TEJIENDO SEGURIDAD DIGITAL

GUARDIANES DIGITALES COMUNITARIOS: CURRÍCULO DE FORMACIÓN DE FORMADORES EN CIBERSEGURIDAD, GOBERNANZA Y DERECHOS DIGITALES PARA ORGANIZACIONES, COMUNIDADES Y PUEBLOS INDÍGENAS Y AFRODESCENDIENTES EN COLOMBIA

Septiembre 2025

INSTITUTO DATA GOYÁ

Guardianes digitales comunitarios: currículo de formación de formadores en ciberseguridad, gobernanza y derechos digitales para comunidades indígenas y afrodescendientes en Colombia / Autoría de Umut Pajaro Velásquez, Denise Machado Leal, Jose A. Rojas Marcelo; Contenido Umut Pajaro Velásquez; Revisión de Perspectiva Étnica Saya Pasillo; Revisión de estilo y Edición Denise Machado Leal. -- Rubiataba, Goiás, Brasil : Instituto Data Goyá, 2025. 45 p. : il.

Incluye referencias.
Texto en español.

Número de Identificación da Obra: 012025- Versión de 29 de septiembre de 2025

1. Educación digital - Colombia - Currículos. 2. Ciberseguridad - Estudio y enseñanza - Colombia. 3. Pueblos indígenas - Educación - Colombia. 4. Afrodescendientes - Educación - Colombia. 5. Formación de formadores.

CDD 370

Información de contacto:
Rubiataba, Goiás, Brasil.
Email: denise@datagoya.com.br

Más recursos disponibles https://datagoya.com.br/

Redacción
Umut Pajaro Velásquez
Denise Machado Leal
Jose A. Rojas Marcelo

Contenido
Umut Pajaro Velásquez

Revisión de Perspectiva Étnica
Saya Pastillo

Revisión de Estilo, Diseño y Edición
Denise Machado Leal

Equipo de Trabajo del Proyecto Tejiendo Seguridad Digital:
Denise Machado Leal – Líder, Experta en Protección de Datos para Pueblos Indígenas y Tradicionales, y Diseñadora de Formación de Formadores
Umut Pajaro Velásquez – Colíder, Experto en Gobernanza de Internet y Educación Digital, y Diseñador de Currículo
Jose A. Rojas Marcelo (Quantvia Legal Advisors) – Colíder, Experto en Seguridad Digital, y Diseñador de Evaluación de Seguridad Digital
Ximena Cuzcano – Experta en Seguridad Digital y Perspectiva de Género
Saya Pastillo – Experta en Tecnología y Gobernanza de Internet Desde la Perspectiva de las Comunidades y Pueblos Indígenas
Karen Gutiérrez – Integradora Experta de Comunidades, Pueblos y Organizaciones Locales (Colombia)
Isac Pulido – Pasante y Apoyo en Procesos de Integración y Comunicación.

GUARDIANES DIGITALES COMUNITARIOS: CURRÍCULO DE FORMACIÓN DE FORMADORES EN CIBERSEGURIDAD, GOBERNANZA Y DERECHOS DIGITALES PARA COMUNIDADES INDÍGENAS Y AFRODESCENDIENTES EN COLOMBIA

En colaboración con HIVOS, en el marco del proyecto “Connect, Defend, Act” en Colombia, el Instituto Data Goyá y su equipo desarrollaron este currículo de estudios en seguridad digital adaptado a las OSC, que incluye los siguientes temas: Introducción a la seguridad digital, estudios sobre Legislación y normativas sobre protección de datos aplicables a las OSC, Identificación y respuesta ante las ciberamenazas más comunes que enfrentan las OSC, Herramientas de cifrado y comunicación segura, Estrategias de mitigación de riesgos.

Además, hemos colaborado con la organización facilitadora de Acción Comunitaria indicada por HIVOS (Fundación SIDOC), y otras organizaciones, para las sugerencias, comentarios, reflexiones y diseño del contenido de un currículo eficaz que asegure una respuesta adecuada a las necesidades de las OSC. El Currículo incluye métodos de evaluación claros que garantizan su eficacia y posibilidad de medición, y al final se convierte en una formación sostenible en seguridad digital. Agradecemos a HIVOS por la colaboración y oportunidad.

RESUMEN

1. INTRODUCCIÓN: FUNDAMENTOS PARA EL FORMADOR DE FORMADORES

Este currículo surge como una herramienta para fortalecer las capacidades de líderes y lideresas indígenas y afrodescendientes en Colombia, que asumirán el rol de formadores comunitarios en seguridad digital. Su propósito es ofrecer una base conceptual y metodológica que combine la Formación de Formadores (FdF) con la Educación Popular, garantizando procesos de aprendizaje participativos, culturalmente pertinentes y orientados a la acción.

Los futuros Guardianes Digitales no solo recibirán conocimientos técnicos, sino que también desarrollarán habilidades pedagógicas y organizativas para replicar el aprendizaje en sus comunidades. De esta manera, la formación trasciende la simple transmisión de información y se convierte en un proceso colectivo de empoderamiento, capaz de responder a las brechas de acceso, apropiación y seguridad digital que enfrentan los territorios.

En este sentido, el currículo se apoya en tres fundamentos principales: reconocer la tecnología como un espacio que puede reproducir desigualdades o fortalecer la autonomía comunitaria; promover el diálogo de saberes, articulando conocimientos técnicos con saberes ancestrales y organizativos; y garantizar que cada módulo conduzca a acciones concretas que refuercen la soberanía tecnológica comunitaria y la defensa de derechos en el entorno digital.

1.1 PROPÓSITO Y FILOSOFÍA DEL CURRÍCULO

Este documento presenta una propuesta curricular diseñada para la formación de líderes y lideresas de comunidades indígenas y afrodescendientes en Colombia, con el objetivo de que se conviertan en “Guardianes Digitales”. No se trata de un manual técnico tradicional, sino de una propuesta político-pedagógica. Su propósito fundamental es empoderar a estas comunidades para que no solo utilicen las tecnologías digitales de manera segura, sino que también participen activamente en la construcción de un ecosistema de internet más justo, equitativo e inclusivo. Los Guardianes Digitales serán facilitadores capaces de proteger a sus comunidades, defender sus derechos colectivos e individuales en el entorno digital y articular sus voces en los espacios donde se decide el futuro de la red.

La filosofía que sustenta este currículo parte del reconocimiento de que la tecnología no es una herramienta neutral. Su diseño, implementación y gobernanza pueden tanto replicar y amplificar las estructuras de poder y las desigualdades existentes como

desafiarlas.[1] Por consiguiente, la apropiación tecnológica debe ser un acto crítico, consciente y colectivo, orientado a fortalecer la autonomía y los planes de vida de cada comunidad.

1.2 EL ENFOQUE PEDAGÓGICO: HIBRIDANDO LA FORMACIÓN DE FORMADORES CON LA EDUCACIÓN POPULAR

Para lograr un impacto profundo y sostenible, este currículo fusiona dos potentes enfoques pedagógicos: la Formación de Formadores (FdF) y la Educación Popular (EP).

1.2.1 Principios de la Formación de Formadores (FdF)

El modelo FdF proporciona la estructura para escalar el conocimiento de manera efectiva. Se organiza en un proceso de tres etapas: una fase de pre-capacitación para identificar necesidades, una etapa de capacitación intensiva y una fase de post-capacitación para acompañar la réplica.[2] El objetivo de la FdF no es simplemente transferir información, sino "el desarrollo en los alumnos" [3], capacitándolos en habilidades cruciales como la planificación de acciones formativas, el diseño de materiales didácticos y la evaluación de procesos.[4] Se busca que los nuevos formadores desarrollen autonomía y creatividad, aspirando no a imitar al maestro, sino a "buscar lo que buscan ellos", es decir, a encontrar sus propias soluciones para los desafíos de su entorno.[3]

1.2.2 Principios de la Educación Popular (EP) y el Diálogo de Saberes

Un modelo FdF estándar resulta insuficiente para contextos culturales y políticos tan específicos. Por ello, se enriquece con los principios de la EP, garantizando su relevancia cultural y su potencial empoderador.

- Partir de la Realidad: Todo proceso educativo debe comenzar con el análisis crítico de la propia realidad de los participantes.[6] Sus vivencias, conocimientos y luchas no son un punto de partida anecdótico, sino una fuente legítima de saber que estructura todo el aprendizaje.
- Diálogo de Saberes: Se rompe la jerarquía tradicional entre el "experto" que enseña y el "aprendiz" que recibe. El conocimiento técnico del facilitador entra en un diálogo horizontal con los saberes ancestrales, organizativos, territoriales y culturales de la comunidad.[8] El conocimiento se co-construye de manera colectiva, reconociendo que cada participante es portador de saberes valiosos.
- Praxis (Acción-Reflexión-Acción): El aprendizaje es un ciclo dinámico que no

termina en el aula. Cada módulo está diseñado para conducir a una acción concreta dentro de la comunidad. La reflexión sobre los resultados de esa acción alimenta y enriquece el siguiente ciclo de aprendizaje, garantizando que el conocimiento se aplique y se transforme en experiencia.[8]

- Dimensión Política: La educación es un acto inherentemente político. Este currículo no busca formar consumidores pasivos de tecnología, sino sujetos críticos, conscientes de las relaciones de poder en el entorno digital y capaces de organizarse para transformar sus realidades.[6]

1.3 CONTEXTO: LA REALIDAD DIGITAL DE LAS COMUNIDADES ÉTNICAS EN COLOMBIA

El desarrollo de este currículo responde a un contexto complejo y paradójico que enfrentan las comunidades indígenas y afrodescendientes en Colombia en su relación con el mundo digital.

- **La Brecha de Acceso Persistente:** Por un lado, existen importantes iniciativas gubernamentales y del sector privado para expandir la conectividad. Programas como "Juntas de Internet", "Conectividad para Cambiar Vidas" y el despliegue de infraestructura 4G buscan conectar a millones de colombianos en zonas rurales y apartadas.[11] Sin embargo, la realidad en muchos territorios es otra. Investigaciones en departamentos como Vaupés revelan un acceso "a cuentagotas": intermitente, de muy baja velocidad y a menudo limitado a pequeños puntos de conexión comunitarios, lo que impide un uso significativo de la red.[13] La brecha en la cobertura de internet entre hogares indígenas y no indígenas sigue siendo una realidad palpable.[1]
- **La Brecha de Apropiación:** El acceso a la infraestructura es solo una parte del desafío. La brecha digital tiene múltiples facetas: motivacional (el deseo de conectarse), material (acceso a dispositivos y asequibilidad), de habilidades y de uso (la capacidad de aprovechar la conexión para fines relevantes).[13] Un informe de la Fundación Karisma revela que el 72% de las personas defensoras de derechos humanos en Colombia, muchas de ellas pertenecientes a comunidades étnicas, tienen niveles bajos o medios de apropiación digital, lo que aumenta directamente su vulnerabilidad.[15] La falta de un acompañamiento adecuado y de contenidos culturalmente pertinentes puede convertir el simple acceso en un nuevo riesgo.[14]
- **Un Ecosistema de Riesgos Complejo:** La llegada de la conectividad, en ausencia de una preparación adecuada, expone a las comunidades a un ecosistema de riesgos diverso. Estos van desde la exposición de niños, niñas y adolescentes a contenidos inapropiados como violencia o pornografía [16], hasta la erosión de la identidad cultural por la influencia de estilos de vida globales que pueden parecer más atractivos para la juventud.[14] Más grave aún, el espacio

> digital se ha convertido en un nuevo frente de ataque contra líderes y lideresas sociales, ambientales y comunitarios. Amenazas directas, ciberacoso, campañas de desprestigio, phishing (suplantación para robar información) y acceso no autorizado a sus cuentas son incidentes comúnmente reportados.[15]

La política pública colombiana ha impulsado la conectividad como una solución fundamental para el desarrollo y el cierre de brechas.[12] El discurso oficial se ha centrado en la expansión de la infraestructura física y el aumento del número de conexiones. Sin embargo, la evidencia de organizaciones de la sociedad civil y la investigación académica muestra que este acceso, cuando finalmente llega a los territorios más apartados, es a menudo precario y no va acompañado de procesos de formación que respondan a las necesidades y realidades locales.[13]

Esta desconexión entre la política de infraestructura y la realidad de la apropiación genera una profunda paradoja: la conectividad, presentada como una herramienta de empoderamiento, puede convertirse en un vector de nuevos y graves riesgos socioculturales y de seguridad.[14] Las comunidades se ven inmersas en un entorno digital diseñado en otros contextos, con lógicas de mercado y valores que pueden ser ajenos o incluso contrarios a sus cosmovisiones y formas de organización.[17] El desafío, por lo tanto, no es simplemente la "falta de internet", sino la falta de un internet que les pertenezca y les sirva.

En consecuencia, este currículo se propone ir más allá de la "alfabetización digital" tradicional, que se limita a enseñar el uso de herramientas. El objetivo es avanzar hacia la construcción de una **"Soberanía Tecnológica Comunitaria"**. Este concepto implica que las comunidades desarrollen la capacidad colectiva no solo para usar la tecnología de forma segura, sino para gobernarla: decidir *qué* tecnologías adoptar, *cómo* integrarlas de acuerdo con sus propios valores y planes de vida, y *para qué* fines utilizarlas, como el fortalecimiento de su autonomía, la defensa de sus territorios y la promoción de sus culturas. El currículo se convierte así en una herramienta para construir esta soberanía desde la base.

2- MÓDULOS

El currículo se estructura en seis módulos progresivos que combinan teoría, práctica y reflexión colectiva, diseñados para responder a las necesidades de las comunidades indígenas y afrodescendientes frente a los desafíos del mundo digital.

El Módulo 1 introduce la noción de territorio digital, explicando de manera accesible qué es Internet, quiénes son sus principales actores y cómo circula la información, con actividades prácticas que permiten vincular la tecnología a la realidad local. El Módulo 2 aborda los derechos en el mundo digital, mostrando cómo los derechos humanos se expresan en línea, cómo defenderlos y qué herramientas legales y comunitarias pueden emplearse.

El Módulo 3 se centra en la ciberseguridad comunitaria, brindando conocimientos básicos de cuidado digital, mapeo de riesgos y un catálogo de herramientas libres y seguras, fortaleciendo la idea de cuidado colectivo. El Módulo 4 explora la gobernanza de Internet y la participación comunitaria, vinculando las luchas locales con escenarios nacionales, regionales y globales, y promoviendo la construcción de agendas propias desde las comunidades.

El Módulo 5 desarrolla protocolos de respuesta a incidentes, ofreciendo guías claras y ejercicios prácticos para que las comunidades puedan reaccionar de manera organizada y efectiva frente a amenazas digitales. Finalmente, el Módulo 6 se dedica al rol del formador comunitario, ofreciendo herramientas pedagógicas, metodológicas y de planificación para asegurar la réplica del currículo en cada territorio, consolidando un efecto multiplicador.

En conjunto, estos módulos garantizan un proceso integral de formación que articula el aprendizaje técnico con el fortalecimiento político, cultural y organizativo de las comunidades en su camino hacia la soberanía digital.

2.1 MÓDULO 1: NUESTRO TERRITORIO DIGITAL - COMPRENDIENDO EL ECOSISTEMA DE INTERNET

El objetivo es desmitificar la tecnología y construir una comprensión fundamental y crítica de cómo funciona Internet, quiénes son sus actores clave y cómo se relaciona con el territorio físico y comunitario.

2.1.1 ¿Qué es Internet? De lo Abstracto a lo Concreto (Pedagogía de la Analogía)

Para que la comprensión de Internet sea significativa, es crucial anclarla en conceptos y realidades conocidas por las comunidades. La infraestructura física de la red —cables submarinos, fibra óptica, satélites y antenas— se explicará utilizando analogías con elementos del territorio, como los ríos que conectan comunidades, los caminos veredales o las

redes de comunicación oral que tejen el tejido social. Se visualizarán los esfuerzos de conectividad del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)[11] en mapas del país, mostrando dónde se ubican las "carreteras principales" de la información y dónde persisten los "caminos de trocha" digitales o las "zonas de silencio", coincidiendo a menudo con los territorios étnicos.

Actividad Práctica: Mapeo de Nuestro Territorio Digital

En un mapa físico del resguardo, consejo comunitario o territorio colectivo, los participantes dibujarán su realidad de conexión. Identificarán dónde se conectan (en casa, en un quiosco, en el parque), quiénes proveen esa conexión (una empresa, una Junta de Internet comunitaria), el tipo de acceso (WiFi, datos móviles), y mapearán la calidad de la señal en diferentes zonas. También discutirán los costos económicos asociados, un factor clave que limita el acceso para muchas familias.[1] Esta actividad transforma el concepto abstracto de "la red" en una realidad tangible, económica y geográfica, permitiendo un primer diagnóstico colectivo de sus fortalezas y debilidades de conexión.[13]

2.1.2 ¿Quién Manda en la Red? Actores y Poder en el Ecosistema Digital

Internet no es un espacio sin gobierno; sus reglas y su dirección son el resultado de la interacción y, a menudo, de la tensión entre diversos actores. Se presentará el modelo multi-actor (o *multi-stakeholder*) que define la gobernanza de internet, compuesto por el gobierno, el sector privado, la academia, la sociedad civil y la comunidad técnica.[19] Se identificarán los actores más relevantes en el contexto colombiano, explicando sus roles e intereses:

- **Gobierno:** MinTIC y la Comisión de Regulación de Comunicaciones (CRC), encargados de formular políticas públicas y regular el sector.[19]
- **Sector Privado:** Empresas como Google, Telefónica o los proveedores locales de internet, cuyo interés principal es la expansión de servicios y el mantenimiento de la infraestructura.[19]
- **Sociedad Civil:** Organizaciones como la Fundación Karisma, la Fundación para la Libertad de Prensa (FLIP) o Colnodo, que abogan por un internet con enfoque social y de derechos humanos.[19]
- **Academia:** Universidades que investigan los impactos sociales y culturales de las tecnologías.[19]

Actividad Práctica: Juego de Roles: La Mesa de Gobernanza

Para que los participantes comprendan vivencialmente las dinámicas de poder, se realizará un juego de roles. Se les asignará la representación de los diferentes actores y se planteará un tema de debate relevante, como: "Una empresa de telecomunicaciones quiere instalar una antena en un sitio sagrado de la comunidad a cambio de ofrecer internet gratuito". Cada grupo deberá defender los intereses de su rol. El objetivo es que experimenten las tensiones, negociaciones y desequilibrios de poder que existen en la toma de decisiones sobre el futuro de internet, entendiendo por qué es crucial que su propia voz esté presente en esas discusiones.[19]

2.1.3 El Flujo de la Información: ¿De Dónde Viene y a Dónde Va?

Se explicarán conceptos técnicos básicos de manera accesible, recurriendo nuevamente a analogías. Los servidores y la "nube" se pueden comparar con una "chagra" o una huerta comunitaria donde se siembra y almacena la información. Las direcciones IP son como la dirección de una casa, y los paquetes de datos son como las cartas que un mensajero lleva de un lugar a otro. Se abordará un aspecto crítico del internet actual: la centralización de la información y los servicios en un puñado de grandes corporaciones tecnológicas.[21] Esto tiene implicaciones directas sobre la diversidad cultural, el control de la información y la soberanía de los datos.

Actividad Práctica: El Camino de un Mensaje

Los participantes trazarán el viaje hipotético de un mensaje de WhatsApp o una foto enviada desde su comunidad a un familiar en otra ciudad. Identificarán todos los intermediarios que "tocan" o pueden "ver" ese mensaje: el proveedor de internet local, los cables de fibra óptica, los servidores de Meta (Facebook/WhatsApp) en otros países. Este ejercicio visual y práctico permite comprender de forma intuitiva la vulnerabilidad de la información y sienta las bases para entender la importancia vital del cifrado, que se abordará en el Módulo 3.

Para las comunidades indígenas y afrodescendientes, el concepto de "territorio" trasciende lo puramente físico; es un entramado complejo de relaciones sociales, culturales,

espirituales y de gobierno propio. La llegada de la tecnología digital no solo introduce una herramienta, sino que crea un nuevo espacio de interacción que puede entenderse como una extensión de su territorio ancestral: el **territorio digital**.[13] Este nuevo territorio no es un espacio neutral. Está configurado y gobernado por actores con intereses económicos y políticos que a menudo son ajenos o incluso contrarios a los de las comunidades.[19] Las mismas luchas históricas por la tierra, la autonomía y la protección de los recursos naturales se replican y adquieren nuevas formas en este dominio. La disputa por el espectro radioeléctrico, la defensa contra la extracción masiva de datos personales (el nuevo extractivismo) o la lucha por una representación cultural digna y no folclorizada son ejemplos de estas tensiones.

Por lo tanto, este módulo debe enmarcar la comprensión de Internet no como una herramienta externa que se "usa", sino como un nuevo territorio que debe ser gobernado, defendido y apropiado según los principios de la gobernanza territorial propia. Esta resignificación es fundamental para una apropiación culturalmente relevante y políticamente movilizadora. Conceptos como "ciberseguridad" pueden traducirse a la práctica de la "guardia indígena digital", y la "gobernanza de internet" se convierte en la tarea de construir un "plan de vida digital" que se articule con el plan de vida de la comunidad.

2.2 MÓDULO 2: NUESTROS DERECHOS EN EL MUNDO DIGITAL

El objetivo es traducir el marco abstracto de los derechos digitales a situaciones concretas y defendibles, empoderando a los participantes para reconocer violaciones y exigir garantías, tanto a las plataformas como al Estado.

2.2.1 De los Derechos Humanos a los Derechos Digitales: Una Extensión Natural

Se establecerá un principio fundamental: los derechos digitales no son una categoría nueva y separada de derechos. Son la extensión y aplicación de los derechos humanos universalmente reconocidos —como el derecho a la privacidad, a la libertad de expresión, a la no discriminación o al acceso a la información— al entorno digital.[22] Se revisará el marco legal colombiano, que cuenta con una base sólida como la Ley 1581 de 2012 sobre Protección de Datos Personales y una rica jurisprudencia de la Corte Constitucional que ha adaptado estos derechos al mundo en línea.[24]

Actividad Práctica: Círculo de Palabra: ¿Qué Derechos son Importantes para Nosotros?

El aprendizaje partirá de la propia comunidad. Se abrirá un diálogo (círculo de palabra o un foro en línea) donde los participantes compartirán cuáles son los derechos y valores más relevantes en su cosmovisión y su lucha diaria: el derecho a la autonomía, a la consulta previa, a la cultura propia, a la tierra y al territorio. A partir de esta base, se guiará una reflexión colectiva sobre cómo la llegada de la tecnología (un celular, una conexión a internet) está afectando, fortaleciendo o poniendo en riesgo esos derechos fundamentales.

2.2.2 "Traduciendo" los Derechos: De la Ley a la Vida Cotidiana

Para que sean herramientas útiles, los derechos deben ser comprensibles y aplicables. Este submódulo se dedicará a "traducir" cada derecho clave a un lenguaje sencillo y a situaciones cotidianas.

- **Derecho a la Privacidad y Protección de Datos**[23]: Se explicará como el derecho a decidir qué se comparte sobre uno mismo, la familia y la comunidad. Se analizará el concepto de consentimiento informado: ¿entendemos realmente a qué estamos dando permiso cuando instalamos una aplicación? Se usará el caso de la aplicación CoronApp, impulsada por el gobierno durante la pandemia, como ejemplo de recolección masiva de datos y los debates que generó sobre la privacidad.[27]
- **Derecho a la Libertad de Expresión** [23]: Se explorarán sus límites y alcances. ¿Qué puedo decir en línea? Se abordará la diferencia crucial entre la opinión crítica, la información verificable y los discursos de odio o la incitación a la violencia. Se analizará la problemática de la moderación de contenidos, donde las decisiones de empresas tecnológicas extranjeras pueden silenciar voces legítimas, como ocurrió con denuncias durante el Paro Nacional de 2021.[27]
- **Derecho al Olvido** [23]: Se presentará como el derecho a solicitar que se elimine de internet información personal que es falsa, que ya no es relevante o que causa un daño injustificado a la reputación de una persona.
- **Derecho a la Identidad Cultural y al Anonimato:** Se discutirá la dualidad de la identidad digital: puede ser una herramienta para fortalecer y difundir la cultura propia, pero también un riesgo de folclorización o de debilitamiento de la identidad comunitaria, especialmente entre los jóvenes.[14] Se abordará el derecho al anonimato como una herramienta de protección esencial para defensores y activistas que enfrentan persecución.[25]
- **Protección de Niños, Niñas y Adolescentes (NNA):** Se tratarán de manera específica los riesgos que enfrentan los NNA en línea (exposición a contenidos

dañinos, ciberacoso, grooming) y las responsabilidades de la familia y la comunidad en su acompañamiento y protección, en línea con la legislación colombiana que busca crear entornos digitales seguros para ellos.[16]

2.2.3 Defendiendo Nuestros Derechos: Mecanismos y Aliados

Reconocer un derecho vulnerado es el primer paso; saber cómo defenderlo es lo que otorga poder. Se explicarán las vías prácticas para la exigibilidad de derechos:

- **Mecanismos de las Plataformas:** Cómo usar las herramientas de reporte de contenidos en redes como Facebook o YouTube.
- **Acción de Tutela:** Se explicará qué es la tutela como mecanismo judicial para la protección de derechos fundamentales, pero también se señalarán sus limitaciones actuales, ya que la Corte Constitucional ha determinado que, en muchos casos, se debe agotar primero la vía de reclamación con la plataforma, lo que puede generar demoras e incertidumbre.[26]
- **Organizaciones Aliadas:** Se presentará el rol de organizaciones de la sociedad civil que son aliadas clave en la defensa de los derechos digitales en Colombia, como la **FLIP**, **Dejusticia** y **Access Now**, que pueden ofrecer asesoría legal y técnica.[19]

Actividad Práctica: Simulación de Denuncia

En grupos pequeños, los participantes trabajarán sobre un caso hipotético relevante para su contexto (ejemplo: “una empresa turística publica en Instagram fotos de un ritual sagrado sin el permiso de la comunidad, usándolas para publicidad”). Deberán diseñar una estrategia paso a paso para solicitar la eliminación del contenido, detallando qué harían primero (reportar en la plataforma), qué información recopilarían y a qué aliado podrían contactar si la plataforma no responde.

2.2.4 Matriz de Traducción de Derechos Digitales

La siguiente tabla sirve como herramienta pedagógica central del módulo. Su objetivo es convertir conceptos legales abstractos en un formato práctico y accionable, directamente conectado con la realidad y los valores comunitarios.

Derecho Digital (Lenguaje Formal)	**¿Qué Significa en Nuestra Comunidad? (Traducción)**	**Ejemplo de Riesgo/Violación**	**¿Cómo lo Defendemos? (Acción Comunitaria)**

Derecho a la Privacidad y Protección de Datos Personales (Ley 1581) [24]	El derecho a decidir quién puede saber cosas sobre nosotros, nuestra familia y nuestra comunidad. Es como decidir a quién invitamos a entrar a nuestra maloca o casa.	Una app de salud del gobierno pide acceso a todos mis contactos y fotos sin explicar para qué.[27] Se publican fotos de un líder comunitario en redes sociales con información falsa para amenazarlo.[15]	1. No dar permiso a la app. 2. Preguntar en la comunidad si otros tienen el mismo problema. 3. Contactar a una organización aliada para pedir consejo. 4. Usar mensajería cifrada para hablar del tema.
Derecho a la Libertad de Expresión [23]	El derecho a contar nuestra verdad, a denunciar las injusticias y a compartir nuestras ideas, siempre que no llamemos a la violencia contra otros. Es nuestra palabra en la red.	Facebook elimina un video donde la guardia indígena está documentando un abuso, diciendo que es "contenido violento".[27]	1. Guardar una copia del video. 2. Apelar la decisión en la plataforma. 3. Documentar el caso (capturas de pantalla). 4. Contactar a la FLIP o a un medio de comunicación aliado para visibilizar la censura.
Derecho a la Identidad y la Cultura Propia [14]	El derecho a que nuestra cultura, lengua y tradiciones sean respetadas en internet, y a decidir cómo queremos mostrarlas al mundo, sin que nos conviertan en un adorno.	Un influencer visita la comunidad, graba a los niños sin permiso de sus padres y sube un video que se burla de sus costumbres.	1. Reportar el video en la plataforma por acoso o irrespeto a menores. 2. Organizar una respuesta comunitaria en redes, explicando por qué ese contenido es dañino. 3. Crear contenido propio que muestre la cultura con dignidad.
Derecho a la Protección de NNA en Internet [16]	El deber de toda la comunidad de cuidar a nuestros jóvenes para que puedan aprovechar internet sin que les hagan daño, protegiéndolos de engaños y abusos.	Un adulto desconocido contacta a una joven de la comunidad por redes sociales, le pide fotos íntimas y luego la amenaza con publicarlas si no le da dinero (sextorsión).	1. Apoyar a la joven, asegurándole que no es su culpa. 2. No ceder a la extorsión. 3. Bloquear y reportar al agresor. 4. Documentar las amenazas. 5. Buscar apoyo en organizaciones especializadas o en el ICBF.

Para las comunidades étnicas en Colombia, cuya historia está marcada por la lucha por los derechos territoriales y la autonomía, la defensa de sus derechos en el entorno digital adquiere una dimensión estratégica. Las amenazas a su pervivencia física y cultural a menudo comienzan con la estigmatización, la desinformación y los ataques contra sus líderes, lideresas y procesos organizativos.[22] Hoy, una parte significativa de esta violencia se perpetra en el espacio digital.[15] Las campañas de desprestigio en redes sociales, la suplantación de identidad de sus organizaciones o la vigilancia digital de sus comunicaciones no son problemas tecnológicos aislados; son las nuevas armas utilizadas en la disputa por el territorio.

En este contexto, la defensa de los derechos digitales —como la privacidad, la libertad de expresión o la identidad— no es un fin en sí mismo. Se convierte en una **estrategia fundamental y contemporánea para la defensa del territorio, la cultura y la vida**. Proteger la cuenta de WhatsApp de una lideresa no es solo un acto de "ciberseguridad personal", es un acto de protección de toda la comunidad y su proceso organizativo. Combatir una noticia falsa sobre un proceso de consulta previa no es solo "verificar hechos", es defender la legitimidad de su lucha y su derecho a la autodeterminación. Este módulo debe, por tanto, conectar explícitamente cada derecho digital con la agenda de defensa territorial y los planes de vida de las comunidades, dotando a este aprendizaje de un sentido de urgencia, relevancia y poder transformador.

2.3 MÓDULO 3: CUIDANDO NUESTRA MALOCA DIGITAL - CIBERSEGURIDAD COMUNITARIA

El objetivo es desarrollar capacidades prácticas y fomentar una cultura de cuidado digital colectivo, enfocándose en la prevención, la identificación de riesgos contextuales y el uso de herramientas accesibles, seguras y de código abierto.

2.3.1 Mapa de Riesgos Comunitário: ¿De qué nos cuidamos?

El punto de partida para la seguridad es comprender las amenazas específicas que enfrenta la comunidad. Se iniciará un diálogo que conecte los riesgos ya conocidos en el mundo físico (amenazas, chismes, robos, vigilancia) con sus manifestaciones en el entorno digital. Se presentarán los incidentes de seguridad más comunes reportados por defensores de

derechos humanos en Colombia, que incluyen el acceso no autorizado a dispositivos y cuentas, el *phishing* (engaños para robar credenciales) y la suplantación de identidad.[15] Además, se destacará la alarmante cifra de que el 50% de las personas defensoras encuestadas ha recibido amenazas directas a través de medios digitales.[15] Se prestará especial atención a los riesgos diferenciados que afectan a grupos específicos:

- **Jóvenes:** Se analizarán amenazas como el ciberacoso, los retos virales peligrosos y la sextorsión, que explotan las vulnerabilidades propias de la adolescencia.[16]
- **Mujeres:** Se abordará la violencia de género en línea, que se manifiesta a través de acoso sistemático, difusión no consentida de imágenes íntimas y campañas de desprestigio que atacan su credibilidad y participación en la vida pública.[18]

Actividad Práctica: Cartografía de Riesgos Digitales

Inspirada en metodologías participativas como la cartografía social o el mapeo corporal, y adaptando técnicas de organizaciones como Tactical Tech [33], esta actividad invita a los participantes a visualizar sus riesgos. En el medio de su preferencia se pide que represente a la comunidad, identificarán y dibujarán las amenazas digitales que más les afectan a nivel individual (el robo de una cuenta de Facebook), familiar (un joven siendo acosado en un grupo de WhatsApp) y comunitario (una campaña de desinformación contra la autoridad local). Este ejercicio permite comprender visualmente cómo un riesgo digital aparentemente individual puede tener profundas repercusiones en la confianza y la cohesión de toda la comunidad.

2.3.2 Higiene y Cuidado Digital Básico: Nuestros Primeros Pasos

Se enseñarán prácticas fundamentales de seguridad de una manera sencilla, memorable y aplicable de inmediato.

- **Contraseñas Fuertes y Únicas:** En lugar de combinaciones complejas y difíciles de recordar, se enseñará la técnica de crear “frases de contraseña” largas y fáciles de memorizar (ej: "Micasatiene2perrosy1gato!"). Se enfatizará la regla de oro: una contraseña única para cada servicio importante.[35]
- **Autenticación de Dos Factores (2FA):** Se explicará este concepto crucial utilizando la analogía de “ponerle dos candados a la puerta de la casa”. Se mostrará cómo activar la 2FA en servicios clave como WhatsApp, Facebook y el correo electrónico, lo que impide el acceso no autorizado incluso si alguien

roba la contraseña.[35]

- **Navegación y Conexión Segura:** Se enseñará a identificar sitios web seguros que utilizan el protocolo https (reconocible por el ícono del candado en el navegador). Se insistirá en la importancia de desconfiar de enlaces sospechosos recibidos por mensaje o correo y en evitar el uso de redes WiFi públicas y abiertas para realizar actividades sensibles como transacciones bancarias o comunicaciones privadas.[37]
- **Identificación de Phishing:** A través de ejemplos reales y adaptados al contexto local (ej. un mensaje falso sobre un subsidio del gobierno), los participantes aprenderán a reconocer las señales de un intento de phishing: urgencia, errores de ortografía, solicitudes de información personal, etc.

2.3.3 Caja de Herramientas del Guardián Digital: Software Libre y Seguro

Se presentará un catálogo curado de herramientas digitales que son de código abierto (lo que permite su auditoría y genera más confianza), gratuitas y, fundamentalmente, diseñadas para funcionar de manera eficiente en condiciones de baja conectividad. La selección se basa en recomendaciones de organizaciones expertas y de confianza en el ámbito de los derechos humanos y la tecnología, como Security in-a-box, Electronic Frontier Foundation (EFF), SocialTIC y Amnistía Internacional.[39]

Actividad Práctica: Instalaton y Configuraton

Esta es una sesión eminentemente práctica. Con el acompañamiento de los facilitadores, los participantes instalarán y configurarán estas herramientas en sus propios dispositivos (si los tienen) o en equipos comunitarios. El objetivo es que no solo conozcan la herramienta, sino que aprendan a usarla y a configurarla de forma segura desde el primer momento.

2.3.4 Catálogo de Herramientas de Cuidado Digital

La siguiente tabla actúa como una ficha técnica de referencia rápida, visual y fácil de entender, que justifica la elección de cada herramienta y empodera a los usuarios a tomar decisiones informadas.

Nombre y Función	¿Por qué la Elegimos?	¿Dónde la Consigo?	Un Consejo Clave

Signal: Para chatear y llamar de forma privada y segura.	Gratis, cifrado de extremo a extremo por defecto, no guarda tus mensajes, funciona bien con pocos datos, recomendada por defensores de DDHH.[35]	Play Store, App Store, Sitio Oficial	Activa el "Bloqueo de registro" (PIN de seguridad) para que nadie más pueda registrar tu número en otro teléfono.
KeePassXC: Para guardar todas tus contraseñas en un solo lugar seguro y sin necesidad de internet.	Gratis, código abierto, funciona sin conexión a internet (offline), lo que da más control y seguridad sobre los datos. Ideal para zonas con mala conectividad.[42]	Sitio Oficial (para PC)	Guarda el archivo de tu base de datos en un lugar seguro y crea una copia de seguridad en una USB. ¡No olvides tu contraseña maestra!
ProtonVPN: Para proteger tu conexión a internet, especialmente cuando usas una red WiFi pública.	Tiene una versión gratuita funcional y sin límite de datos, con una política de no guardar registros de tu actividad. Basada en Suiza, con fuertes leyes de privacidad.[43]	Play Store, App Store, Sitio Oficial	Úsala siempre que te conectes a una red WiFi que no sea la de tu casa o de confianza (ej. en un parque, un café internet, un aeropuerto).
Cryptomator: Para crear una "caja fuerte" digital y proteger tus archivos importantes en tu computador, USB o en la nube.	Gratis, código abierto, fácil de usar. Cifra los archivos antes de subirlos a servicios como Google Drive o Dropbox, dándote una capa extra de seguridad.[43]	Play Store, App Store, Sitio Oficial	Crea una bóveda para los documentos más sensibles de tu organización o comunidad. Así, incluso si alguien accede a tu cuenta de la nube, no podrá leer los archivos.

La ciberseguridad, en su enfoque tradicional, se centra en el individuo: "protege *tu* contraseña", "instala un antivirus en *tu* computador". Sin embargo, esta perspectiva es insuficiente y a menudo inadecuada para contextos comunitarios como los de los pueblos indígenas y afrodescendientes, donde el bienestar es un asunto colectivo y la seguridad de una persona está intrínsecamente ligada a la seguridad del grupo. Un informe de la Fundación Karisma subraya que la falta de protocolos de seguridad colectivos es un problema más grave que la falta de apropiación de herramientas por parte de los individuos.[15]

Un ataque digital contra una lideresa o un líder no es un ataque aislado; es un ataque contra la organización, el proceso y la comunidad en su conjunto.[44] Por lo tanto, la respuesta debe ser necesariamente colectiva. Este módulo debe trascender el paradigma de la "autoprotección individual" para construir un marco de **"cuidado digital colectivo"**. Este enfoque reinterpreta las prácticas de seguridad como actos de solidaridad y responsabilidad mutua. "Yo protejo mi cuenta de WhatsApp no solo por mi seguridad, sino para proteger la

información de todos mis contactos y no poner en riesgo a mi comunidad". Se deben promover prácticas como la revisión de seguridad en parejas, la creación de "círculos de confianza" para compartir alertas y apoyarse mutuamente[44], y la definición de responsabilidades compartidas, como designar a una persona para que ayude a otros a actualizar sus aplicaciones. En esta visión, la "maloca digital" (el espacio comunitario en línea) se cuida en minga, con el esfuerzo y el compromiso de todos.

2.4 MÓDULO 4: LA MINGA/CABILDO DIGITAL - GOBERNANZA DE INTERNET Y PARTICIPACIÓN COMUNITARIA

Objetivo: Empoderar a los participantes para que se reconozcan como actores legítimos y necesarios en la gobernanza de internet, proporcionándoles el conocimiento y las herramientas para incidir en las políticas y decisiones que afectan sus vidas digitales y sus territorios, reforzando la autonomía digital comunitaria con la capacidad de decidir sobre el uso de plataformas, datos y tecnologías desde sus propios principios de gobernanza

2.4.1 ¿Qué es la Gobernanza de Internet y por qué nos Importa?

Retomando los conceptos del Módulo 1, se profundizará en la idea de que la "gobernanza de internet" es el proceso mediante el cual los diversos actores (gobierno, empresas, sociedad civil, etc.) toman decisiones sobre las reglas del juego en el mundo digital.[19] Para que este concepto no sea abstracto, se utilizarán ejemplos concretos que impactan directamente la vida de las comunidades:

- La decisión sobre el precio de los planes de datos móviles.
- La regulación que obliga (o no) a las plataformas a eliminar contenidos de odio y racismo.
- La asignación de fondos públicos para conectar escuelas rurales.
- Las leyes sobre derechos de autor que pueden afectar la forma en que se comparte el conocimiento ancestral.

El mensaje central es claro: si las comunidades no participan en estas discusiones, otros tomarán las decisiones por ellas, y es probable que esas decisiones no reflejen sus necesidades, valores o derechos.[47]

2.4.2 La Mesa Colombiana de Gobernanza de Internet: Un Espacio para Incidir

Se presentará en detalle la Mesa Colombiana de Gobernanza de Internet como el principal escenario nacional para este diálogo. Se explicará qué es, quiénes participan (representantes del MinTIC, la CRC, empresas como Google, y organizaciones de la sociedad civil)[19], y cómo funciona. Se destacará su carácter voluntario, no jerárquico y su objetivo de promover el diálogo más que de imponer consensos.[47] Se revisarán los temas que habitualmente se discuten, como la libertad de expresión, la ciberseguridad, el acceso y los derechos de autor.[19] Críticamente, también se reconocerá uno de sus mayores desafíos: la necesidad de incluir más y mejores voces de las regiones y de las comunidades étnicas, que históricamente han estado subrepresentadas.[47]

Actividad Práctica: Analizando una Acta de la Mesa

Para desmitificar este espacio, a menudo percibido como técnico y lejano, se trabajará con un extracto simplificado de un acta real de una reunión de la Mesa (disponibles públicamente en su sitio web [47]). En grupos, los participantes leerán el extracto e identificarán quiénes hablaron, qué posturas defendieron y qué intereses podrían estar detrás de cada intervención. Esta actividad permite comprender de manera práctica la dinámica del debate y la importancia de preparar argumentos sólidos para participar.

2.4.3 Construyendo Nuestra Agenda: De la Queja a la Propuesta

Este submódulo se enfoca en desarrollar capacidades básicas para la incidencia política comunitaria, adaptada al ecosistema digital. El proceso se estructura en pasos claros y sencillos:

1. **Identificar y Diagnosticar el Problema:** Partiendo de los mapeos y discusiones de los módulos anteriores, se define claramente un problema. Ejemplo: “En nuestra vereda, la señal de internet es intermitente y las tarifas son las más altas de la región, lo que impide que nuestros jóvenes accedan a la educación virtual”.
2. **Recopilar Evidencia:** Se enseña a sustentar el problema con datos. Esto puede incluir los mapas de conectividad elaborados en el Módulo 1, testimonios de la comunidad, comparación de tarifas, etc.

3. **Formular una Propuesta Clara y Concreta:** La queja se transforma en una solicitud. Ejemplo: “Solicitamos al MinTIC y a la CRC que se incluya a nuestra comunidad en la próxima fase del programa Juntas de Internet y que se regule una tarifa social para los planes de datos en territorios étnicos”.[11]
4. **Interoperabilidad entre saberes:** Este eje reflexiona sobre cómo generar un diálogo real entre los marcos internacionales, como la gobernanza global de Internet, y las formas comunitarias de organización propias de los pueblos (asambleas, minkas, cabildos, etc). Las comunidades no siempre se integran a estos procesos de la misma manera: por ejemplo, instalar infraestructura sin participación activa puede generar desapego. En cambio, cuando se construye colectivamente como en una minga donde la comunidad adecúa el espacio y toma decisiones la tecnología se vuelve parte del territorio y se genera apropiación.

   Antes de articular con aliados también es importante reconocer que cada comunidad tiene dinámicas propias: en algunos casos, un llamado del cabildo no convoca, pero sí lo hace el párroco del lugar sí. Más allá de la minka, existen otras formas de organización y participación como los círculos de palabra, trueques de saberes, visitas casa a casa o encuentros festivos. Estas estrategias permiten fortalecer el diálogo desde la confianza, la cultura y el respeto mutuo. Comprenderlas es clave para una interoperabilidad entre saberes más justa y efectiva.
5. **Identificar y Articular con Aliados:** Ninguna lucha se da en solitario. Se identifican posibles aliados: otras comunidades con el mismo problema, organizaciones de la sociedad civil que trabajan en derechos digitales [19], académicos, periodistas o incluso funcionarios locales.
6. **Elegir el Canal de Incidencia:** Se exploran las diferentes estrategias para hacer llegar la propuesta: presentarla formalmente en la Mesa de Gobernanza, realizar una campaña en redes sociales para visibilizar el problema, contactar a un congresista de la región, etc.

Actividad Práctica: Elaborando una Propuesta para la Minga Digital

Trabajando sobre un problema real y prioritario para su comunidad, los participantes, en grupos, elaborarán una propuesta de incidencia de un párrafo, siguiendo la estructura de 5 pasos. Luego, la presentarán ante el resto del grupo, que actuará como un panel de “tomadores de decisión”, ofreciendo retroalimentación constructiva.

Es importante mencionar explícitamente el derecho a la soberanía tecnológica y de datos de los pueblos indígenas y afrodescendientes, como parte de la participación en la gobernanza digital. Esto le da un marco político más sólido.

Para culminar es importante generar evidencia práctica: por ejemplo, que cada comunidad participante elabore una propuesta de principios de gobernanza digital propios o un acta

simbólica de cabildo digital.

2.4.4 Más Allá de Colombia: Espacios Regionales y Globales

Para ampliar la perspectiva y conectar las luchas locales con un movimiento más amplio, se mencionará brevemente la existencia de foros de gobernanza a nivel regional, como el LACIGF (Foro de Gobernanza de Internet de América Latina y el Caribe), y a nivel global, como el Foro de Gobernanza de Internet (IGF) de las Naciones Unidas.[46] Esto ayuda a los participantes a entender que sus desafíos no son únicos y que existe una red global de personas y organizaciones trabajando en temas similares, abriendo puertas para el aprendizaje y la solidaridad internacional.

Las comunidades indígenas y afrodescendientes en Colombia poseen estructuras de gobierno propio reconocidas legalmente, como los Cabildos y los Consejos Comunitarios, que se rigen por planes de vida y etnodesarrollo que guían su futuro. El lenguaje y las lógicas de los espacios formales de gobernanza de internet, con su modelo *multi-stakeholder* y su búsqueda de consensos[19], pueden resultar ajenos a estas formas de organización. Invitar a las comunidades simplemente a "participar" en la Mesa de Bogotá podría ser interpretado como un intento de asimilación a un modelo externo, en lugar de un fortalecimiento del propio.

Iniciativas como el programa Juntanza Étnica demuestran que el camino más efectivo es el fortalecimiento del "gobierno propio e institucionalidad" y el "desarrollo económico autodeterminado".[49] Por lo tanto, este módulo debe reorientar el enfoque. La pregunta central no debe ser únicamente "¿cómo llevamos nuestra voz a la Mesa en Bogotá?", sino, primordialmente, **"¿cómo tomamos decisiones sobre la tecnología aquí, en nuestro territorio, según nuestras propias normas y planes de vida?"**. La participación en espacios externos como la Mesa se convierte entonces en una estrategia decidida y articulada desde el gobierno propio, no en el objetivo final. La "Minga/Cabildo Digital" no es solo una metáfora; es la propuesta de convocar asambleas comunitarias para debatir y decidir sobre su futuro digital, ejerciendo así su derecho al autogobierno también en este nuevo territorio.

2.5 MÓDULO 5: TEJIENDO REDES DE CUIDADO - PROTOCOLOS DE RESPUESTA A INCIDENTES

El objetivo es cocrear un protocolo de respuesta a incidentes de seguridad digital que sea simple, accionable y adaptado a la realidad comunitaria, fortaleciendo la resiliencia colectiva frente a los ataques y transformando momentos de crisis en oportunidades de fortalecimiento organizativo.

2.5.1 ¿Qué es un Incidente y Cuándo se Activa la Alarma?

Para que un protocolo sea efectivo, primero se debe definir claramente qué constituye un "incidente de seguridad digital" en el contexto comunitario. No se trata solo de un hackeo técnico complejo. Un incidente es cualquier evento en el entorno digital que ponga en riesgo a una persona, a un proceso organizativo o a la comunidad en su conjunto. Ejemplos concretos incluyen:

- Una amenaza directa recibida por WhatsApp o Facebook.
- La difusión de un rumor falso o una campaña de desprestigio contra una autoridad o un proyecto comunitario.
- El robo o la pérdida de un celular que contiene información sensible (contactos, fotos, documentos).
- La creación de un perfil falso en redes sociales que suplanta la identidad de una organización o un líder para generar confusión.

Una vez identificado el incidente, es crucial evaluar su gravedad. Se establecerán niveles de riesgo (bajo, medio, alto) basados en dos criterios principales: la credibilidad de la amenaza y el impacto potencial que podría tener sobre la persona o la comunidad.[44]

Actividad Práctica: Clasificando Casos

Se presentarán a los participantes varios escenarios de incidentes digitales. En grupos, deberán discutir y clasificar cada caso según el nivel de riesgo, justificando su decisión. Por ejemplo: ¿Es más grave un insulto anónimo en un comentario de Facebook o un mensaje privado con una amenaza de muerte de un perfil identificado? Esta discusión ayuda a desarrollar un criterio colectivo para la toma de decisiones bajo presión.

2.5.2 El Protocolo de Respuesta Rápida: Un Plan en 5 Pasos

Se presentará una estructura de protocolo clara y fácil de recordar, adaptada de marcos profesionales de respuesta a incidentes[53] y de guías prácticas diseñadas para activistas

y defensores de derechos humanos.[44]

1. **Paso 1: Contener y Evaluar (¡No entrar en pánico!):** La primera reacción ante una crisis no debe ser impulsiva. Lo primordial es proteger a la persona afectada y evitar que el daño se extienda. Esto puede implicar acciones inmediatas como desconectar un equipo de internet, avisar a la persona amenazada para que tome precauciones físicas, o cambiar temporalmente una contraseña. Se debe hacer una evaluación rápida: ¿qué pasó?, ¿quién está afectado?, ¿el riesgo sigue activo?[44]
2. **Paso 2: Documentar la Evidencia:** Este paso es crucial. Se debe guardar toda la evidencia posible del incidente: tomar capturas de pantalla de los mensajes o perfiles, guardar los enlaces (URLs), y anotar fechas, horas y nombres de usuario. Una buena documentación es indispensable para cualquier denuncia formal posterior ante las plataformas o las autoridades.[44]
3. **Paso 3: Comunicar al Círculo de Confianza:** Nadie debe enfrentar una crisis en soledad. Es vital activar una red de apoyo interna previamente definida. Se establecerá el concepto de "círculo de confianza" o "red de cuidado", un pequeño grupo de personas dentro de la comunidad a quienes se debe notificar inmediatamente. Este círculo es el primer anillo de respuesta y apoyo.[44]
4. **Paso 4: Analizar y Erradicar:** Una vez contenida la emergencia inicial y con el apoyo del círculo de confianza, se analiza la situación con más calma para decidir las siguientes acciones. Esto puede incluir bloquear al usuario agresor, reportar la publicación o el perfil a la plataforma, cambiar todas las contraseñas relacionadas o realizar un análisis más profundo del dispositivo si se sospecha de un malware.[54]
5. **Paso 5: Recuperar y Aprender:** La respuesta no termina cuando se elimina la amenaza. Es fundamental brindar apoyo a la persona afectada, reconociendo que los ataques digitales tienen un impacto emocional y psicológico real.[44] Finalmente, el círculo de confianza y la comunidad deben reflexionar sobre lo ocurrido: ¿qué falló en nuestras prácticas de seguridad?, ¿qué podemos hacer diferente para evitar que esto vuelva a pasar? Este paso de aprendizaje colectivo es lo que permite que el protocolo y la comunidad se fortalezcan con cada experiencia.[53]

2.5.3 Creando Nuestro Propio Protocolo Comunitario

No existe un protocolo único que sirva para todos. Cada comunidad debe diseñar y adaptar su propio plan de respuesta en función de sus capacidades, recursos, estructura organizativa y los riesgos específicos que enfrenta. Se utilizarán las preguntas guía del *Earth Defenders Toolkit* para facilitar este proceso de cocreación: ¿Quiénes son nuestros aliados más cercanos? ¿A quién podemos llamar en una emergencia? ¿Quiénes son nuestros oponentes y

qué tipo de tácticas usan? ¿Cuál es nuestra información más sensible que debemos proteger?[55]

Actividad Práctica: Diseñando el Protocolo de la Comunidad

Utilizando una plantilla visual y sencilla (un "lienzo" o "canvas"), los participantes completarán los campos de su propio protocolo comunitario. Este ejercicio práctico les permitirá materializar el plan, definiendo elementos clave como: los nombres y contactos de las personas que integran el círculo de confianza, el nombre y número de la organización aliada a la que pueden llamar para pedir asesoría técnica o legal (ej. FLIP, SocialTIC), y el contacto de la autoridad propia relevante (ej. el capitán de la guardia indígena, un miembro del consejo comunitario).

2.5.4 Seguimiento de Alertas: Plantilla de Protocolo Comunitario de Respuesta Rápida

Esta plantilla no es un documento burocrático, sino una herramienta de trabajo visual y tangible. Puede ser impresa y colocada en un lugar visible en la sede comunitaria, sirviendo como una guía de acción rápida en momentos de crisis.

PROTOCOLO DE RESPUESTA RÁPIDA - GUARDIANES DIGITALES

1. INCIDENTE (¿Qué pasó?):
(Espacio para describir brevemente el evento)

---

2. NIVEL DE RIESGO: (Marcar con una X)
( ) BAJO ( ) MEDIO ( ) ALTO

3. PASO 1: CONTENER (Acción Inmediata)

- [ ] Avisar a la persona afectada.
- [ ] Desconectar el equipo de internet.
- [ ] Cambiar contraseña principal.
- Otro: _

4. PASO 2: DOCUMENTAR (Guardar Pruebas)

- [ ] Tomar captura de pantalla.
- [ ] Guardar enlace (URL).
- [ ] Anotar fecha, hora y usuario.
- Otro: _

5. PASO 3: COMUNICAR (¿A quién llamamos?)

- **Círculo de Confianza Interno:**

- Nombre: _ _ _ _ _ _ _ _ Contacto: _ _ _ _ _ _ _ _
- Nombre: _ _ _ _ _ _ _ _ Contacto: _ _ _ _ _ _ _ _

- **Apoyo Externo (Aliados):**
  - Organización: _ _ _ _ _ _ _ _ Contacto: _ _ _ _ _ _ _ _
- **Autoridad Propia:**
  - Cargo: _ _ _ _ _ _ _ _ Contacto: _ _ _ _ _ _ _ _

6. PASO 4: ACCIÓN (¿Qué hacemos ahora?)

- [ ] Bloquear usuario/perfil.
- [ ] Reportar a la plataforma.
- [ ] Borrar publicación.
- [ ] Revisar configuración de privacidad.
- Otro: _

7. PASO 5: APRENDER (Lección para la próxima vez)
(Espacio para reflexión colectiva sobre cómo mejorar)

Los protocolos de respuesta a incidentes en el mundo corporativo o gubernamental son, por lo general, procedimientos técnicos y gerenciales enfocados en la eficiencia y la mitigación de daños a la organización.[53] Sin embargo, para una comunidad, un incidente digital, especialmente una amenaza o un ataque de desinformación, es un evento profundamente traumático. Genera miedo, siembra desconfianza y tiene el potencial de fracturar el tejido social y paralizar los procesos organizativos.

La respuesta, por lo tanto, no puede ser meramente técnica; debe ser también emocional, social y política. La necesidad de apoyo psicosocial es un componente explícito y vital en los protocolos de seguridad diseñados para periodistas y activistas, quienes enfrentan presiones similares.[44] En este sentido, la creación y práctica de un protocolo en un contexto comunitario debe enmarcarse no como un ejercicio burocrático, sino como un **ritual de cuidado y fortalecimiento colectivo**. La práctica regular del protocolo a través de simulacros no solo mejora la respuesta técnica, sino que, fundamentalmente, construye confianza, reduce el miedo al visibilizar la red de apoyo existente y reafirma los lazos de solidaridad. Cuando un incidente real ocurre, la comunidad no reacciona desde el pánico individual, sino desde una práctica compartida y ensayada. De esta manera, el protocolo se convierte en una manifestación tangible de la cohesión organizativa y la resiliencia del grupo, transformando una vulnerabilidad en una oportunidad para fortalecerse.

2.6 MÓDULO 6: EL ROL DEL FORMADOR COMUNITÁRIO: FACILITANDO EL SABER

Objetivo: Equipar a los nuevos formadores con las herramientas pedagógicas, metodológicas y de planificación necesarias para replicar exitosamente este currículo en sus propias comunidades, adaptándolo de manera creativa y pertinente a sus contextos específicos.

2.6.1 El Arte de Facilitar: Principios de la Educación para Adultos

Para que la réplica sea efectiva, los nuevos formadores deben dominar los principios de la andragogía (educación para adultos), que reconocen que los adultos aprenden de manera diferente a los niños.[2] Los principios clave a interiorizar son:

- **Partir de la Experiencia:** El aprendizaje más significativo para los adultos ocurre cuando el nuevo conocimiento se conecta directamente con su experiencia vital, profesional y comunitaria. El formador debe actuar como un puente entre la experiencia de los participantes y los nuevos conceptos.[3]
- **Aprendizaje Activo y Participativo:** Se debe superar el modelo de "presentación" o "charla magistral", donde el formador habla y los demás escuchan. Es crucial utilizar métodos activos que promuevan la discusión, la exploración conjunta, la resolución de problemas y el aprendizaje a través del hacer.[2]
- **Crear un Ambiente de Confianza y Respeto:** El rol del formador no es el de un experto que posee toda la verdad, sino el de un facilitador que guía un proceso de descubrimiento colectivo. Esto requiere actitudes de escucha activa, respeto por todas las opiniones, empatía y humildad para aprender también de los participantes.[4]

2.6.2 Planificando la Réplica: De la Idea a la Acción Formativa

Se guiará a los participantes a través de un ciclo de planificación completo, dotándolos de una hoja de ruta para organizar sus propios talleres.[3]

1. **Análisis de Necesidades:** El primer paso es preguntarse: ¿qué es lo más urgente y relevante para mi comunidad en este momento? ¿Necesitan enfocarse más en las herramientas de seguridad del Módulo 3 debido a amenazas recientes? ¿O es más prioritario entender la gobernanza de internet del Módulo 4 para incidir en un proyecto local?[2]
2. **Definición de Objetivos de Aprendizaje:** Con base en las necesidades, se

definen objetivos claros y alcanzables. ¿Qué quiero que los participantes sepan, sientan o puedan hacer al finalizar el taller?[5]

3. **Diseño y Adaptación de Actividades:** Se enseñará a no solo replicar las actividades de este currículo, sino a adaptarlas. ¿Las analogías usadas aquí funcionan en mi comunidad o debo crear otras? ¿Qué casos o ejemplos locales puedo usar para que los conceptos sean más cercanos? La contextualización es clave, especialmente en entornos rurales e indígenas.[60]
4. **Preparación de Materiales y Logística:** Se debe planificar con antelación los recursos necesarios. ¿Necesito imprimir las tablas y plantillas? ¿Tengo acceso a un proyector? ¿Cómo puedo facilitar el taller si no hay electricidad o conexión a internet?[61]
5. **Evaluación Participativa:** La evaluación no es un examen. Se enseñarán métodos sencillos y participativos para valorar si se cumplieron los objetivos, como rondas de palabra final, dibujos que representen lo aprendido, o pequeños sociodramas donde se apliquen los conocimientos.[58]

2.6.3 La Caja de Herramientas del Formador

Se proporcionará un conjunto de recursos y técnicas prácticas para la facilitación:

- **Técnicas de Dinamización:** Actividades "rompehielos" para iniciar, "energizantes" para momentos de cansancio, y técnicas para fomentar la discusión ordenada y productiva en grupos pequeños.[2]
- **Manejo de Grupos:** Estrategias para gestionar diferentes personalidades en un grupo: cómo moderar a un participante que habla demasiado, cómo motivar la participación de los más tímidos, y cómo mediar en posibles conflictos o desacuerdos.[4]
- **Adaptación de Contenidos:** Habilidades para simplificar lenguaje técnico, crear nuevas metáforas y analogías que resuenen con la cultura local, y contextualizar los ejemplos. Se hará hincapié en la importancia de adaptar los materiales a las particularidades de la ruralidad.[60]
- **Uso de Recursos Offline:** Se explorarán estrategias creativas para enseñar sobre tecnología sin depender de ella, utilizando herramientas como papelógrafos, tarjetas con conceptos, teatro del oprimido y otras dinámicas que no requieren conexión a internet ni dispositivos digitales.[61]

Actividad Práctica Final: "Mi Primer Taller"

Como culminación del proceso de formación, cada participante (o en pequeños grupos) tendrá la oportunidad de diseñar y facilitar una micro-sesión de 15 a 20 minutos sobre uno de los temas del currículo. Este ejercicio práctico les permitirá aplicar todo lo aprendido y

recibir retroalimentación constructiva de sus compañeros y del facilitador principal. Esta actividad funciona como un rito de paso, consolidando su confianza y su identidad como nuevos "Formadores de Formadores" comunitarios.

El modelo tradicional de Formación de Formadores a menudo se centra en la replicación fiel de un contenido predefinido.[3] Sin embargo, este enfoque es inadecuado para la vasta diversidad cultural, social y contextual de las comunidades indígenas y afrodescendientes en Colombia. Un currículo de "talla única" está destinado al fracaso. La investigación sobre educación mediada por tecnologías en contextos rurales e indígenas demuestra que la clave del éxito radica en la capacidad de contextualizar y adaptar las propuestas pedagógicas a cada realidad.[60] El rol del Asistente Docente Indígena (ADI) en algunos modelos educativos es, precisamente, el de ser un intérprete y puente cultural.[60]

El verdadero desafío para el nuevo Guardián Digital no será memorizar el contenido de este currículo, sino reinventarlo y adaptarlo creativamente a su comunidad. Por lo tanto, este módulo final debe redefinir su rol. No es un simple "replicador de contenidos", sino un **"traductor cultural"** y un **"tejedor de redes"**.

- Como **traductor cultural**, su habilidad más preciada será tomar los conceptos universales de ciberseguridad, derechos y gobernanza, y "traducirlos" al lenguaje, las metáforas, los valores y las lógicas de su propia gente. Su éxito dependerá de su creatividad pedagógica para hacer que el conocimiento sea pertinente y significativo.
- Como **tejedor de redes**, su labor no concluye al finalizar un taller. Su rol es mantener viva la conversación, conectar a los participantes de su comunidad con la red más amplia de Guardianes Digitales que se está formando en otras regiones, y servir de puente con las organizaciones aliadas. Su función es seguir fortaleciendo el tejido de cuidado digital a nivel local, territorial y nacional.

En definitiva, este currículo no solo busca entregar un conocimiento, sino iniciar y nutrir un movimiento de comunidades que se apropian críticamente de la tecnología para defender sus derechos y fortalecer su autonomía.

3- ACTUALIZACIÓN CONTINUA DEL CURRÍCULO PARA RESULTADOS EFECTIVOS

Se entiende que el currículo proporciona las bases necesarias para la enseñanza de la seguridad digital, la gobernanza de internet y los derechos digitales, abarcando las realidades de los pueblos indígenas, los afrodescendientes, las comunidades rurales y urbanas. Sin embargo, es importante destacar que quienes implementan el currículo deben actualizarlo para reflejar las realidades locales o regionales de donde se aplica el contenido, ya que puede haber pequeñas diferencias que requieran atención.

Como resultados efectivos de un currículo capaz de formar individuos para convertirse en formadores, esperamos generar un mayor empoderamiento de las comunidades en temas digitales, reduciendo los riesgos de inseguridad y enseñando a implementar nuevas herramientas para ser desarrolladas en cursos, capacitaciones u otros espacios de formación.

4- MÉTODOS DE EVALUACIÓN Y MEDICIÓN DE IMPACTO

Para garantizar la eficacia del currículo y su posibilidad de medición, se propone que del comienzo al final se hagan mediciones de la aplicabilidad del contenido y del uso de los conocimientos propuestos. En relación al impacto, con la evaluación de nível de seguridad y conocimiento, es posible mensurar cuales materiales del currículo y curso serán más impactantes.

4.1 MÉTODOS DE EVALUACIÓN

Para evaluar el currículo se propone la realización de reuniones en línea con expertos (en el tema de seguridad digital, gobernanza de internet y de la realidad de las comunidades locales) y personas interesadas/ estudiantes. A través de este método se permite identificar las necesidades específicas y las expectativas. Se aplicará mediante encuestas iniciales, entrevistas breves o ejercicios prácticos de diagnóstico, lo que facilita ajustar los contenidos a la realidad del grupo esperado para la formación de formadores que utilizará este currículo posteriormente

Además, también se propone como método una evaluación formativa. Durante la formación y utilización del currículo, será realizada de manera continua en cada módulo a través de actividades y ejercicios en formularios donde tanto se mensurara el conocimiento, como la pertinencia de contenidos. Su función es retroalimentar tanto al formador como a los

participantes, ajustando el ritmo y las metodologías para maximizar el aprendizaje.

4.1.1 Guía para reuniones

Las reuniones tienen como propósito crear un espacio participativo y seguro en el que expertos, o expertos y estudiantes puedan intercambiar percepciones sobre el currículo, identificar aciertos, detectar vacíos y proponer mejoras. Se recomienda que estas reuniones se realicen en diferentes momentos del proceso (al inicio, a mitad y al final), de manera que permitan medir la evolución del aprendizaje y la pertinencia cultural de los contenidos. Para orientar la conversación, se proponen usar preguntas guía como:

- ¿Qué partes del currículo pueden mejorar? ¿Qué contenidos faltan?
- ¿Existen temas que deberían explicarse con mayor profundidad o ejemplos más cercanos a la realidad local?
- ¿Los conceptos técnicos y étnicos están adecuados? Hay que adaptar o cambiar algo para que sea más eficaz y aplicable?
- ¿Qué tan fácil y claro es para aplicar los conocimientos adquiridos en la vida comunitaria cotidiana?
- ¿Qué mejoras se podrían implementar para fortalecer el currículo?

Es importante que las reuniones sean moderadas con metodologías participativas (círculo de palabra, lluvia de ideas, priorización colectiva), de manera que todas las voces sean escuchadas y que las respuestas recolectadas se puedan documentar sistemáticamente para alimentar los informes de evaluación y retroalimentación del programa.

4.1.2 Preguntas clave para formulários

Los formularios de evaluación permiten recopilar información sistemática y comparable sobre el proceso de formación. Se recomienda que sean breves, accesibles y aplicados en distintos momentos (diagnóstico inicial, durante cada módulo y al final del proceso). Las preguntas deben enfocarse tanto en el nivel de conocimiento como en la pertinencia y aplicabilidad de los contenidos. Algunos ejemplos de preguntas clave son:

- ¿Qué nivel de conocimiento previo tiene sobre seguridad digital y gobernanza de internet?
- ¿Cuáles son sus expectativas principales respecto a esta formación?
- ¿Qué tan útil considera el contenido del módulo trabajado para su comunidad?
- ¿Qué temas le resultaron más difíciles o menos claros?
- ¿Tiene alguna sugerencia, comentario o pregunta sobre los módulos?
- ¿Cómo pretendes implementar los aprendizajes de este curso como formador/ facilitador comunitario?
- ¿Crees que los conocimientos adquiridos en el curso, los puedes aplicar en la práctica en tu vida diaria comunitaria?
- ¿Tienes alguna sugerencia sobre algún tema que deba incluirse en el curso?
- ¿Cómo califica su satisfacción con el curso?
- ¿Tiene alguna sugerencia, comentario o pregunta sobre el curso/ currículo?

Lo importante es que sus resultados sean analizados de manera conjunta por el equipo de coordinación para retroalimentar la metodología y medir el impacto real del currículo en el fortalecimiento de capacidades comunitarias.

4.1.3 Taller virtual de mapeo de riesgos de seguridad digital

Como herramienta para futuros aplicadores (especialmente para OSC que trabajan con pueblos indígenas y afrodescendientes en Colombia) del currículo que deseen validar el currículo y sus informaciones también se deja como sugerencia un tercer método posible que se realiza a través de un taller en el formato visualizado abajo.

TALLER VIRTUAL DE MAPEO DE RIESGOS DE SEGURIDAD DIGITAL (90 MINUTOS)

El objetivo del taller es descubrir y priorizar los riesgos (no las soluciones): *activo/valor* + *amenaza/actor* + *condición/vulnerabilidad* + *consecuencia*. Esta estructura está alineada con marcos de evaluación de riesgos ampliamente usados en OSC

0) PREPARACIÓN (ANTES DE LA SESIÓN)

- **Convocatoria y consentimiento** (sin grabación, seudónimos permitidos).

- **Plan de conectividad baja:** audio primero; pizarra → Google Sheets/Forms; canal de respaldo por WhatsApp.
- **Roles:** facilitación, co-facilitación/relatoría, soporte técnico, intérprete(s) si aplica (lengua indígena).
- **Enfoque intercultural:** si se tocan **conocimientos/archivos sensibles**, solo nombrar categorías ("canto ritual", "mapa sagrado") sin detalles salvo autorización comunitaria.

1) LA SESIÓN (CON CONECTIVIDAD)

A. Apertura segura y reglas (5')

- Acordar: no grabar; usar seudónimos si alguien lo prefiere; respeto intercultural.
- Consulta de calidad de conectividad por chat: 🟢 / 🟠 / 🔴.
- **Modo baja conectividad:** respuestas por audio; relator anota en Sheet.

B. Descubrimiento de activos y flujos (15')

Disparador amplio: "Imagina que mañana aparece en internet información interna de la organización (listas de contactos, fotos de reuniones, planes de incidencia, actas de asamblea). ¿Qué sería *más grave* que se haga público o se pierda?"

Preguntas concisas:

- ¿Qué cosas serían críticas si se pierden o publican?
- ¿Dónde "viven" esa información hoy (teléfono propio/OSC, USB, nube, computador)?
- ¿Quién las usa y con quién se comparten (roles, no nombres)?
  Captura (relator): tabla *Activo – Ubicación – Quién usa – Con quién se comparte* + **impacto preliminar**(Alto/Medio/Bajo).

C. Contexto y actores (10')

Disparador: “En temporada de consulta/elecciones, aparecen cuentas nuevas que atacan a la comunidad; también hay intereses extractivos cercanos.”

Preguntas: ¿Qué coyunturas tensas hay? ¿Quién podría querer frenar su trabajo o mirar sus datos (aliado/neutral/posible agresor)?

Captura: *Actor – Motivación – Capacidad (B/M/A) – Activo que le interesa*.

Objetivo: mapear amenazas plausibles para el cálculo de **probabilidad**.

D. Incidentes y señales (15’)

Casos en lenguaje simple (elegir 3):

- *Engaño por mensaje/correo*: “parece de una entidad, pide “verificar clave” con un enlace”.
- *Archivo que enferma el equipo*: “abrí ‘lista.xls’ y el equipo se puso lento/aparecieron ventanas raras”.
- *Suplantación*: “perfil con foto del líder pidió dinero/datos”.
- *Doxxing/escarnio*: “publicaron teléfono/dirección de alguien”.
- *Corte de señal o revisión de celular* el día de una asamblea.

Preguntas: ¿Pasó algo parecido? **Sí/No/No sé**. ¿Cuándo? (≤3m / 3–12 / >12). ¿A qué afectó (personas, reputación, archivos, actividad)?

Captura: *Evento – Fecha – Canal – Activo – Consecuencia*.

Fundamento: priorizar por recencia y frecuencia.

E. Cuentas llave y dependencias (10’)

Explicación simple (1’): *Cuentas llave* = llaves maestras que abren sistemas críticos. Ejemplos:

- **Correo institucional** (admin que crea o borra cuentas).
- **Redes sociales** (propietario de la página/perfil).

- **Dominio y hosting** del sitio web (quien paga/renueva).
- **Nube de archivos** (quien puede invitar/expulsar).
- **Banca/donaciones** (acceso a movimientos).

Preguntas: ¿Cuáles existen? ¿Quién tiene la llave? ¿Hay copia o recuperación? ¿Alguna depende de un solo equipo o persona?

Captura: lista *Recurso crítico – Quién tiene la llave (rol) – ¿Backup/recuperación? – Dependencia única (Sí/No)*.

Objetivo: reducir puntos únicos de falla en el análisis.

F. Exposición pública y temas controvertidos (10')

Disparador: "Una publicación sobre tierras/medio ambiente generó cientos de comentarios hostiles y mensajes privados agresivos."

Preguntas: ¿Qué canales públicos usan (web, Facebook, TikTok, radios)? ¿Qué temas detonan ataques? ¿Perfiles falsos recientes?

Captura: lista de **canales calientes** con fecha/tema.

Objetivo: Insumos para riesgos reputacionales/legales y de suplantación.

G. Priorización (20')

Metodología: esquema probabilidad×impacto usado en evaluaciones organizacionales.

- El relator convierte respuestas en **enunciados de riesgo**:
  "Existe el riesgo de **[amenaza/actor]** contra **[activo]** por **[condición]**, con **[consecuencia]**."
- Votación rápida (chat): cada persona marca 3 riesgos que considera **más probables** y 3 con **mayor impacto en personas/cultura/operación**.

- El equipo de facilitación cruza votos y **recencia** de incidentes para armar un **Top-10**.

H. Cierre (5')

- Revisión del Top-10 (solo lectura).
- Explicar qué pasará con los datos (custodia/anonimización).
- Recordatorio de **canales de ayuda** (helplines y recursos).

3) MODO BAJA CONECTIVIDAD

Considerando el escenario donde hay muchas personas, comunidades y organizaciones con baja conectividad, proponemos maneras distintas para ejecutar la sesión:

- **Video opcional;** solo audio si hay cortes.
- **Pizarra → Google Sheets** (pestañas: *Activos, Actores, Incidentes, Cuentas llave, Riesgos*).
- **Respuestas por WhatsApp** con códigos cortos

4) PRODUCTOS Y RESULTADOS

Como productos que salen de esta sesión (en ambos modos - con conectividad o baja conectividad):

- Identificación de necesidades específicas (a través de: Matriz de riesgos, Registro de incidentes de los últimos 12–18 meses, Top-10 de riesgos priorizados);
- Retroalimentación del currículo (a través de: Mapa de actores - motivación/capacidad, listado de cuentas llave y dependencias únicas).

4.2 EVALUACIÓN DE IMPACTO

Esa evaluación es una búsqueda para medir si el currículo genera cambios sostenibles en la práctica comunitaria. Se aplicará mediante el seguimiento de indicadores como:

- Número de documentos, plantillas o modelos creados;
- Número de reuniones y formaciones para comunidades;
- Adopción de protocolos colectivos de seguridad digital.
- Casos de incidencia comunitaria en gobernanza de internet.
- Percepción de mayor seguridad y autonomía digital por parte de los participantes.

Con este enfoque, la evaluación no se limita a medir resultados individuales, sino que se convierte en un proceso participativo, transparente y orientado a fortalecer la autonomía digital de las comunidades.

REFERENCIAS

1. La triple barrera para reducir brechas digitales para pueblos indígenas - ¿Y si hablamos de igualdad?, https://blogs.iadb.org/igualdad/es/brechas-digitales-pueblos-indigenas/
2. Formación para Formadores (FpF) Metodología de formación, https://ec.europa.eu/programmes/erasmus-plus/project-result-content/cb5685ff-4c8a-4ae0-8d3f-dfee5c3dc3fe/AgriSafetyNet_Training_Methodology_IO3_ES.pdf
3. FORMACION DE FORMADORES - OIT/Cinterfor, https://www.cinterfor.org/sites/default/files/file_publicacion/manual_seg.pdf
4. formación de formadores, http://www.halinco.de/html/proy-es/mat_did_1/form_form.htm
5. Formación de Formadores - OCW, https://ocw.ehu.eus/pluginfile.php/47292/mod_resource/content/1/Guia_Docente.pdf
6. Redalyc.La Educación Popular: Una construcción colectiva desde el Sur y desde abajo, https://www.redalyc.org/pdf/2750/275031898079.pdf
7. Educación popular: una mirada de conjunto - Info CDMX, https://infocdmx.org.mx/escuela/curso_capacitadores/educacion_popular/decisio10_saber1.pdf
8. INVESTIGACIÓN-ACCIÓN Y EDUCACIÓN POPULAR - Biblioteca Hegoa, https://biblioteca.hegoa.ehu.eus/downloads/21409/%2Fsystem%2Fpdf%2F4576%2FM-7054.pdf
9. La Educación Popular en las luchas por los ... - DVV International, https://www.dvv-international.de/es/educacion-de-adultos-y-desarrollo/ediciones/ead-72-2009/contribuciones/la-educacion-popular-en-las-luchas-por-los-derechos-humanos-en-america-latina
10. LA EDUCACIÓN POPULAR EN EL SIGLO XXI. UNA RESISTENCIA INTERCULTURAL DESDE EL SUR Y DESDE ABAJO - SciELO Colombia, http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S2216-01592015000200006
11. A través de 19 Comunidades de Conectividad – Juntas de Internet se conectarán los hogares más apartados de Vaupés - MinTIC, https://www.mintic.gov.co/portal/715/w3-article-397578.html
12. Informe al Congreso MinTIC 2023 – 2024 - Camara de Representantes, https://www.camara.gov.co/sites/default/files/2024-11/INF-DE-GESTION-MIN-TIC.pdf
13. Latin America in a glimpse Amazonía - Derechos Digitales, https://www.derechosdigitales.org/wp-content/uploads/DD_Amazonia_3_Colombia.pdf
14. Internet a cuentagotas: brecha digital de los pueblos indígenas en ..., https://www.dejusticia.org/acceso-a-internet-en-la-amazonia/
15. ENTRE DESCONEXIONES Y RIESGOS: ENTRE ..., https://web.karisma.org.co/wp-content/uploads/2024/12/Informe-seguridad-digital-k-lab.pdf

16. Riesgos digitales a los que se exponen los niños y cómo prevenirlos - ICBF, https://www.icbf.gov.co/ser-papas/riesgos-digitales-los-que-se-exponen-los-ninos-y-como-prevenirlos
17. Jóvenes colombianos luchan por una educación digital sin barreras sociales ni raciales para los estudiantes indígenas | Noticias ONU - UN News, https://news.un.org/es/story/2021/02/1487982
18. impactok23.pdf - Fundación Karisma, https://web.karisma.org.co/wp-content/uploads/2024/10/impactok23.pdf
19. La gobernanza de internet como plataforma para impulsar políticas en la educación con TIC. El caso de Colombia | Opera, https://revistas.uexternado.edu.co/index.php/opera/article/view/5127/6819
20. Gobernanza - Dominio .CO - MinTIC, https://gobernanzadeinternet.mintic.gov.co/752/w3-propertyvalue-198152.html
21. Digital Inclusion and Internet Content Governance - Organization of American States, https://www.oas.org/en/iachr/expression/reports/Digital_inclusion_eng.pdf
22. Informe Inclusión digital y gobernanza de contenidos en internet - Organization of American States, https://www.oas.org/es/cidh/expresion/informes/Inclusion_digital_esp.pdf
23. ¿Qué derechos digitales existen y cuál es su importancia? - Universidad Europea, https://colombia.universidadeuropea.com/blog/derechos-digitales/
24. Salud Digital y Derechos Digitales en Colombia - COLEV - Universidad de los Andes, https://colev.uniandes.edu.co/images/documentos/IP-DRAG-ESP-Colombia-FINAL.pdf
25. Los derechos digitales en Colombia: ¿cuáles son y cómo se regulan?, https://colombia.unir.net/actualidad-unir/derechos-digitales/
26. Desinformación y violencia en línea afectan la conversación pública en Colombia - Publicaciones y otras publicaciones | FLIP, https://flip.org.co/publicaciones/otras-publicaciones?item=desinformacion-y-violencia-en-linea-afectan-la-conversacion-publica-en-colombia
27. Índice | El Índice Derechos Digitales es una alianza de organizaciones de la sociedad civil que trabajan temáticas relacionadas con los derechos humanos en entornos digitales. El Índice pretende catalizar las actividades de sus integrantes y servir como espacio de comunicación sobre cuestiones urgentes para el ejercicio de esos derechos en Colombia., https://indicederechos.digital/
28. Moderación de contenidos y partes interesadas locales en Colombia | Article 19, https://www.article19.org/wp-content/uploads/2024/05/v.2_ESPANOL_Content_Moderation_and_Local_Stakeholders_in_Colombia.pdf
29. Ley sancionada en Colombia busca proteger a los menores de edad de los peligros de la internet: estas son las nuevas medidas, https://www.infobae.com/colombia/2025/07/23/fue-sancionada-ley-de-entornos-digitales-sanos-que-busca-proteger-a-los-menores-de-edad-en-internet/
30. Nuevo desorden mundial: ataques digitales a la libertad de reunión pacífica y asociación,

https://www.accessnow.org/press-release/nuevo-desorden-mundial-ataques-digitales-a-la-libertad-de-reunion-pacifica-y-asociacion/

31. Entre desconexiones y riesgos: seguridad digital para las personas ..., https://web.karisma.org.co/entre-desconexiones-y-riesgos-seguridad-digital-para-las-personas-defensoras-de-derechos-humanos-en-colombia/
32. Publicaciones y otras publicaciones | FLIP, https://flip.org.co/publicaciones/informes
33. Property:Existing toolkits and resources, https://gendersec.tacticaltech.org/wiki/index.php?title=Property:Existing_toolkits_and_resources&until=Taller+de+cartograf%C3%ADa+y+seguridad+digital+dirigido+a+mujeres%2C+Oaxaca%2C+Mexico
34. Visualizar Información para la Incidencia - SocialTIC, https://socialtic.org/wp-content/uploads/2017/06/VIFA_Espan%CC%83ol_Digital.pdf
35. Seguridad-Digital-Conceptos-y-Herramientas-Básicas-Mayo-2020.pdf - Conexo, https://conexo.org/wp-content/uploads/2020/06/Seguridad-Digital-Conceptos-y-Herramientas-B%C3%A1sicas-Mayo-2020.pdf
36. Guía de seguridad digital para todos - CAMECO, https://www.cameco.org/media/es_gu_a_de_seguridad_digital_para_todos-_cameco.pdf
37. GUIA DE APOYO - UNODC, https://www.unodc.org/documents/Cybercrime/tools-and-resources/guia_de_apoyo_docentes_sp.pdf
38. 6 tipos de protocolos de seguridad de red - Check Point Software, https://www.checkpoint.com/es/cyber-hub/network-security/what-is-network-security/6-types-of-network-security-protocols/
39. Herramientas de seguridad digital | Puntal - ONU-DH, https://hchr.org.mx/puntal/prevencion-y-proteccion/prevencion/seguridad-y-prevencion-de-riesgos/herramientas-de-seguridad-digital/
40. Plataforma de Recursos de Seguridad Digital - Amnistía Internacional Security Lab, https://securitylab.amnesty.org/es/digital-resources/
41. Digital Security Resource Hub for Civil Society - Amnesty International Security Lab, https://securitylab.amnesty.org/digital-resources/
42. ¿Qué necesitas proteger?, https://securityinabox.org/es/
43. Top 5 apps de seguridad para proteger tus datos en 2025, https://preyproject.com/es/blog/5-aplicaciones-para-mejorar-la-seguridad-de-datos-y-dispositivos
44. Protocolos de Seguridad para Periodistas - International Center for ..., https://www.icfj.org/sites/default/files/2022-12/PROTOCOLOS%20DE%20SEGURIDAD%20%28Final%2010-29-2022%29.pdf
45. Tercer informe de Gobernanza de Internet en Colombia - Comisión de Regulación de Comunicaciones, https://crcom.gov.co/es/biblioteca-virtual/tercer-informe-gobernanza-internet-en-colombia
46. Apoyo a iniciativas de Gobernanza de Internet en América Latina y el Caribe - LACNIC, https://www.lacnic.net/7101/1/lacnic/gobernanza-de-internet

47. Colombia | Global Information Society Watch, https://www.giswatch.org/en/country-report/internet-governance/colombian-bureau-internet-governance
48. Reunión Mesa Colombiana de Gobernanza de Internet - - ISOC, Colombia, https://www.isoc.co/es/noticias/reunion-mesa-colombiana-de-gobernanza-de-internet
49. Fortaleciendo los pueblos afrocolombianos e indígenas en Colombia - Latin America Leadership Program, https://lalp.georgetown.edu/es/news/strengthening-afro-colombian-and-indigenous-peoples-in-colombia
50. Foro de gobernanza de internet de América Latina y el Caribe ¿A qué retos se enfrenta la región? | Asociación para el Progreso de las Comunicaciones, https://www.apc.org/es/news/foro-de-gobernanza-de-internet-de-america-latina-y-el-caribe-que-retos-se-enfrenta-la-region
51. Foro de Gobernanza de Internet de América Latina y el Caribe (LACIGF) en Santiago, Chile, https://datosprotegidos.org/lacigf-stgo-chile/
52. Foro regional de Gobernanza de internet - LACIGF 2023 - Universidad Externado, https://www.uexternado.edu.co/departamento-de-derecho-de-los-negocios/foro-regional-de-gobernanza-de-internet-lacigf-2023/
53. ¿Qué es la respuesta a incidentes? - IBM, https://www.ibm.com/mx-es/topics/incident-response
54. ¿Qué es la respuesta a incidentes? - IBM, https://www.ibm.com/es-es/topics/incident-response
55. Guía: Seguridad digital para las personas defensoras de la Tierra ..., https://www.earthdefenderstoolkit.com/kit-de-herramientas/seguridad-digital-para-las-personas-defensoras/?lang=es
56. Respuesta a incidentes | INCIBE-CERT, https://www.incibe.es/incibe-cert/incidentes/respuesta-incidentes
57. Guía de respuesta a incidentes - CISA, https://www.cisa.gov/sites/default/files/2024-05/WWS-Sector_Incident-Response-Guide_ES.pdf
58. Qué es la formación de formadores y cuáles son sus principales aportes a la educación profesional - Universidad ORT Uruguay, https://ie.ort.edu.uy/blog/que-es-la-formacion-de-formadores-y-cuales-son-sus-principales-aportes-a-la-educacion-profesional
59. La formación de formadores. Pertinencia de los procesos dialógicos, recursivos y subyacentes - SciELO México, https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2448-84372017000100088
60. Secundarias Rurales Mediadas por Tecnolog´Ias en ... - Unicef, https://www.unicef.org/argentina/media/10721/file/Secundarias%20Rurales%20Mediadas%20por%20Tecnolog%C3%ADas%20en%20la%20Argentina.pdf
61. Las 4 “C”: Principios para una integración tecnológica en escuelas rurales, https://es.fabretto.org/las-cuatro-c-integracion-tecnologica/

62. Educación rural mediada por tecnología tradicional en tiempos de pandemia 2020-2022 | Entre Ciencia e Ingeniería - Portal de Revistas UCP, https://revistas.ucp.edu.co/index.php/entrecienciaeingenieria/article/view/2778
63. Educación rural mediada por tecnología tradicional en tiempos de pandemia 2020-2022, http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1909-83672022000100051