad de datos para luego vendernos crecepelos. O no instalar Centros de Datos en territorios con estos niveles de estrés hídrico.

¿Quiere decir eso que nosotros como consumidores no tenemos que nada que hacer?

Por supuesto que no.

En primer lugar cuando pensamos en nuestro consumo de datos, formamos parte de un ecosistema digital. Y con nuestro consumo podemos cambiarlo, pero no de manera individual sino colectiva, que es donde reside nuestro poder. Nuestros gestos individuales son gotas perdidas en la nada en solitario, y forman ríos dentro de una colectividad.

Claro que podemos dejar de utilizar las redes sociales, las plataformas de streaming, o hacer limpieza de nuestra bandeja de entrada y desuscribirnos de las newsletter.

Pero es más importante que reflexionemos y creemos esta conversación con nuestros seres queridos.

En primer lugar cuando pensamos en nuestro consumo de datos, formamos parte de un ecosistema digital. Y con nuestro consumo podemos cambiarlo, pero no de manera individual sino colectiva, que es donde reside nuestro poder.
Aurora Gómez, Tu Nube Seca Mi Río.

Por ejemplo, que a nuestros familiares y amigos les digamos que no vamos a participar en el Whatsapp de la familia porque es una barbaridad a nivel de privacidad, pero también en consumo de agua y energía. Que a nuestros colectivos activistas que no pensamos utilizar los servicios de Google para organizarnos. A nuestras empresas que utilizar la IA para nuestros procesos diarios quizás no sea la mejor opción.

Y si somos trabajadores del sector tecnológico, podemos traer esa mirada para que nuestras actividades sean más eficientes en agua y energía.



O como ciudadanía presionar a nuestros gobiernos y ayuntamientos locales para que tomen mejores decisiones en la gestión de datos. Y sobre todo, que no permitan esta proliferación tan peligrosa de Macro-Centros de Datos como la que amenaza España y otros territorios.



Asumiendo nuestra Soberanía Digital

Asumir nuestra parte de #SoberaníaTecnológica es vital para cambiar nuestro rol como consumidores en un ecosistema digital.

Aurora Gómez, Tu Nube Seca Mi Río.



¿Por qué? Porque al hacerlo nos sentimos con más conocimiento y poder. Pocas cosas te hacen sentir más poder que tener un servidor propio, y ser capaz de gestionar tus propios servicios como web, correo o redes sociales. Al abrazar nuestra soberanía digital asumimos unos comportamientos digitales más conscientes.

Cuando abrimos una red social libre como Mastodon, nos damos cuenta de toda la publicidad que nos evitamos (que consumen muchos datos). Nos acostumbramos a borrar los post antiguos, porque sabemos que son una sobrecarga en el servidor. Porque conocemos al admin, y entendemos parte de sus decisiones en cuanto a manejo de recursos limitados. E incluso limitamos el número de Gifs y los cambiamos por nuestros molones emojis. 😊

Y así volvemos a ser conscientes de que nuestros datos «pesan», «consumen», y «son caros». Pero también tenemos más capacidad de acción.

En resumen, como consumidores digitales podemos tomar responsabilidad de nuestro rol. Asumir un papel activo y presionar con nuestras preferencias de consumo. Hacer del consumo digital un proceso activo y consciente, sobre el que reflexionar en colectivo.



Distribúyase

Contenidos importantes y únicos: perdidos, perdidos como lágrimas en la lluvia... ¿Cómo hacemos para publicar y compartir de nuevas maneras, para dejar de ser evanescentes? Tres mantras y seis formas nuevas de hacer las cosas.

“Está habiendo denuncias de que se dieron de baja programas de MAGA viejos. Apparently hubo un problema en el canal de Youtube... Se perdieron archivos, hubo un “MAGAleaks” y se perdieron cosas... Perdidos, perdidos como lágrimas en la lluvia. Tal vez alguno de los archivos sólo los tiene un fanático en VHS en la casa.”

Tomás Rebord, en su programa radial[]*

Es común; nos acostumbramos a que con cierta frecuencia, cada tantos días al año, alguien en la Internet pierde sus contenidos o el acceso a su sitio web o a sus redes sociales...

A veces se lo toma con humor (¿o resignación?) y se comienza de nuevo. Otras tantas, es tal el impacto de ver arrasado un archivo comunitario, de un grupo social, incluso laboral o personal, que ponerle onda es difícil.

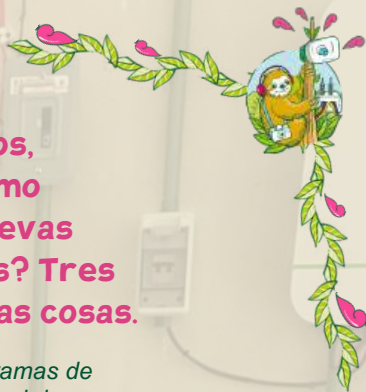
Hablar de “bajar algo”, “darle de baja”, refiere a la operación de borrado, destrucción, eliminación definitiva de cierto contenido, en general, por parte de una plataforma corporativa. A menos que se tenga una copia de respaldo. En el centro de este traspíe reiterado hay un problema de uso de la tecnología que – ¡sí, sí, sí! – podemos eludir.

Si solamente tenés unos segundos más, quedate con ésto: cuidá tu memoria de contenidos, hacé backups (copias de respaldo), publicá usando redes distribuidas. La lógica de torrents, de compartir archivos entre pares sigue más vigente que nunca. Los VHS se borran. Youtube censura. Las redes comunitarias nos cuidan.

Si tenés un minuto más, recordá estas máximas como mantras:

Tu lugar de difusión no puede ser tu lugar de almacenamiento. Mi plataforma de difusión no puede ser mi única plataforma de almacenamiento. Youtube no puede funcionar, no funciona, como archivo de un proyecto.

Y si tenés unos cuantos minutos más, te contamos 6 cosas nuevas que programadorxs y activistas están cuestionándose y cambiando.



Internet centralizada versus internet distribuida

Internet es fantástica y no tiene la culpa ;) Pero el espíritu capitalista que lo invade todo llevó a que la arquitectura de la red global se volviera ultra-centralizada; en la geopolítica latinoamericana, por ejemplo, los cuellos de botella hacia el resto del mundo pasan casi exclusivamente por EEUU. Muchísima, radicalmente mucha de nuestra información es almacenada por sólo un par de proveedores de servicios, o servidores, en centros de datos que asemejan monocultivos de computadoras. Enviamos nuestra información allí y así les entregamos el control de nuestra vida personal, de nuestra presencia online o de nuestros ingresos económicos a CINCO oligopolios. Si se cae una hora cualquiera de las big tech, nos damos cuenta de que perdimos temporalmente acceso a "nuestras cosas", a medios de comunicación, a transacciones... ¿Existe un espacio alternativo? Sí, se llama web distribuida, federada o descentralizada.

Hace pocos años, algunos activistas comenzamos a imaginar una Internet más justa. En lugar de una Internet basada en servidores (computadoras) propiedad de una persona o un par de grandes corporaciones, nos interesaba pensar en algo que muchas personas pudieran gobernar en conjunto. Ese algo se parece a cadenas o blockchains y generó un montón de proyectos y herramientas web3. PERO ESTE despliegue de criptomonedas, NFTs y metaversos no vino con un horizonte ético interesante, de mejora de los bienes comunes para la humanidad.

Como contrapropuesta, la web distribuida o dweb apuesta a respetar una serie de principios: beneficios distribuidos, responsabilidad ambiental, favorecer el uso de software libre, minimizar la vigilancia y manipulación algorítmica de las conductas humanas. Y las herramientas técnicas distribuidas que se producen deben servir como medios para llegar a estos fines. Si tu billetera virtual me vigila y vende mi información, no cambia el juego, no construye una sociedad mejor.





Podés leer todos los Principios en inglés aquí:

<https://getdweb.net/principles/>

Estamos por publicar la versión en castellano, así que no te olvides de revisar nuestro blog ;)

Redes distribuidas y federadas

En las redes sociales privadas y centralizadas como Facebook, Twitter, Instagram o Threads, se suma el problema de que lo que las personas leen está ordenado, gestionado y censurado mediante algoritmos con fórmulas misteriosas¹ que FILTRAN ciertos contenidos, personas y temas, diseñados para que queramos trabajar cada vez más en organizar datos que nos segmentan y convierten en publicitables.

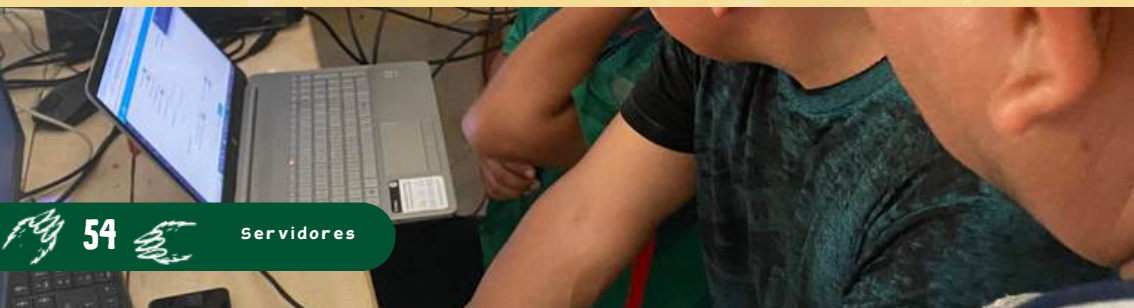
En cambio las redes libres, además de ofrecer su código fuente, lo que permite comprender sus algoritmos, se basan en acuerdos de federación y no tienen algoritmos de priorización, por lo que se llega directamente a las personas usuarias.

Además se les da mayor libertad en la elección de cómo quieren acceder al contenido que siguen, pudiendo utilizar multitud de aplicaciones, siempre y cuando sean compatibles con cierto protocolo común. Por ejemplo, Mastodon, PeerTube, BookWyrm son redes libres que usan ActivityPub, protocolo que en Suttty nos convence mucho y permite un intercambio de mensajes de tipo "actualización de estado" entre los servidores. Nosotros tenemos un perfil social en Mastodon, acá: <https://todon.nl/@suttty>

¿Y los sitios web?

Cuando pensamos más allá de un archivo, video o contenido en concreto y miramos los sitios web, también encontramos infinidad de problemas debido a la centralización. La vida promedio de las páginas web es de 100 díasssssss, según nuestra fuente.

Los links se rompen, un dominio cambia, un ataque organizado o una actualización tardía tiran abajo el sitio. Si nuestro sitio web depende de un único servidor, tenemos un enorme punto de falla: si el servidor deja de estar en línea (y eso pasa), nuestro sitio también.



La publicación distribuida, en cambio, ayuda a que los sitios sean más accesibles, resilientes y resistentes a la censura. Los seguidores del sitio pueden crear copias del mismo que otros pueden utilizar y volver a compartir, repartiendo la carga del alojamiento. Así, la distribución se convierte en un gesto de apoyo mutuo.

Desde Sutti, nuestra gestora de sitios web libre y gratuita, liberamos la opción "Publicar en la Web distribuida" para todos los sitios desde mayo 2023. Al activarla, cada sitio está disponible a través de los siguientes protocolos P2P (peer-to-peer, de pares): InterPlanetary File System (IPFS) y Holepunch, además del tradicional HTTP, el protocolo web más conocido y utilizado hasta ahora. Esta iniciativa se llama DistributedPress y es trabajo conjunto con Hypha y Filecoin Foundation for the Decentralized Web (FFDW).



Infraestructura distribuida

"Tal vez tener nuestros propios servidores nos ayudaría a adueñarnos de nuestras redes, así como algunos de nosotros compartimos colectivamente la propiedad de algún terreno." - traducido de Sacred Stacks. Un sueño para proyectos del Sur global.

Parece utópico pero no lo es. Estamos a tiempo de reclamar la propiedad colectiva de nuestra tierra, digo, de nuestra dimensión entre redes. Se trata de otra Internet posible, democrática, colectiva, garantizando el Derecho a la Comunicación de los pueblos.

¡El arte de la comunidad cyborg!

¡Queremos redes libres!

Qué es la neutralidad de la red

En estos días finalmente el gobierno de EE.UU. eliminó las protecciones que impedían a los operadores distinguir y priorizar entre distintos tipos de tráfico en Internet. Este fue el fin anunciado de la neutralidad de la red, ya que como consecuencia, los grandes conglomerados que manejan las redes podrían comenzar a discriminar el tráfico y crear para Internet un equivalente a los "paquetes" de canales que ofrecen los proveedores de TV por cable, donde algunos servicios comerciales tengan prioridad y sean más visibles, mientras que el acceso libre a todo lo demás quede relegado a un segundo plano.

El peligro: la invisibilización y censura de facto de medios alternativos y comunitarios.

¿Pero qué significa discriminar el tráfico y qué consecuencias conlleva? Cuando Personal, Claro, Tuenti, etc. te ofrecen "Whatsapp gratis", están violando la neutralidad de la red, porque al hacerlo privilegian el tráfico de un único servicio, mientras que alternativas más seguras como Signal (o incluso Telegram) "consumen" el paquete de datos que forma parte del plan que contrataste. De esta manera, las alternativas no incluidas en los paquetes promocionales se vuelven más costosas y solo son utilizadas por aquellas convencidas que tengan el dinero para pagar el plan más caro.

Entonces, la llamada neutralidad de la red es un principio fundamental para garantizar y universalizar el acceso a la información y el conocimiento.

La red nunca fue neutra

Sin embargo, las piratas creemos que la red nunca fue neutra, por lo que el nombre puede resultar engañoso. El famoso principio punta-a-punta de Internet, donde cada computadora conectada a la red puede acceder a cualquier otra computadora y a su vez puede ser accedida, nunca se cumplió realmente.

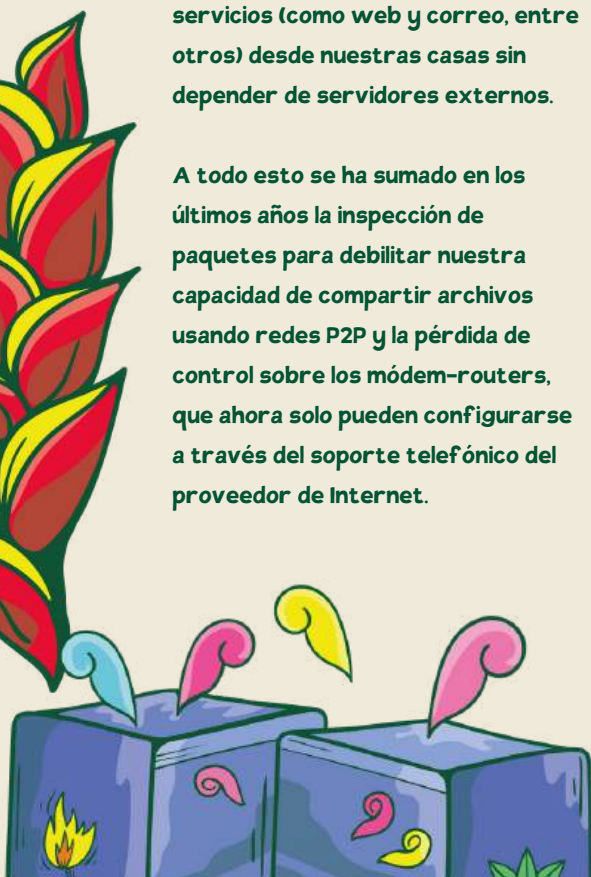
Las configuraciones tecnopolíticas de los servicios de Internet domésticos impiden que las redes sean realmente libres y distribuidas. Entre estas trabas se cuentan el ancho de banda asimétrico, donde podemos bajar más datos de los que podemos subir; los puertos bloqueados, donde no podemos tener nuestros propios servidores de correo; las IPs dinámicas, es decir las direcciones de Internet que cambian todo el tiempo y que si fueran estáticas nos permitirían publicar servicios (como web y correo, entre otros) desde nuestras casas sin depender de servidores externos.

A todo esto se ha sumado en los últimos años la inspección de paquetes para debilitar nuestra capacidad de compartir archivos usando redes P2P y la pérdida de control sobre los módem-routers, que ahora solo pueden configurarse a través del soporte telefónico del proveedor de Internet.

Se trata de un conjunto de medidas que han sido promovidas por el régimen de la Web 2.0. Bajo esta lógica todas las cosas que queremos publicar, difundir y las conversaciones que queremos tener, pasan y se alojan permanentemente en las atractivas infraestructura de servicios de terceros como son Twitter y Facebook.

Asimismo, una gran parte de la infraestructura sobre la que se sostiene Internet (el tendido de primera milla, los cables interoceánicos, por ejemplo) está en manos de un número cada vez más reducido de corporaciones. La participación de los estados es acotada y en muchos casos, se ve influenciada por el lobby que hacen estas empresas. Si la infraestructura de la que depende la red está en manos de un oligopolio, no puede ser neutra ni mucho menos ser controlada por sus usuarias.

Entonces, para nosotras la "red de redes" nunca fue neutra, sino que es política, jerárquica y centralizada.



Qué se hizo y qué hacemos

Aunque la red nunca fue neutra, siempre tuvimos formas de contrarrestar las políticas jerarquizantes de la red y aun cuando estas estrategias han sido sostenidas por aquellas personas con conocimientos técnicos, vemos que aparecen cada vez más proyectos que tienden a habilitar la publicación libre y distribuida antes que centralizada.

De forma artesanal, podíamos configurar nuestros routers domésticos para que permitan conexiones entrantes y lentamente ir configurando una computadora reciclada para que tenga nuestro sitio web personal.

Hace unos años se sumaron proyectos como Freedombox y similares, que permitían que la instalación y configuración de ese servidor doméstico no quedara solo en manos de las que tenían más tiempo para cacharrear.

De la desobediencia tecnológica a las redes libres

Pero todos estos proyectos se montan sobre la infraestructura física de Internet, donde ya vimos que los cables pertenecen a pocos conglomerados y, particularmente en el caso de América Latina, están armados de forma que todo nuestro tráfico global pasa necesariamente por EE.UU.

A la par, podíamos compartir archivos a través de redes P2P como Torrent (tan perseguida por las discográficas y cinematográficas y que todavía vive, más o menos invicta), a la que se fueron sumando proyectos que adaptan esos protocolos para que la publicación pueda ser dinámica e incensurable. Dentro de esos proyectos podemos mencionar a Zeronet, IPFS (utilizada por las piratas catalanas para difundir la convocatoria al referendun de la independencia), DAT, etc.



Las redes libres y comunitarias son proyectos colectivos que surgen de la necesidad local de tener acceso a Internet (y/o del desafío técnico y político de tener una red propia) en aquellas zonas donde no hay un interés comercial. Así surgieron proyectos como guifi.net en Catalunya, Delta y Quintana Libres en Argentina y la red de telefonía celular comunitaria de Oaxaca, México, como experiencias de redes inalámbricas con acceso comunitario a Internet y a las comunicaciones.

Estas redes son gestionadas por sus comunidades, que toman las decisiones en relación a la infraestructura de red porque es construida por ellas mismas. Estas son las redes que queremos, más que neutras: libres y comunitarias.

¿Por qué montar Servidores?

No cabe duda del intercambio y retroalimentación que ha existido entre el movimiento de los medios libres, alternativos o comunitarios y las distintas propuestas de servicios autónomos en línea.

De esta relación han surgido un sin número de experiencias, muchas de las cuales siguen en funcionamiento y brindando un soporte a las distintas comunidades en lucha que requieren herramientas de comunicación digitales. Nos referimos a experiencias como Riseup, Nodo50, Sindominio, Espora, Código Sur, Saravá, Mazorca y otros.

Desde el Laboratorio Popular de Medios Libres, acompañadas por distintas colectivas hermanas de medios libres, hemos podido tejer una red de intercambio de contenidos entre comunicadordxs libres de todo el continente, una coordinación a nivel latinoamericano que ya ha generado varios encuentros internacionales, coberturas conjuntas y campañas coordinadas de difusión de contenidos. A partir de este articular con otros medios libres del continente, también se ha difundido y multiplicado el uso del servidor libre Icecast de Espora.org.



El servicio de streaming que pone a disposición Espora ha sido un pilar sobre el cual hemos tejido esta red latinoamericana, ya que una de las necesidades básicas de muchos radios libres es contar con un servicio de streaming costeable y estable. En esta red hemos promovido constantemente el servicio de Espora por sobre otros comúnmente usados, como Tuneln, Listen2myradio, Giss.tv y otros. Actualmente más de 20 colectivos utilizan diariamente el servicio Icecast de Espora con resultados óptimos. Después de casi cuatro años de uso ininterrumpido, creemos importante fortalecer (y agradecer) el trabajo, tiempo y corazón que Espora ha dedicado al proyecto.

La política inicial de Internet y que buscamos honrar con el proyecto **Servidores Autónomos Replicables**, se basó en los principios de apertura, flexibilidad y distribución. Abierta significa que puede dar conectividad a toda clase de dispositivos. Eso fue lo que permitió que, a finales de los noventa, hubiera el estallido de conexiones con los PC, y es lo que permite ahora conectar a los teléfonos móviles. Flexible significa que puede aceptar nuevos desarrollos — incluso los ahora inimaginables.

Y distribuida significa que la inteligencia está por todas partes, incluyendo la periferia, los extremos o los eslabones marginales. En este contexto, por inteligencia debe entenderse la capacidad procesar y almacenar datos. Es por eso que potencialmente cualquiera tiene a su alcance la capacidad de montar un servidor autónomo y proveer servicios de Internet.

La verdadera forma de fortalecer a Espora.org es replicando y multiplicando copiosamente experiencias similares. Construir una arquitectura libre y descentralizada de internet es un desafío grande, pero que debemos afrontar a la brevedad.

S E R V I D O R E S
A U T Ó N O M O S
R E P L I C A B L E S

La desaparición de la neutralidad de la red y otras modificaciones que se discuten en los parlamentos europeos y americanos, son una señal clara del esfuerzo corporativo de empresas y gobiernos por modificar el ADN original de la Red para imponer su modelo centralizado de negocios y sociedad (con las lógicas pérdidas de libertad y privacidad que ello conlleva).

En el contexto actual, toda organización que resiste al capitalismo debería contar con un servidor autónomo, porque es una herramienta con diversos usos que nos libera de la dependencia de las grandes corporaciones y en gran medida de la vigilancia de gobiernos. Como medios de comunicación libres, y ante la oleada de persecuciones y asesinatos que hemos sufrido los últimos años en latinoamérica, tener un servidor propio no solo nos brinda las capacidades de proveer servicios digitales de comunicación, sino que también nos entrega el control de los datos que fluyen a través de estos servicios.

La descentralización es la clave, frente a la centralización que promueve la infraestructura corporativa (y que hace posible la minería de datos, vigilancia masiva, etc), pero que también involuntariamente replican los servidores autónomos, por ej. Riseup concentra una gran cantidad de cuentas de correo de activistas a nivel mundial, lo cual lo puede convertir en un blanco muy apetecido para los órganos de vigilancia. La mejor forma de evadir la vigilancia e incrementar la seguridad de nuestros datos, es multiplicando los lugares donde estos se alojan, y dando a cada organización el control total sobre éstos.

La arquitectura de la Internet también es una instancia política y por ello nos planteamos el desafío de no solo poner en funcionamiento un servidor autónomo que provea servicios digitales de comunicación (por ej. Pad, Icecast, Libretime), sino que también esta experiencia quede sistematizada de forma que cualquier media-activista pueda levantar un servidor autónomo, sin necesidad de contar con conocimientos previos al respecto.



Creemos que las herramientas que existen en la actualidad nos permiten plantearnos este objetivo sin temor y con la seguridad de contar con el apoyo de quienes ya han caminado este sendero antes.

Este llamado está especialmente dirigido a lxs activistas de medios libres y esperamos posicionarla justamente a través de las redes internas de comunicación entre estas organizaciones, para construir una nuestra autonomía tecnológica.

<https://sar.laboratoriodemedios.org/>

Laboratorio Popular de Medios Libres Octubre 2020





Mamá, ¿Por qué hay una pequeña nube en casa?

Ayudando a la niñas a entender el tecnocapitalismo

¿Sabes lo qué es la nube?

Es donde viven los datos.
Pero no viven en los ordenadores
de tus amigos sino que viven
en empresas del **Tecnocapitalismo**.

Para vivir allí necesitan consumir
mucha energía que provoca más
Cambio Climático.

Necesitan beber mucha agua
para refrigerarse lo que provoca
más **Sequía**.

La **oficina** es un lugar **aburrido** en el que la gente grande van a
hacer cosas **aburridas**.

La gente grande iban a la oficina porque los servidores estaban allí.



La gente grande siguen yendo a la oficina a teletrabajar
porque sus jefes les obligan.



La oficina es donde la gente grande se enfada y dice palabrotas.
La oficina es donde los jefes explotan a las trabajadoras, extraen su plusvalía y les obligan a tareas alienantes.

Trabajos de caca.



Para **teletrabajar** no es necesario usar la nube del tecnocapitalismo.

Pero ... ¿sabías que algunos servidores no son aburridos?

Podrían beber menos agua y consumir menos energía.

Podrían no vivir en Macrogranjas de Datos y venirse a vivir a tu casa.



Te voy a contar lo que pasó en mi casa



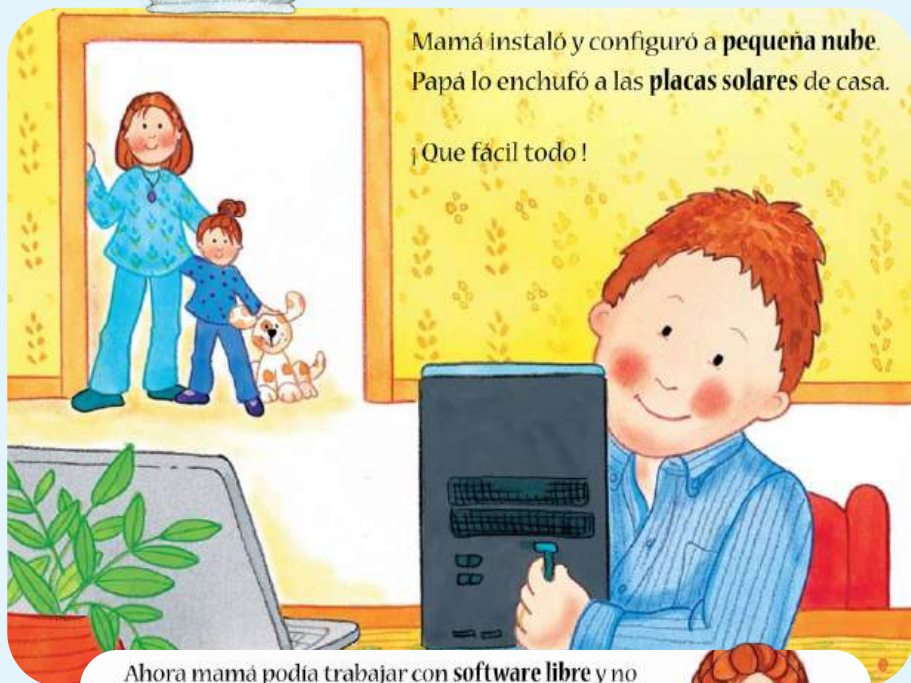
Una noche oí a papá y mamá primero **llorar**, después decir **palabrotas** y finalmente **reír**.

Al día siguiente me dijeron que dejaban sus trabajos, montaban una cooperativa con sus amigos y que **una pequeña nube se venía a vivir a casa**.



La nube era una cajita negra que **parpadeaba**

Dentro vivía **INTERNET**

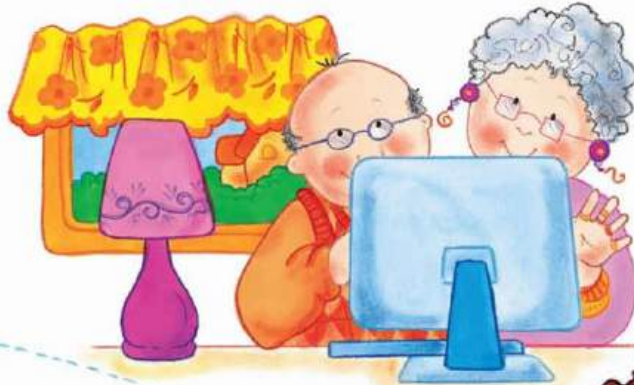


Mamá instaló y configuró a **pequeña nube**.
Papá lo enchufó a las **placas solares** de casa.
¡Que fácil todo!

Ahora mamá podía trabajar con **software libre** y no
con el software privativo que le obligaban a usar
en la aburrida oficina.



Podíamos compartir fotos
manteniendo la **privacidad**.



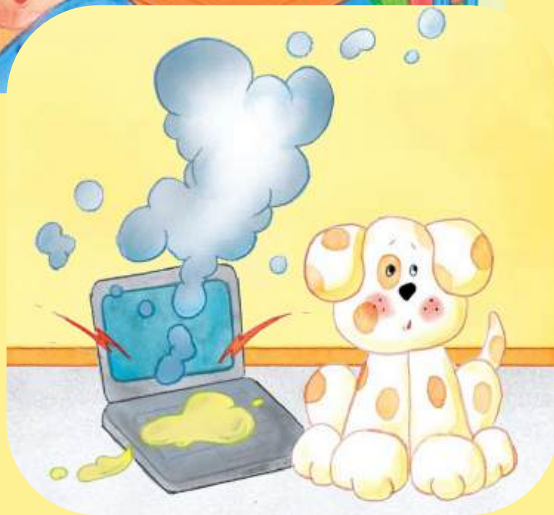
Mantenían también la privacidad de los clientes y hacían **asambleas** con la otra gente grande de la **cooperativa**.



Gracias a esta nube podía **jugar a Doom** desde el cole, charlar con mis compas del **Fediverso** y con XMPP preparar acciones contra Burger King, Campos de Golf y Jets privados.



Y aunque mi perro Kropotkin se haga pipí encima del ordenador los **datos siguen cifrados** y guardados en pequeña nube.





Sabes que con pequeña nube
mantienes tu soberanía, aprendes
a trastear e imaginar
otra Internet posible.

¡Viva la soberanía digital!

Pero ... No todo el mundo piensa así.

A algunos niños de clase les gusta presumir de sus ordenadores manzana,
de su software que no es suyo y de tener sus datos en **las nubes de otros**.



Esos niños se ríen de tu pequeña nube.
dicen que eres una friki.



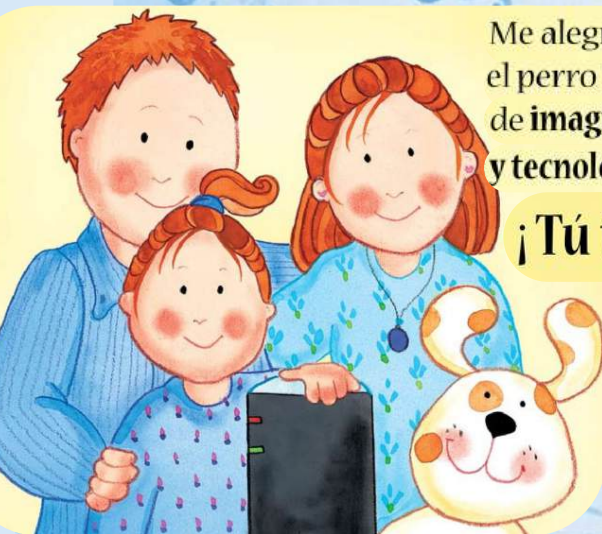
¡Porque ellos están celosos!

Están atrapados en la Internet de caca
que el tecnocapitalismo ha impuesto.
Ya no son capaces de imaginar algo mejor.

Con nubes propias, software libre, redes
descentralizadas y tecnología que
no haga daño al planeta.

Los niños envidiosos observan las luces de tu pequeña nube
funcionando mientras palpan sus barrotes.

Las luces hacen: **¡Poporipó-poporipó!**



Me alegro de que Papá, Mamá y
el perro Kropotkin sean capaces
de **imaginar otros mundos**
y tecnologías posibles.

¡Tú también puedes!

ARCHIVO

ÍNDICE

- Guía Rápida para la Preservación Digital de Videos
- Componentes principales del archivo
- Herramienta de catalogación: Tainacan
- Niveles de preservación digital
- Archivos comunitarios
- Flujo de trabajo 1 y 2



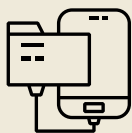
**WITNESS****MIRALO****GRÁBALO****CÁMBIALO**

GUÍA RÁPIDA PARA LA PRESERVACIÓN DIGITAL DE VIDEOS

La preservación digital engloba una serie de acciones continuas para cuidar la documentación valiosa y para asegurar que sea accesible a lo largo del tiempo, incluyendo la recolección, organización, catalogación, almacenamiento, mantenimiento y preservación a largo plazo. La preservación digital permite proteger contra la pérdida de archivos, contra la manipulación y permite a las personas usuarias autorizadas encontrar videos y fotografías auténticos.

ETAPAS CLAVE

La preservación digital puede dividirse en las siguientes etapas clave. A medida que desarrolles tus flujos de trabajo de archivo, documenta tus decisiones y los pasos para que puedas seguirlos de forma coherente mientras creas tu colección.



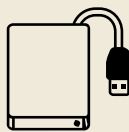
**Crea y
Transfiere**



**Recopila y
Organiza**



Cataloga



Almacena



**Preserva a
Largo Plazo**

CREA Y TRANSFIERE

Cuando captures videos y fotografías, considera qué información adicional vas a necesitar para su preservación y usos futuros. Verifica, por ejemplo, los requisitos para su uso y conservación como evidencia, como la captura de metadatos. Los metadatos pueden entenderse como datos sobre datos: información creada automáticamente por las cámaras y que puede también ser agregada manualmente a los archivos.



**Los metadatos importantes que hay que capturar o crear son:**

- ☐ La fuente del video o la fotografía (el "quién", el "dónde" y el "cuándo").
- ☐ La descripción del evento grabado (el "qué").
- ☐ Las restricciones necesarias requeridas por motivos de seguridad y privacidad.
- ☐ La cadena de custodia (por ejemplo, la cronología de quien ha manejado el video, empezando por quien lo creó).

Tips adicionales:

- ☐ Al compartir o descargar, transfiere los archivos completamente y sin cambios ni compresión adicional.
- ☐ Al crear videos editados, exporta una copia de alta resolución para su preservación, aunque sólo necesites utilizar versiones de menor resolución.

MEJORA LA EVIDENCIA DE LA AUTENTICIDAD

Puede ser útil demostrar que tus archivos están intactos y sin alterar, sobre todo si utilizas el video con fines probatorios. Los hash son secuencias de letras y números que se generan al ejecutar determinados algoritmos en el archivo. Los valores hash son únicos para cada archivo, por lo que los hashes coincidentes indican que los archivos son copias exactas, mientras que los hashes no coincidentes indican que los archivos no son copias exactas. También puedes comprobar si un archivo ha cambiado ejecutando y realizando un seguimiento de sus hashes a lo largo del tiempo. Los algoritmos hash más comunes para verificar la integridad de los archivos son SHA-1 y MD5.

 unknown.mp4	
 VID_20220301_230609880.mp4	
44f8621efd08b43865f49c6aa986c40d209d0c2a	unknown.mp4
44f8621efd08b43865f49c6aa986c40d209d0c2a	VID_20220301_230609880.mp4

Los hashes SHA-1 de unknown.mp4 y VID_20220301_230609880.mp4 coinciden, por lo que son copias exactas del mismo video.





MINI GUÍA ARCHIVAR: PRESERVAR TU DOCUMENTACIÓN

webrec.m4v
webrec(1).m4v

```
dbfee0bbc69a5194ce65ccaafe828123ccac65ac  webrec.m4v  
44f8621efd08b43865f49c6aa986c40d209d0c2a  webrec(1).m4v
```

Los hashes SHA-1 de webrec.m4v y webrec(1).m4v no coinciden, por lo que no son copias exactas.

Tips sobre los hash:

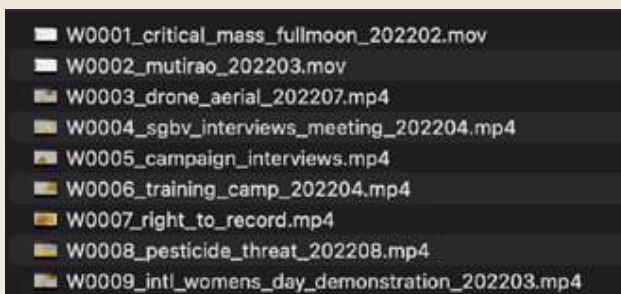
- ☐ Genera y registra los hashes lo antes posible en el ciclo de vida del video/foto, por ejemplo, cuando captures o descargues el video/foto de tu cámara por primera vez. Utiliza aplicaciones de documentación especializadas u otras herramientas de hash (consulta "Herramientas gratuitas y/o de código abierto").
- ☐ Comprueba los hashes periódicamente como parte del mantenimiento de la colección, y siempre que necesites demostrar la integridad de tus archivos.

RECOPILA Y ORGANIZA

Organizar tu colección implica ordenar tus archivos en una estructura coherente de directorios o carpetas y nombrar claramente esos directorios. Una buena organización es necesaria para mantener la procedencia y el orden original de tus archivos y para asegurar que estos no se pierdan o sobrescriban accidentalmente. Es más fácil encontrar registros en una colección bien organizada.

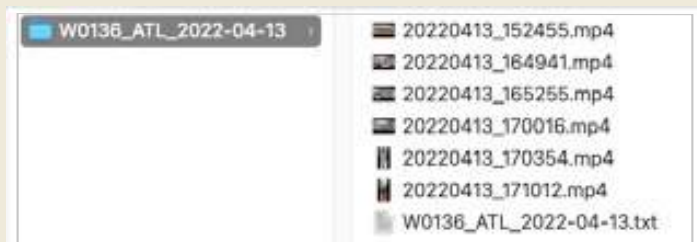
Tips:

- ☐ No cambies los nombres de archivo asignados por la cámara.
- ☐ Nombra los videos editados de forma coherente y mantén tus archivos de proyecto.
- ☐ Crea una plantilla de asignación de nombres y utiliza identificadores únicos que te ayuden a organizar y distinguir tus archivos.

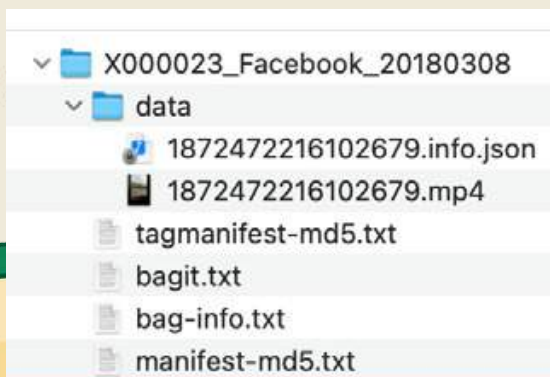


Ejemplo de nombre de un archivo utilizando identificadores únicos.

- ☐ No utilices caracteres especiales tales como @#\$%&*:"' <>?/\`|, acentos o espacios en los nombres de carpetas o archivos.
- ☐ Coloca tu video, o conjunto de videos, en un "paquete de información": un contenedor autodescriptivo — generalmente una carpeta o directorio con un nombre claro y único — que también puede incluir cualquier documentación o metadatos relacionados.



Ejemplo de paquete informativo sencillo que incluye videos y un documento de texto descriptivo.



Ejemplo de un paquete de información más complejo que utiliza el formato estándar BagIt de empaquetado.



- ☐ Cuando organices tus paquetes, mantén intactos su contexto y relaciones originales, como la organización por fecha de creación y/o fuente.



Un paquete organizado en una estructura de directorios basada en la fecha, la ubicación y de la persona que graba.

CATALOGA

Catalogar es importante para crear y organizar información descriptiva de manera estructurada, de modo que los registros puedan encontrarse, utilizarse y comprenderse. Para garantizar el acceso en el futuro, especialmente en el caso de colecciones amplias, contar con algún tipo de catalogación es fundamental. Puedes utilizar una hoja de cálculo para hacer un catálogo sencillo, una base de datos o una herramienta de gestión de medios para un catálogo más complejo.

Tips para Catalogar:

- ☐ Define una estructura de catálogo, que pueda incluir información descriptiva, contextual, técnica, y de derechos; palabras clave; y más información.
- ☐ Crea campos/columnas en la hoja de cálculo o tabla para dividir la información en fragmentos de datos suficientemente granulares que permitan clasificarlos y buscarlos fácilmente (por ejemplo, campos de nombre de archivo, fecha, duración, etcétera, para describir un archivo de video).

Para evitar la redundancia de datos que puede dar lugar a incoherencias, cada

- ☐ hoja de cálculo o tabla sólo debe describir un tipo de entidad (por ejemplo, video). Crea varias hojas de cálculo o tablas si necesitas describir varios tipos de entidades (por ejemplo, videos, eventos, personas). Puedes señalar registros en diferentes tablas utilizando identificadores únicos.





MINI GUÍA ARCHIVAR: PRESERVAR TU DOCUMENTACIÓN

- ☐ Asigna a cada registro/fila de la hoja de cálculo o tabla un identificador único. El uso de identificadores únicos garantiza que cada registro/fila pueda ser correctamente referenciado y distinguido de otros registros/filas, incluso si tienen datos similares.

ID	First Name	Last Name
C001	Luis	Rodríguez
C002	Luis	García
C003	Daniel	Rodríguez

- ☐ Crea una lista de control de términos y definiciones preferidos cuando varios términos puedan describir lo mismo (por ejemplo, "deforestación" y "tala"), o cuando se trabaje en varios idiomas.

- ☐ Especifica el formato preferido para los valores tales como las fechas (por ejemplo, aaaa-mm-dd en lugar de dd-mm-aaaa), y utilízalo de forma coherente.

Date recorded
2022-08-04
8/4/2022
Aug 4, 2022
4-Aug-2022

Diferentes formas de representar las fechas: elige un formato y utilízalo sistemáticamente.

- ☐ Para que los catálogos sean más completos y cohesionados, puedes establecer reglas, como campos de entrada de datos obligatorios, para asegurarte de que se recoge la información crucial.
- ☐ Utiliza el mismo esquema de metadatos en toda tu comunidad o sector puede ayudar a que tus datos sean más interoperables. Por ejemplo, para describir los recursos digitales pueden utilizarse normas ampliamente adoptadas, como Dublin Core (<https://www.dublincore.org>).



ALMACENA

El almacenamiento se refiere a los medios y métodos utilizados para guardar y acceder a tus documentos. Independientemente del tipo de medio o dispositivo que utilices, ninguno durará para siempre. La vida útil real de los medios de almacenamiento o el hardware depende de muchos factores, como su entorno y uso. Las buenas prácticas de almacenamiento incluyen la elección del almacenamiento adecuado, la realización de copias de seguridad (backup) y el monitoreo activo.



Tips:

- ☐ Utiliza la regla 3-2-1: mantén 3 copias de tu colección, en 2 medios/ plataformas de almacenamiento diferentes (como un disco duro portátil y un proveedor de almacenamiento en la nube), con 1 copia geográficamente alejada de las otras.



- ☐ Para las partes de tu almacenamiento que se actualizan con frecuencia, utiliza programas para hacer copias de seguridad (backup) a fin de realizar respaldos incrementales.
- ☐ Controla el acceso físico y electrónico a tu colección para evitar manipulaciones y eliminaciones accidentales o deliberadas; también para proteger la identidad de quienes se encuentran en situaciones de alto riesgo o para respetar la privacidad.



- ☐ Ten en cuenta la capacidad de tu soporte informático, la naturaleza y el tamaño de tu colección y los requisitos de acceso a la hora de elegir los soportes y las configuraciones de almacenamiento. Recuerda que los dispositivos de almacenamiento necesitan mantenimiento.
- ☐ Comprueba la temperatura / humedad relativa de tu entorno de almacenamiento con las recomendaciones para tu dispositivo. La humedad elevada y las fluctuaciones de temperatura suelen ser perjudiciales para los dispositivos. Para el embalaje, utiliza barreras o capas que bloqueen el intercambio de humedad y temperatura, como dos cajas guardadas en un armario en una habitación central, sin paredes exteriores. Empaca los dispositivos en un día seco.



Tips para Almacenar:

- ☐ La tasa de averías de los soportes de almacenamiento aumenta con el tiempo. Considera actualizar/sustituir los soportes y dispositivos de almacenamiento aproximadamente cada 5 años para minimizar el riesgo.
- ☐ Ten cuidado con los virus o programas espía (spyware o software espía) si tus dispositivos de almacenamiento están conectados a una red.
- ☐ Cifrar tus dispositivos o volúmenes de almacenamiento es importante, pero puede ser arriesgado si se pierde la llave de cifrado.
- ☐ Monitorea tu colección periódicamente. Elige un día al año para revisar / limpiar tus archivos, como un aniversario o una fecha importante como el Día de la Tierra (22 de abril) o el Día Mundial del Patrimonio Audiovisual (27 de octubre).





PRESERVA A LARGO PLAZO

La preservación a largo plazo requiere de un compromiso de acciones futuras.

Considera:

- ☐ Cambios en la tecnología de grabación o captura que podría requerir de nuevos métodos de recopilación y de manejo de videos y fotografías.
- ☐ Cambios en la tecnología de almacenamiento que afecten la disponibilidad de ciertos medios, dispositivos, cables o conectores; y el costo de los medios o servicios. Esto podría requerir migrar los medios a diferentes tipos de servicios o de medios de almacenamiento.
- ☐ Cambios en las necesidades de las personas usuarias (por ejemplo, los requerimientos probatorios, su habilidad de comprender el contenido, etcétera) lo que podría requerir actualizar tus enfoques en tu colección o de catalogación.
- ☐ La obsolescencia del formato de archivos puede hacer que los formatos en tu colección sean difíciles de abrir, reproducir o usar. Podrías necesitar crear copias de tus videos y fotografías en formatos nuevos y utilizables.
- ☐ Tu habilidad/capacidad de mantener la colección en el tiempo.

MÁS INFORMACIÓN

Para más información sobre archivar y preservar, te recomendamos consultar los siguientes recursos:

- [Guía para Archivistas para Archivar Video \(WITNESS\)](#) wit.to/GuiaArchivo
- [Lista de reproducción en Youtube \(WITNESS\) en inglés sobre Archivos Comunitarios](#) wit.to/4gfOPyK
- [Micro-tesauros \(HURIDOCS\)](#) wit.to/microtesauro-huridocs
- [Planifica la información que necesitas \(HURIDOCS\)](#) wit.to/planifica-info
- [La Caja de Herramientas para Defensorxs de la Tierra \(Digital Democracy\)](#) earthdefenderstoolkit.com/inicio/?lang=es



MÁS INFORMACIÓN

- Sitio web de Herramientas de Tecnología para la Documentación de Derechos Humanos en inglés (Engine Room) documentation-tools.theengineerroom.org
- Guía ¿Debo Recolectar y Archivar estos Videos? en inglés (WITNESS) wit.to/Archiving-Decisions-US

Grabar / Capturar Metadata

Proofmode (Android, iOS)

Tella (Android, iOS)

Hashing

Hash Droid (Android)

MD5 (incluido en Mac)

QuickHash (Linux, macOS, Windows)

Copiar Archivos/Migración

Robocopy (Windows)

Rsync (Linux, macOS)

Save (Android, iOS)

TeraCopy (macOS, Windows)

Empaquetar

BagIt (especificaciones escritas)

Bagger (Windows, Linux, macOS)

Exactly (macOS, Windows)

DART (Windows, Linux, macOS)

Leer metadatos de

archivos/ Escribir

Exiftool (macOS, Windows)

Medialnfo (Linux, macOS, Windows)

Catalogar / Publicar

Mukurtu (Drupal)

Omeka (Linux u hospedado)

Uwazi (Linux u hospedado)

Tainacan (WordPress)

Reformatear

Audacity (Linux, macOS, Windows)

FFmpeg (Linux, macOS, Windows)

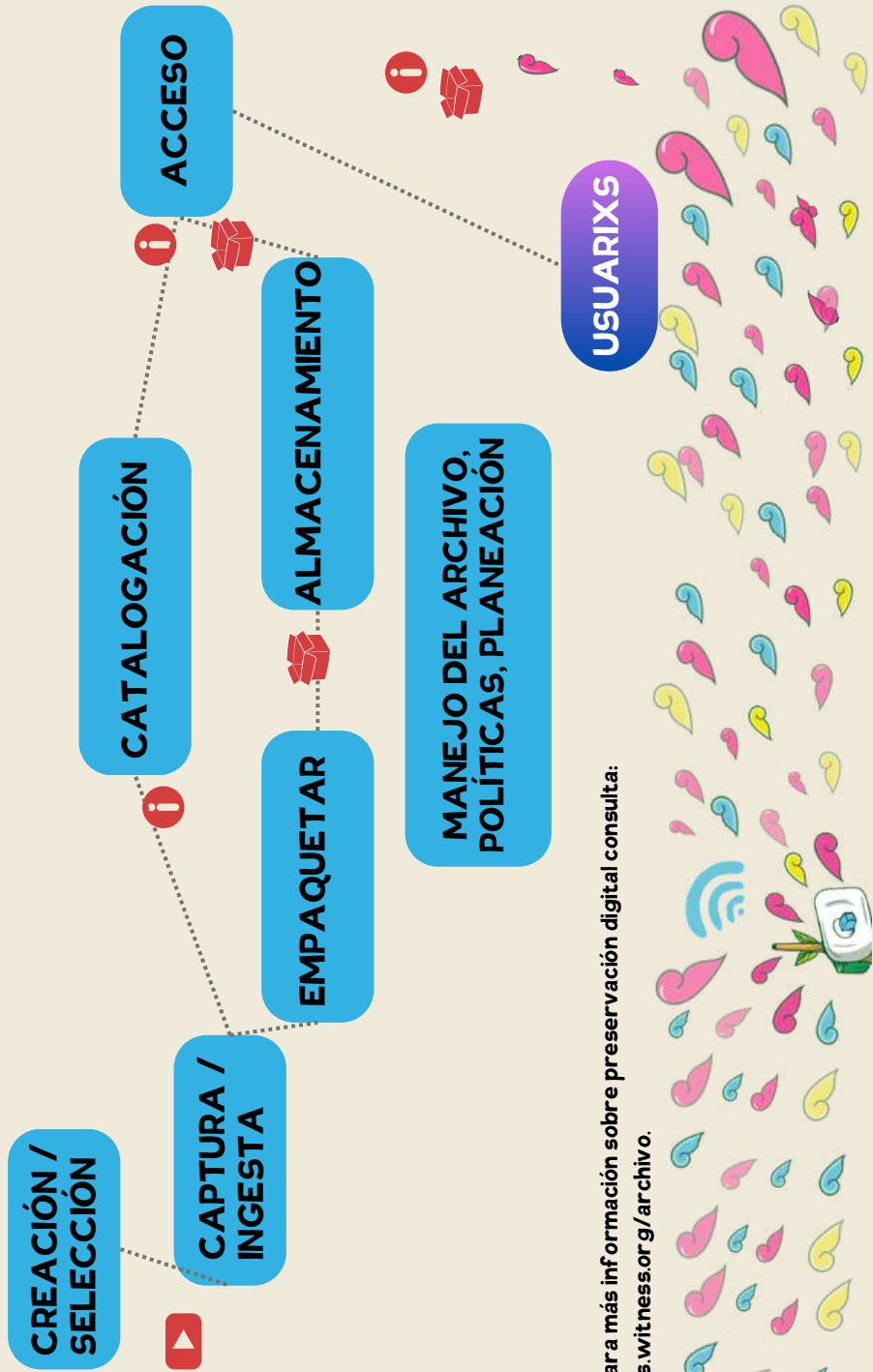
Handbrake (Linux, macOS, Windows)

Descarga la Guía rápida para la preservación digital de video en wit.to/GuiaPreservacionDigital



COMPONENTES PRINCIPALES DEL ARCHIVO

ARCHIVO



Para más información sobre preservación digital consulta:
es.witness.org/archivo

Tainacan

tainacan.org/es

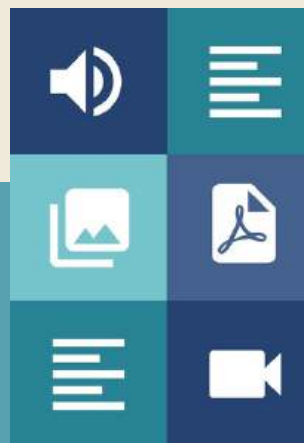
Tainacan es una plataforma gratuita y de código abierto para crear repositorios digitales.

Su instalación es mediante un plugin en WordPress, que se puede usar, copiar, modificar y redistribuir sin restricciones (su código fuente está disponible en GitHub).

La instalación de Tainacan puede ser en servidor local o en línea, y puede tener colecciones privadas; colecciones públicas, con metadatos privados o públicos. La instalación y su documentación completa en Wiki están disponibles en español. El foro en línea proporciona una amplia guía para ayudar con la configuración, donde se puede pedir ayuda o informar errores con soporte multilingüe.

Costos y seguridad | Tainacán no tiene costos de instalación ni de actualización, pero sí depende del alojamiento de WordPress, ya sea a través de un servicio de alojamiento web (costos según proveedores locales) o de una configuración de servidor local (como los Servidores Autónomos Replicables <https://sar.laboratoriodemedios.org/>). Las medidas de seguridad del proveedor de servicios en línea o de la instalación local definirán la seguridad de los datos, a partir de un conjunto mínimo de configuraciones de protección.

Participación y colaboración comunitaria | Una característica muy importante para la participación de la comunidad es el envío externo de elementos, con aprobación posterior antes de publicar. También es posible comentar cada elemento, lo que se puede habilitar para usuarios anónimos o identificados. La configuración para las personas usuarias en Tainacan es similar a los roles y permisos de WordPress. El sistema de registro permite a quienes son moderadores realizar un seguimiento de los cambios.



Tainacan

Customización | Puedes controlar y configurar los metadatos como texto, número, lista de selección, fecha, geolocalización (que permite visualizar elementos en un mapa), URL (para contenido incrustado de plataformas externas) y taxonomía (una lista jerarquizada controlada de términos). La gestión de medios se realiza principalmente a través de WordPress. Hay múltiples formas de personalizar los filtros y la visualización de las colecciones. Es posible conectar elementos de la misma o de diferentes colecciones. Después de configurar el esquema de metadatos, es posible cargar elementos a través de archivos CSV, lo que permite importar bases de datos. Y también podrás descargar tus datos como CSV.

Usabilidad y accesibilidad | La interfaz de Tainacan es muy accesible y fácil de usar, con un panel y funcionalidades sencillas. La instalación consiste en instalar plugins dentro del panel de WordPress y configurar la colección es rápido. Más allá del tema de diseño del Tainacan, otros temas de WordPress como Blocksy funcionan perfectamente con Tainacan, mientras que otros temas (como Elementor) requieren ajustes sencillos de diseño.



Sostenibilidad | Tainacan ha sido desarrollado por universidades brasileñas y, aunque inicialmente estaba destinado a colecciones culturales y museológicas (como Brasileira), muchos proyectos de derechos humanos están adoptando Tainacan. La inversión constante de las universidades hace de Tainacán una herramienta estable y sostenible para la comunidad. A pesar de ser una herramienta construida y consolidada desde 2014, a septiembre de 2024 la última versión publicada es la 0.21.8. Se están haciendo algunas revisiones finales para la versión 1.0.

Pasos para estructurar tu repositorio |

1. Conozca la herramienta antes de comenzar a catalogar para saber cómo formatear sus datos;

2. Diseña el modelo de datos teniendo como referencia metadatos descriptivos, administrativos, técnicos, estructural y de preservación. Para ayudar con este proceso, elige cerca de cinco registros de cada tipo de documento (como video, foto, audio, texto, etc.), para saber qué necesitas para cada;

3. Creas taxonomías jerarquizadas y diccionario de datos;

4. Si la catalogación se hará de forma colectiva, crea una página para el envío de elementos para posterior evaluación y publicación – con reglas para cada campo;

5. Sé minucioso en la recopilación de datos y en la descripción del contenido, maneja la información sin distorsión por sesgos, prejuicios o interpretaciones personales.



NIVELES DE PRESERVACIÓN DIGITAL



NIVEL 1

Algunos videos se guardan en dispositivos de individuos, pero no deliberada o sistemáticamente.

Se toma la decisión consciente de recopilar videos. Hay cierta claridad sobre lo que se recopilará y quién es responsable de hacerlo.

La recolección se realiza regularmente y con cierta consistencia. Las pautas sobre lo que se debe recopilar se redactan y revisan en el proceso.

Pautas documentadas y detalladas sobre lo que se debe recolectar y lo que no. Se cuenta con flujos de trabajo paso a paso para que la recolección se haga consistentemente.

COLECCIÓN

CATALOGACIÓN

No se realiza una catalogación, aunque se puede haber guardado alguna documentación con videos por casualidad.

Se recopila y guarda algunos metadatos que describen los videos (por ejemplo, en un formulario, en un correo electrónico), pero no necesariamente compilados de forma centralizada o estructurada.

Un documento de catalogación simple, centralizado y estructurado, como una hoja de cálculo, se configura y se usa para describir y rastrear videos. Las reglas/expectativas para la recopilación de metadatos y la entrada de datos se redactan y revisan en el proceso.

Se implementan estructuras de datos más complejas utilizando herramientas de bases de datos. Las reglas de catalogación se documentan en un diccionario de datos y con vocabularios controlados.



NIVEL 1

NIVEL 2

NIVEL 3

NIVEL 4

ALMACENAMIENTO

Los videos son almacenados por individuos en sus propios dispositivos. Se desconoce quién tiene qué.

Los videos se descargan en su mayoría desde dispositivos de individuos al almacenamiento centralizado y compartido, pero no están organizados sistemáticamente. No hay método estándar para nombrar archivos.

Los videos almacenados están bien organizados (por ejemplo, en directorios claramente nombrados) y se hace referencia al catálogo, por lo que son fáciles de identificar y recuperar.

El almacenamiento se monitorea y se respalda regularmente.

PRESERVACIÓN A LARGO PLAZO

Algunos videos pueden mantenerse, pero no hay decisión deliberada sobre qué preservar y qué no.

Se busca asegurar que se guarde el contenido y los metadatos, con menos preocupación por la disponibilidad y accesibilidad a largo plazo. El foco está en archivar videos recién recopilados, y hay menos capacidad para tratar con videos antiguos que pueden haber sido guardados por casualidad en el pasado.

El contenido y los metadatos se guardan con más intención hacia un uso a largo plazo, aunque no se toman acciones de preservación específicas. Se presta atención a revisar los videos más antiguos, evaluando lo que es valioso preservar e incorporar al archivo hacia el futuro.

Se establecen pasos proactivos para garantizar la preservación: el reemplazo de hardware, planes de recuperación ante desastres, colaboraciones con otras organizaciones. Los videos más antiguos se incorporan a la colección de archivo, incluidos pasos como la digitalización, si es necesario.

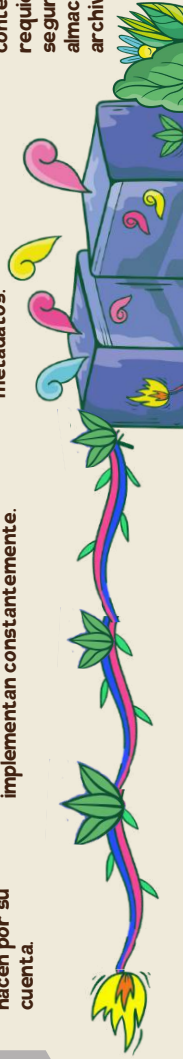
SEGURIDAD Y CONTROL INTERNO

No hay medidas de control o seguridad salvo lo que las personas hacen por su cuenta.

Se establece cierto control sobre dónde se mantienen los videos y quién deberían tener acceso, pero las contraseñas y el cifrado seguro no se implementan constantemente.

Las contraseñas seguras se utilizan en todos los dispositivos y plataformas desde donde se acceden y almacenan contenidos y metadatos.

Cuentas e inicios de sesión individuales, que permiten potencialmente diferentes niveles de acceso, en dispositivos o plataformas donde se accede y almacena contenido y metadatos. Identificación y delineación de contenido o metadatos que requieren un manejo más seguro. Cifrado en almacenamiento de dispositivos o archivos, si se requiere.



ACCESO
Y USO ÉTICO

NIVEL 1

No hay protocolos para compartir videos. Valoración limitada de cómo se podría usar el contenido o cómo restringir su uso.

NIVEL 2

Acceso restringido ampliamente, pero no hay protocolos para permitir diferentes niveles de acceso o restricción de contenido específico. Se responde a consultas, pero la identificación, búsqueda y recuperación de los materiales se realizan ad hoc. Alcance limitado o inactivo para compartir públicamente.

NIVEL 3

El contenido específico se puede marcar con diferentes restricciones o niveles de acceso (por ejemplo, consentimiento seguro/ necesario, rostros eliminados, advertencia de contenido gráfico necesario, etc.) Mayor capacidad de responder sistemáticamente a las consultas. Compromiso proactivo en oportunidades para compartir y usar contenido.

NIVEL 4

Protocolos claramente documentados sobre el contenido que debe ser marcado, redactado, eliminado y/o compartido. Flujos de trabajo claros para revisar y redactar contenido. Uso/ préstamo estratégico de contenido para apoyar casos legales y campañas. Capacidad para agregar y analizar datos para compartir /usar.

Fuente: Levels of Digital Preservation, National Digital Stewardship Alliance.





RECURSOS Y PRESUPUESTO

NIVEL 1	Recursos existentes y sin presupuesto asignado.	Los recursos, personas y equipos disponibles son los existentes, es decir, no se cuenta con presupuesto dedicado/específico para equipos o mano de obra.	Presupuesto sostenible, roles dedicados, equipo. Planes de sostenibilidad, incluida el reclutamiento y la capacitación de nuevos voluntarios.
NIVEL 2			
NIVEL 3			
NIVEL 4			

Fuente: Levels of Digital Preservation, National Digital Stewardship Alliance.





ARCHIVOS COMUNITARIOS

¿Qué son los archivos comunitarios?

Los archivos comunitarios son creados con el propósito de recopilar y proveer acceso a la historia de una comunidad. Es a través de la participación colectiva que estos archivos funcionan para preservar las narrativas de grupos que han sido desplazados del registro histórico.

A diferencia de los archivos tradicionales, los miembros de la comunidad participan en cada paso de la creación del archivo definiendo el enfoque del mismo, describiendo el material y proveyendo acceso a este. Al ser experimentales y radicales en su modalidad, los archivos comunitarios poseen el potencial de ser espacios de resistencia y promover la movilización de nuestras comunidades. Esto sucede al preservar y colaborar con nuestras comunidades para documentar nuestras historias y relatos. Nuestras comunidades son las titulares del conocimiento.



1

DEFINA LA MISIÓN Y LOS OBJETIVOS DE SU ARCHIVO

- ¿Qué historias quiere preservar y/o amplificar?
- Decida qué tipo de formatos quiere y puede conservar
 - Ej. fotografías, película, papeles
- Defina el periodo de tiempo, la temática y el enfoque geográfico de su archivo comunitario.
- ¿A quién quiere contar estas historias? ¿Por qué debe ser USTED quien está haciendo este proyecto? ¿Cuál es su relación a esta comunidad?
- Establezca los recursos que cada objetivo de su proyecto necesitará como colaboradores, acceso a sitios, equipo, etc.
- Defina su presupuesto



¿Qué son los archivos comunitario?

ARCHIVOS COMUNITARIOS

2 DECIDA CÓMO ORGANIZARÁ SUS COLECCIONES

Es importante que mantenga un registro de todos los materiales que añade a su archivo. Una forma de hacer esto es organizar sus materiales en categorías y sub-categorías desde lo amplio a lo específico.

Para archivos digitales, desarrolle un sistema de codificación que le ayude fácilmente guardar, localizar, identificar y recuperar cualquier material. Por ejemplo: 2019Julio_mi-pelicula.mov

3 DECIDA CÓMO VA A CONSERVAR SU ARCHIVO

Antes que empiece a recolectar material, es importante saber cómo va preservar los materiales en su archivo (al dorso encontrará más información acerca de como preservar su archivo). Si tiene material digital, asegúrese en hacer copias. Por ejemplo, tenga una copia en su computadora, otra copia en un disco duro externo y otro en la nube o servidor

4 COMIENCE A RECOPIAR SU ARCHIVO

TOME EN CONSIDERACIÓN...

- Sea transparente, comparta los objetivos y detalles de su proyecto con su comunidad (si recibe una subvención, cómo se maneja el archivo, etc).
- Descentralice la información. No imite las mismas estructuras que han marginado a su comunidad.
- Asegúrese en lo posible de obtener el permiso de utilizar los materiales de sus contribuidores.





Acceda a bit.ly/CommunityArchives para obtener más recursos e información acerca de archivos comunitarios.

- Asegúrese de dejar a la gente saber si planea en hacer su archivo disponible por internet. Sí será accesible virtualmente, añada un aviso en su sitio web sobre la remoción o desactivación de contenido que sea delicado, perjudicial, o que vaya en contra de los derechos de autor.
- Incorpore un consejo comunitario para establecer colectivamente objetivos, prioridades del archivo. Al incluir más personas en la conversación, se asegura la longevidad del archivo.
- Las transiciones en la administración ocurren y por lo tanto es importante mantener un registro de su inventario y de sistemas y procesos utilizados en gestionar el archivo en caso que necesite entregar el archivo a otra persona.
- ¿Cómo protegerá la privacidad de sus contribuidores? ¿Pondrá restricciones de acceso al archivo?

CÓMO PRESERVAR SU ARCHIVO

PAPEL

- Utilice cajas y carpetas libres de ácido
- Quite todo tipo de clips o grapas. No doblar laminar ni usar ningún tipo de adhesivo.
- Lave sus manos antes manejar originales
- Almacene lejos de la luz, humedad y altas

VIDEO (VHS, MINI DV, HI8)

- No tocar la cinta.
- Almacene sus videos con la cinta rebobinada y de forma vertical en un estante.
- Evite que sean expuestos a campos magnéticos como electrodomésticos
- Etiquete sus videos con información relevante.
- Considere digitalizar sus colección

FOTOGRAFÍAS

- Utilice guantes de algodón al manejar fotografías o sus negativos
- Proteja sus fotos y negativos de la luz
- Almacenar en cajas o sobres libres de ácido, lejos de luz y en temperaturas bajas
- Evitar álbumes de foto con plástico PVC o aditivos
- Evitar el adhesivo ya que atrae insectos

SOPORTE FÍLMICO (PELÍCULA)

- Maneje la cinta por los bordes evitando tocar la imagen.
- Utilice guantes de algodón si necesita limpiar o inspeccionar la cinta
- Almacene en cajas de cartón o contenedores de plástico o metal en un ambiente con baja humedad, luz baja y con una temperatura consistente. No utilice bolsas plásticas.

Fuente: <https://archivistasenespanglish.org/wp-content/uploads/2020/01/archivoscomunitarios.pdf>

MEDIOS DIGITALES

- Transfiera información en formatos obsoletos o casi-obsoletos (ej. disquete o CDs)
- Acceda a sus archivos al igual que su almacén cada seis meses.
- Aplique la regla de 3-2-1: Haga tres copias, utilice dos diferentes tipos de medios para guardar sus copias y guarde una copia en una localización remota. Además, cree copias de acceso.
- Ojo! El promedio de vida de los medios digitales varía:
- DVD/CD's -10 años
- Disco duros, tarjetas de memoria -5-10 años
- Almacenamiento en la nube depende en los términos del servicio de la compañía (!).

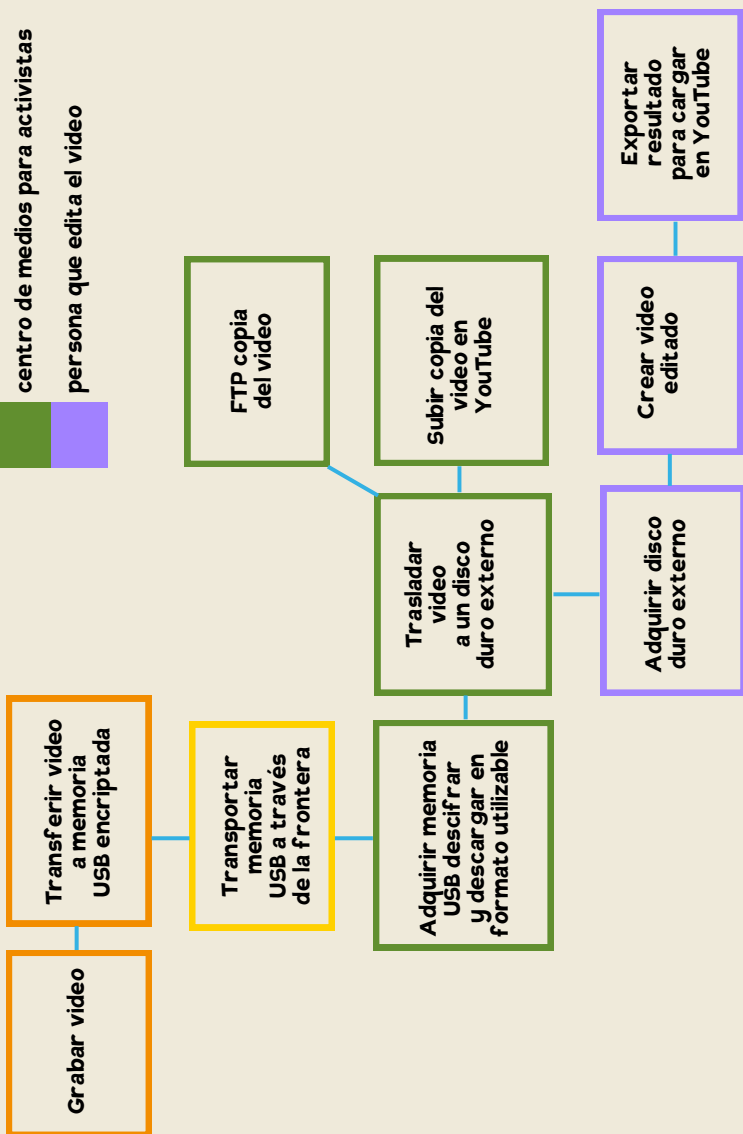
FLUJO DE TRABAJO

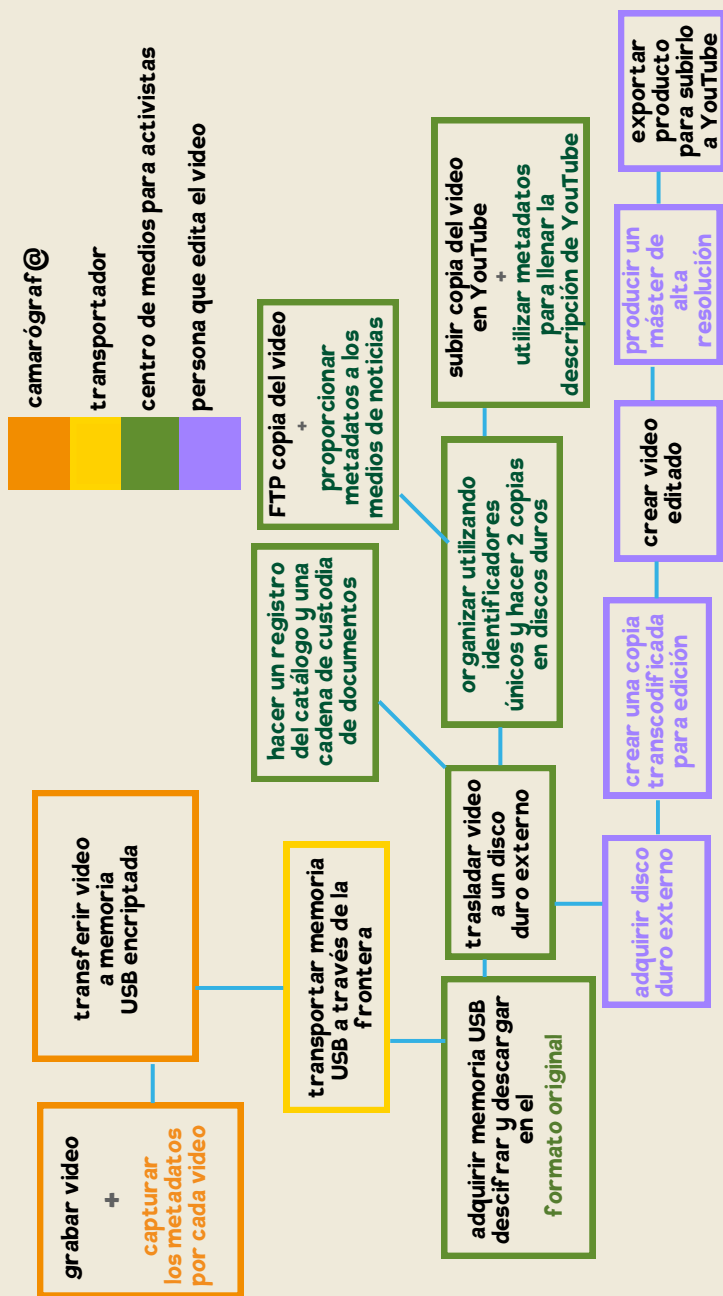
camarógrafo@

transportador

centro de medios para activistas

persona que edita el video





WITNESS | Guía para Activistas para Archivar Video | Creative Commons Atribución-NoComercial-CompartirIgual-Licencia 3.0.



PERFILES ORGANIZACIONES WAYKIS

DOCUMENTACIÓN/ARCHIVO

- **WITNESS** trabaja con colectivos y personas que buscan utilizar videos y tecnología para la defensa y promoción de derechos.
 - Georgia: es parte del equipo de Video como Evidencia.
 - Vito: vive en Brasil y es Director Asociado de Programas.
 - Ines: vive en Brasil y trabaja en el programa de Archivo.
 - Leandro: es el Director de Programas Globales.
 - Laura: vive en México y está a cargo de la dirección del trabajo en América Latina y el Caribe.
 - Ori: vive en Oaxaca, México, es parte del equipo de Witness para America Latina y el Caribe. Tiene experiencia de trabajo con radios y medios comunitarios en la región mesoamericana.
- **Laboratorio Popular de Medios Libres** promueve el software libre, la cultura libre y la comunicación comunitaria en toda América Latina. Buscan ayudar a las comunidades a ser protagonistas de sus historias y defender sus derechos y territorios con tecnología accesible.
 - Armando Gómez Martín. Participa en el Laboratorio Popular de Medios Libres donde promueven la comunicación comunitaria, los medios libres y la autonomía técnica y digital desde las comunidades. Es Capacitador y Comunicador Comunitario, también Activista digital enfocado en seguridad y autonomía informática, pertenece al equipo de SysAdmin de Yanapak.
- **Andrés Tapia** vive en Ecuador, es Coordinador de Incidencia Política de la Coordinadora Latinoamericana de Cine y Comunicación de Pueblos Indígenas CLACPI, periodo 2022-2025; Ex Dirigente de Comunicación de la Confederación de Nacionalidades Indígenas de la Amazonia Ecuatoriana CONFENIAE por dos periodos 2016-2023; Co-fundador y Director de la Radio La Voz de la Confeniae 2019-2023; Co-fundador de la red de comunicadores comunitarios Lanceros Digitales.



PERFILES ORGANIZACIONES WAYKIS

DOCUMENTACIÓN/ARCHIVO



Herramientas digitales de código abierto,
gratuitas, libres de anunciantes y seguras.



PROOFMODE

CONVIERTE TUS FOTOS
Y VIDEOS EN
EVIDENCIA VISUAL
SEGURA Y NOTARIADA

proofmode.org
support@guardianproject.info



- **Guardian Project** es una organización que desarrolla software libre, y gratuito de seguridad digital para equipos móviles.
 - **Fabby**, es Mexicana, vive en Oklahoma, y es la Líder de comunidad de Guardian Project.
- **Cefo**: El Centro de Fortalecimiento de los Derechos Indígenas, también llamado CEFO Indígena, es un programa de carácter colaborativo y sostenido, concebido y desarrollado en 2019 por la Fundación Equitable Origin y la Coordinadora de las Organizaciones Indígenas de la Cuenca Amazónica.

- **Bryan** es cartógrafo, educador popular, y defensor de derechos humanos y del territorio, colaborador del Centro de Fortalecimiento de los Derechos Indígenas (CEFO), coordinador del trabajo de monitoreo territorial en la Península de Yucatán, principalmente con juventudes en Calakmul. Actualmente participa en el proceso jurídico en contra del megaproyecto del Tren no maya.



PERFILES ORGANIZACIONES WAYKIS

SERVIDORES



- **Laboratorio Laboratorio Popular de Medios Libres:** espacio dedicado a la promoción de tecnologías libres y la comunicación comunitaria. Desde 2019 hemos mantenido Yanapak.org como acompañado procesos de internet comunitaria.
 - Nicolás Tapia Correa. Autodidacta en las TICs, participa en el desarrollo de Yanapak.org. También ha colaborado en proyectos de comunicación y derechos humanos.
- **Sutty** que trabaja para ofrecer sitios resilientes y autogestionables para colectivos y activistas con los principios por una Internet popular y diversa comprometida con el Derecho a la Comunicación.
 - elio (él/elle). Vive tanto en Argentina, en el monte, como en el ciberespacio multidimensional. Alguien podría decir que es trans-yogui-jáquer artesanal y comucuidador*. Es parte de la cooperativa (Sutty) (<https://sutty.coop.ar>).
- **NumericaLatina** es una servidora autónoma, basada en software libre, que nació hace casi siete años en el sur-sur del Abyayala, para satisfacer las necesidades digitales de medios de comunicación independientes y de organizaciones sociales, la mayoría de corte anti-autoritario y/o de pueblos originarios. Se financia autogestivamente, gracias al aporte de sus personas usuarias, y por eso con el tiempo ha ido integrando también servicios para empresas, en la lógica del doble proyecto*.
 - Roberto (Beto) fue uno de sus fundadores, cuando volvió a su tierra luego de caminar el continente como artista callejero. En informática, se define como DevOps, es decir, trabaja en la intersección del desarrollo de software y la administración de sistemas. Ha escrito Numérica como una "infraestructura como código", esto es, una metodología de despliegue y mantenimiento automatizado, agnóstica con respecto al hardware subyacente, y migrante de servidor en servidor. Hoy, se dice que vive como ermita en una casa de barro, escondida en algún bosque cordillerano.





PERFILES ORGANIZACIONES WAYKIS SERVIDORES

- **Espora** es un proyecto que apoya con servicios tecnológicos libres para colectivos y organizaciones que trabajan por un cambio social desde abajo y a la izquierda.
 - Pirra: radica en Jobel, Chiapas, al sureste de México y desarrolla infraestructuras con software libre y enfocadas en la privacidad informática. Forma parte del servidor autónomo Espora.org.
- **CAD** investiga, mejora y crea herramientas y técnicas fáciles de usar que fortalecen la soberanía digital de las personas.





PERFILES PARTICIPANTES

AMIKIUR

- **Javiera** es reportera, redactora y vive en Wallmapu. **Paulina** es encargada de equipos y programas para la producción de material audiovisual. Ambas comunicadoras son parte de Radio Kvruruf un medio comunitario, libre y autónomo que apoya en la cobertura y difusión de hechos asociados a la defensa del territorio y la búsqueda del buen vivir en Ngülumapu, territorio ancestral Mapuche donde hoy se ubica Chile.
- Soy **Tara** de Medio Libre la Zarzamora, medio anarcofeminista en el que me desarrollo como comunicadore radial, editora/e y escritora/e de nuestro periodico impreso y online. En el territorio de Ainil leufu me desenvuelvo también como reportera/a por lo que también hago registros audiovisuales y fotograficos en terreno. Además me he desenvuelto en la vida como educadora popular en diferentes territorios, con infancias, mujeres y diversidades sexuales y de género, desarrollando las artes, memoria y la autodefensa olistica de los cuerpos y territorios entre otras temáticas comunitarias.
- **Fundeps:** La Fundación para el Desarrollo de Políticas Sustentables es una organización sin fines de lucro de la provincia de Córdoba que se dedica a la promoción de políticas públicas con garantía de derechos humanos, a través del trabajo en investigación, incidencia en política, litigio estratégico, fortalecimiento de capacidades, campañas de concientización y trabajo en red.
 - **Eliana**, es comunicadora social y se desempeña como Vicedirectora de Fundeps. **Ananda**, es abogada y se desempeña como Encargada de Proyectos del Área de Ambiente de Fundeps. Ambas viven en la provincia de Córdoba, Argentina.

PERFILES PARTICIPANTES

AMIKIUR

- **La Otra Cooperativa** está comprometida a fortalecer las luchas populares, que transformen las estructuras de discriminación, opresión y exclusión, mediante la educación, investigación y comunicación alternativa y comunitaria.
 - Mirian se dedica principalmente all área de documentación visual, audio y audiovisual, Fernanda está a cargo de documentación y es parte del equipo de diseño gráfico, las dos viven en Petén, Guatemala y forman parte de la organización La OTRA Cooperativa.
- **Bolivia:** Nayra Bautista, pertenece al área de comunicación y redes sociales, Yawar Choque pertenece al área de informática y documentación, ambos pertenecemos al país de Bolivia. Y somos miembros de la Asociación de Pueblos Indígenas Originarios Campesinos Qhana Pukara Kurmi, la cual se desempeña en el acompañamiento, defensa y promoción de los derechos humanos de los pueblos indígenas
- **Colombia:** Nilson Huetia, un apasionado estudiante de comunicación en el programa "Vientos de Comunicación" de la organización indígena CRIHU, se desempeña en el ámbito técnico de la red comunitaria "Red Nasa Piçkwe ikh". **Fraidy Castro, parte del grupo de comunicación de la misma red, ha fortalecido su labor con sus conocimientos, trabajando junto a otros jóvenes en la búsqueda de herramientas y tecnologías innovadoras para proteger y empoderar a su comunidad. ¡Juntos están construyendo un futuro más conectado y seguro!





PERFILES PARTICIPANTES

AMIKIUR

- Lluvia Comunicación es un colectivo intercultural que habita el centro-sur de la Amazonía de Ecuador, acompañando desde el año 2003 la protección de los territorios indígenas de las culturas Shuar/Achuar, los derechos colectivos y derechos de la naturaleza, a través de la comunicación comunitaria y la capacitación-acción.
- CPO: un movimiento socio-político que articula a diferentes comunidades del Pueblo Maya y mestizo que luchan por derechos fundamentales y por la construcción del Estado Plurinacional para el Buen Vivir de los Pueblos.
- Centro de Derechos Humanos Tepeyac: acompaña procesos organizativos con las comunidades de la región Istmo de Tehuantepec, en el Estado de Oaxaca en pro de los derechos humanos, procurando una vida digna para todas y todos.
- Radio Padiuxi: se fundó en 2014. Esta radio comunitaria transmite por el 98.9 de frecuencia modulada. En su programación retoman las voces de los jóvenes, las mujeres, los ancianos de la comunidad e integrantes de regidurías del municipio. Las instalaciones están ubicadas en la sede del Comisariado de Bienes Comunales.



PERFILES PARTICIPANTES

AMIKIUR

- **Gobierno Territorial Autónomo de la Nación Wampis:** surge con el objetivo de hacer frente a las amenazas contra la conservación del territorio desde una gestión territorial que dialogue con nuestras costumbres y garantice una vida grata para nuestra población.
- **Radio Kurruf:** RadioKurruf es un espacio radial autónomo nacido bajo la lluvia y levantado por el viento de Wallmapu
- **Pakkiru de Pastaza:** representa a las 16 comunas, pueblos y asociaciones kichwas de la Provincia de Pastaza. A través del Consejo de gobierno se busca continuar con la propuesta de Kawsak Sacha "Selva Viviente" para asegurar una verdadera protección de nuestro territorio, así como la continuidad de las prácticas culturales y del buen vivir de nuestras comunidades







































