La brecha digital y los riesgos cibernéticos en comunidades indígenas en el Municipio de San José del Fragua en el Caquetá: Análisis de vulnerabilidades y propuestas de resiliencia.

Estudiantes:

Jackson Apraez Soto

Mario Jorge Álvarez Daza

Director:

Eduard Antonio Mantilla Torres

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Maestría en Ciberseguridad

Florencia 2026

Dedicatorias

Doy gracias a Dios por continuar mis estudios como futuro Magister, agradecimiento total a mi Madre y Hermano, gracias a sus consejos y apoyo recibido durante mi formación profesional, Mis hijos que son mi motivación e inspiración de mis logros y mis metas. Me siento orgulloso me llena de satisfacción recibir la herencia más valiosa que puedo heredar. (Jackson Apraez Soto).

A Dios, por brindarme la valentía, el entendimiento y la paciencia en cada etapa de este recorrido. A mi esposa, por ser mi compañera de vida, mi refugio en los días difíciles y mi fuerza en los momentos de duda. Gracias por tu paciencia, tu amor incondicional y por creer en mí cuando más lo necesitaba. Sin tu apoyo, este logro no habría sido posible. A mis hijos, quienes son mi mayor inspiración. Cada paso que doy, cada meta que alcanzo es por y para ustedes. Este logro también les pertenece, porque son el motor que me impulsa a superarme día a día. A mis padres, por su amor sin reservas, su respaldo incesante y por instruirme que el esfuerzo y la humildad pueden abrir caminos que el talento por sí mismo no puede. A mis profesores y mentores, quienes con su orientación y sabiduría me impulsaron a superar lo académico y a descubrir entusiasmo en lo que realizo. (Mario Jorge Alvarez Daza).

Agradecemos a los directores y tutores de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de aprender y enriquecer nuestros conocimientos a nivel profesional, por otro lado, a los directivos, asesores y compañeros de aprendizaje que me acompañaron en este largo proceso, reconozco sin duda alguna que sin su apoyo y colaboración éste logro no hubiera sido posible.

Agradecimientos

Este proyecto lo dedicamos a nuestras familias, padres, esposas e hijos, que han sido de gran apoyo incondicional en esta ruta de sacrificio de días enteros y noches de mucho esfuerzo, son la fuente de motivación e inspiración para continuar con nuestra preparación profesional, nuestros diferentes tutores también ha sido un apoyo muy importante, siempre hemos contado con el apoyo incondicional de ánimo que reconforta y da fuerzas para seguir adelante para poder entregar las actividades exigidas a tiempo.

Resumen

La expansión de los medios de comunicación, el desarrollo de nuevos recursos informáticos, la implementación de infraestructuras con tecnologías avanzadas y el uso creciente de dispositivos digitales inteligentes han aumentado el riesgo de exclusión en poblaciones vulnerables, como las comunidades indígenas. Estas comunidades enfrentan barreras estructurales, culturales y tecnológicas que limitan significativamente su apropiación digital. Este estudio tiene como objetivo analizar la brecha digital y los riesgos cibernéticos que enfrenta el pueblo Inga, asentado en el municipio de San José del Fragua, Caquetá, y proponer estrategias que fortalezcan su resiliencia digital mediante la adopción de prácticas de ciberseguridad contextualizadas culturalmente. Se aplica una metodología de enfoque mixto, combinando un análisis cuantitativo mediante encuestas estructuradas dirigidas a jóvenes estudiantes y miembros de la comunidad con un análisis cualitativo basado en observaciones directas y entrevistas semiestructuradas. Los resultados evidencian bajos niveles de alfabetización digital, acceso restringido a las tecnologías de la información y escaso conocimiento en ciberseguridad, factores que aumentan su vulnerabilidad frente a los riesgos informáticos. Como respuesta, se propone un programa de formación en competencias digitales y seguridad informática adaptado a su realidad sociocultural, orientado a mejorar el conocimiento, la percepción y las prácticas digitales seguras. El estudio establece que es necesario formular políticas públicas con enfoque intercultural que promuevan la inclusión digital y la ciberseguridad comunitaria, como una vía para avanzar hacia el cumplimiento de los Objetivos de Desarrollo Sostenible en entornos rurales e indígenas.

Palabras clave: Brecha digital, ciberseguridad, comunidades indígenas, inclusión digital.

Abstract

The expansion of media, the development of new IT resources, the implementation of infrastructures with advanced technologies, and the increasing use of smart digital devices have heightened the risk of exclusion for vulnerable populations, such as Indigenous communities. These communities face structural, cultural, and technological barriers that significantly hinder their digital inclusion. This study aims to analyze the digital divide and the cyber risks faced by the Inga people, located in the municipality of San José del Fragua, Caquetá, and to propose strategies that strengthen their digital resilience through the adoption of culturally contextualized cybersecurity practices. A mixed-methods approach is applied, combining a quantitative analysis through structured surveys targeting young students and community members, with a qualitative analysis based on direct observations and semi-structured interviews. The results show low levels of digital literacy, limited access to information technologies, and scarce knowledge in cybersecurity—factors that increase their vulnerability to cyber threats. In response, a training program is proposed, focused on digital and cybersecurity skills tailored to their sociocultural context, aimed at improving knowledge, perception, and safe digital practices. The study concludes that it is essential to formulate intercultural public policies that promote digital inclusion and community-based cybersecurity as a means to advance the achievement of the Sustainable Development Goals in rural and Indigenous environments.

Keywords: *Cybersecurity, digital divide, digital inclusion, Indigenous communities*

Tabla de contenido

Lista de Tablas

Lista de Figuras

Glosario

Amenaza cibernética: circunstancia o individuo que tiene el potencial de dañar un sistema mediante la denegación de servicio, el robo, la destrucción, la divulgación o la alteración de datos.

Antivirus: Software o programa utilizado para identificar, prevenir y deshacerse de cualquier amenaza detectada de código dañino (virus informáticos).

Autenticación: se refiere a las medidas de seguridad que permiten identificar al usuario que quiere acceder a un sistema. Evita que la identidad sea sustituida.

Brecha digital: es la desigualdad en el acceso, uso, o impacto de las Tecnologías de la Información y la Comunicación (TIC). Afecta a grupos sociales diferenciados por criterios como la edad, el género, la cultura, la ubicación geográfica o el nivel económico.

CIS (Centro de Seguridad en Internet): son un conjunto de prácticas recomendadas reconocidas y consensuadas a nivel mundial para ayudar a los profesionales de la seguridad a aplicar y administrar las medidas de seguridad cibernética.

Educación digital: puede definirse como una formación ofrecida a individuos que están geográficamente dispersos o separados o que interactúan en tiempos diferidos del docente empleando los recursos telemáticos.

Hacking ético: serie de pruebas o test conocidos como "pruebas de penetración" cuyo objetivo es superar las numerosas brechas de seguridad que tiene la red de una organización para demostrar su eficacia o, por el contrario, poner de manifiesto la vulnerabilidad del sistema.

Hackers: persona con amplios conocimientos para explotar las redes de información con fines económicos o personales.

Resiliencia cibernética: es la capacidad de una organización para identificar, responder y recuperarse rápidamente de un incidente de seguridad informática.

Riesgo: posibilidad de que una amenaza específica dañe o pierda el control de un activo de información aprovechando una vulnerabilidad.

Virus informático: programa malicioso que puede dañar el ordenador o interferir en su funcionamiento habitual, provocando la pérdida de información.

Vulnerabilidad: Una debilidad en un sistema informático (o grupo de sistemas) que compromete su integridad, confidencialidad o disponibilidad se conoce como vulnerabilidad.

Introducción

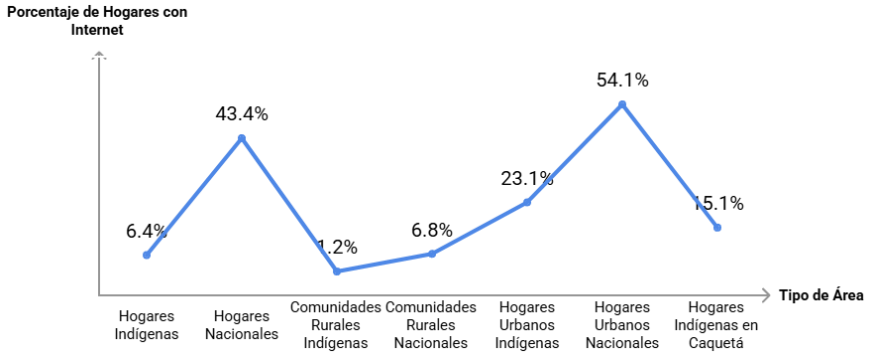
Este estudio se enfoca en el departamento de Caquetá, donde residen aproximadamente 8.825 personas indígenas, entre ellas miembros del pueblo Inga, asentados especialmente en el municipio de San José del Fragua. Esta comunidad indígena en específico es descendiente de los Incas, tiene su origen principal en el Valle del Sibundoy (Putumayo) y pertenece a la familia lingüística quechua, hablando el idioma Ingano. Según el censo (DANE, La información del DANE, 2022), 19.561 personas indígenas se auto reconocen como pueblo Inga, distribuidas en Putumayo, Nariño, Cauca y Caquetá. Culturalmente, los Inga comparten elementos con el pueblo Camëntsá, aunque se diferencian por su tradición viajera y espíritu comercial. Son ampliamente reconocidos como médicos tradicionales, con profundo conocimiento de las plantas y del uso ceremonial del yagé, planta sagrada a través de la cual los chamanes establecen contacto con el mundo espiritual. Su organización familiar gira en torno al fogón, y sus viviendas suelen ser rurales y de tipo campesino.

Su economía se basa en la agricultura (maíz, fríjol, papa, hortalizas y frutales), la ganadería y el comercio de productos como la leche. Muchos miembros del pueblo Inga se movilizan a distintas regiones del país para establecer redes comerciales, sin perder su conexión con el territorio ancestral al que retornan periódicamente. Pese a su riqueza cultural y conocimientos ancestrales, esta población enfrenta profundas brechas en ámbitos como educación, salud, empleo, acceso a tecnologías digitales y condiciones de vida digna. La limitada infraestructura tecnológica y la baja cobertura de Internet agravan estas desigualdades, restringiendo el acceso a información, servicios básicos y oportunidades de desarrollo.

El Censo Nacional de Población y Vivienda (CNPV, 2018), muestra una marcada brecha digital en las comunidades indígenas. En la figura 1 se puede observar cómo solo el 6,4% de las

viviendas indígenas tienen acceso a Internet, en contraste con el 43,4% del total nacional. Esta disparidad es aún más pronunciada en las áreas rurales, donde la cobertura en comunidades indígenas es de apenas 1,2%, frente al 6,8% del total nacional. En cabeceras municipales, la diferencia sigue siendo significativa: el 23,1% de los hogares indígenas tienen acceso a Internet, mientras que en el total nacional la cifra asciende al 54,1%. Para el departamento de Caquetá, la cobertura alcanza un 15,1%, una cifra moderadamente superior en comparación con regiones como Vaupés, Chocó y Vichada, donde la conectividad indígena es inferior al 6%. Estos datos evidencian que las comunidades indígenas, al enfrentar una brecha digital significativa, son particularmente vulnerables a los riesgos informáticos. La falta de acceso a infraestructura tecnológica, formación en ciberseguridad y herramientas de protección digital las expone a fraudes en línea, robo de identidad y desinformación, lo que impacta su seguridad y confianza en el uso de las TIC.

Fig. 2. *Descripción basada en el Censo Nacional de Población y Vivienda (CNPV) 2018.*



Tomado https://microdatos.dane.gov.co/index.php/catalog/643/

La figura 1 muestra los porcentajes de hogares indígenas con acceso o cobertura de Internet, evidenciando las marcadas desigualdades en conectividad en estas comunidades.

La falta de medidas adecuadas de ciberseguridad expone a las comunidades indígenas a riesgos significativos, comprometiendo la integridad de su información cultural, económica y

personal, así como su autonomía y sus derechos digitales. Sin estrategias de protección eficaces, estas poblaciones permanecen vulnerables ante fenómenos como la explotación digital y la exclusión en un entorno global cada vez más interconectado. En este contexto, se hace necesario diseñar estrategias orientadas a reducir la brecha digital en las comunidades indígenas, especialmente en zonas rurales, donde el acceso a Internet continúa siendo un desafío crítico para el desarrollo social y económico. Asimismo, es preciso evaluar las vulnerabilidades asociadas a esta brecha en el pueblo Inga, ubicado en el municipio de San José del Fragua, departamento del Caquetá, frente a los riesgos cibernéticos. Esto con el fin de formular propuestas de resiliencia que promuevan una inclusión tecnológica efectiva y fortalezcan la seguridad digital de estas comunidades, considerando sus realidades culturales y sociales específicas.

Planteamiento del Problema

Las comunidades indígenas del departamento del Caquetá, se enfrenta a diversos desafíos derivados de la creciente demanda en la era digital, la situación de la brecha digital es complicada e influye en el progreso social y económico del Municipio de San José del Fragua, los intentos de optimizar la conectividad a distintas comunidades indígenas de la región, se continúa lidiando con retos enormes vinculados al acceso a la tecnología por medio de la educación digital, dejando limitada las posibilidades de acceder a herramientas tecnológicas y expuestos de ataques cibernéticos.

La brecha digital en las comunidades indígenas es una problemática global a nivel mundial, a menudo enfrentan un sin número de obstáculos como el acceso a la internet, infraestructura tecnológica, economías no sostenibles, educación digital y la integridad cultural. Esta brecha no solo reduce el acceso a la información y a servicios públicos esenciales, sino que además limita las oportunidades de desarrollo educativo y laboral (González, 2021).

El Municipio de San José del Fragua, región distinguida por su diversidad cultural y ecoturística Amazónica, actualmente cuentan con infraestructura y dispositivos tecnológicos obsoletos, dificultando el acceso a Internet y quedando más vulnerables a los riesgos cibernéticos, aunque también por su inequidad económica, la conectividad a internet es baja, lo que obstaculiza a la comunidad indígena a involucrarse de manera integral en el desarrollo de la educación digital.

A pesar del aumento en la disponibilidad de tecnología digital, muchos indígenas de la población aún enfrentan barreras para acceder a estas, factores como la falta de infraestructura de conectividad, la escasez de dispositivos accesibles y la carencia de habilidades digitales adecuadas crean una brecha digital que excluye a ciertos segmentos de la comunidad, especialmente a aquellos en situación de vulnerabilidad económica o social.

Como parte de la estrategia e implementación de la política de gobierno digital y sus principios de innovación y prospectiva tecnológica, el Ministerio de la Tecnologías de Información y Comunicaciones MINTIC publica la resolución 01117 de 2022 por la cual se establecen “los lineamientos de transformación digital para las estrategias de ciudades y territorios inteligentes de las entidades territoriales, en el marco de la Política de Gobierno Digital”. Dentro de esta resolución, se establece que todas las entidades territoriales que establezcan estrategias de este tipo serán obligados a acogerse a los principios establecidos, a tener adoptado e implementado el modelo de madurez para Ciudades y Territorios Inteligentes del MINTIC y a cumplir con las condiciones señaladas en el anexo técnico II de la misma resolución (MinTIC, Lineamientos de transformación digital, 2022).

Las comunidades indígenas del Municipio de San José del Fragua, departamento del Caquetá, enfrenta una considerable brecha digital y los riesgos cibernéticos a los que están expuestos cada día, limitando el acceso a las tecnologías de la información y la comunicación (TIC), impidiendo el desarrollo de conocimientos básicos, necesarios para la inserción en el mundo moderno interconectado. La falta de alfabetización digital deja a estas comunidades expuestas a diversas amenazas cibernéticas, debido a un bajo nivel de conocimiento sobre ciberseguridad, análisis de vulnerabilidades y propuestas de resiliencia, necesarias para navegar de manera segura en internet.

El estado actual sobre crecimiento de las amenazas cibernéticas y el aumento exponencial de las tecnologías de la información cada día va en un aumento, lo que exige una defensa y cooperación globales más sólidas, afectando la operación y seguridad digital de cualquier organización en todo el mundo, estas zonas de inclusión tecnológica, donde el enfoque está en enseñar las técnicas necesarias de ciberseguridad, con la preparación y capacitación adecuada para

enfrentar estos desafíos que representa una amenaza constante. Esta brecha digital debe ser abordada con buenas prácticas en ciberseguridad, programas de alfabetización digital, herramientas tecnológicas accesibles, previniendo los ataques cibernéticos que vivimos a diario. (Microsoft, 2024)

Formulación del Problema

Diferentes escenarios que plantean la posibilidad de pérdida de información se manifiestan en eventos de seguridad informática a escala mundial, al mismo tiempo que se abordan estos ataques de ciberseguridad, las nuevas tecnologías también ofrecen a los ciberdelincuentes nuevas oportunidades.

Una investigación de (Almanza 2022) con respecto a la seguridad de la información, descubrió tres eventos principales, el primero es la instalación de software no autorizado (55,56 %), el segundo los virus y troyanos (46,3%), y el tercero por el acceso no autorizado a la web, en consecuencia, la fuga de información se produce en la escala identificada (19,14%), iluminando el panorama actual de las amenazas (Almanza, 2022), en Colombia el 12 de septiembre del año 2023, se reportaron ciberataques masivos de portales web de la rama Judicial, el Ministerio de Salud, la Superintendencia de Industria y Comercio y muchas otras entidades (Pais, 2023).

Con la colaboración de los equipos Red y Blue Team en ciberseguridad, encontramos que una de las vulnerabilidades son los sistemas de seguridad desactivados como antivirus y firewalls, el acceso no autorizado a los equipos de cómputo, políticas de seguridad, guías técnicas CIS, la implementación de medidas de hardenización y la falta de capacitación de los empleados en la organización.

Pregunta problema

¿Cuáles son las principales vulnerabilidades y amenazas cibernéticas que enfrentan las comunidades indígenas, y cómo influye la falta de alfabetización digital en su seguridad en línea, especialmente en contextos rurales?

Justificación

Reducir la brecha digital en las comunidades indígenas del municipio de San José del Fragua, departamento del Caquetá, el manejo de plataformas digitales son clave para mejorar las oportunidades sociales y económicas a estas comunidades indígenas, la implementación de estrategias defensivas de ciberseguridad y alfabetización digital con programas de formación, se podrán adquirir las competencias necesarias para utilizar las TIC de manera segura y efectiva, contribuyendo a la inclusión digital y el empoderamiento de comunidades indígenas resilientes.

Estas comunidades enfrentan mayores riesgos de ataques cibernéticos, suelen carecer de una infraestructura frágil y sin profesionales especializados en seguridad informática, lo que las convierte en objetivos fáciles para ciberdelincuentes, la falta de concientización y educación digital agrava la vulnerabilidad de los indígenas, siendo víctimas fáciles de técnicas de ingeniería social y otros métodos de ataque cibernético (Informe de Ciberseguridad, 2016).

La iniciativa busca empoderar a estas comunidades indígenas mediante la sensibilización en ciberseguridad, alfabetización digital efectiva y la creación de habilidades prácticas para la autogestión segura en entornos digitales, la educación en ciberseguridad no solo es una medida preventiva contra ataques informáticos, sino que también incrementa la confianza en el uso de tecnologías emergentes, fortaleciendo el desarrollo personal y comunitario, al reducir la brecha digital, se incrementa la posibilidad de que los indígenas de la región accedan a plataformas de educación digital, mejorando su aprendizaje y oportunidades en un mundo digital cada vez más interconectado.

A diferencia de los programas ofrecidos por el MINTIC, que generalmente son amplios y no siempre contextualizados para comunidades indígenas, este proyecto está diseñado específicamente para el contexto cultural, social y educativo de las comunidades indígenas del

municipio de San José del Fragua, al enfocarse en esta comunidad local, el proyecto adapta los contenidos y las metodologías a la realidad de sus habitantes, abordando las limitaciones de acceso, conectividad y niveles de alfabetización digital particulares de estas comunidades, pues ofrece un enfoque de proximidad, centrado en los desafíos locales específicos, algo que los programas nacionales no pueden cubrir con la misma profundidad ni personalización.

Este proyecto tiene el potencial de generar un impacto positivo a largo plazo, mejorando el bienestar económico y social de las comunidades indígenas, aprovechando las tecnologías digitales es crucial para fomentar la innovación tecnológica y mejorar sus conocimientos del mundo tecnológico y tan bien a que se exponen en la navegación en la web si en el uso adecuado o conocimiento básicos de ciberseguridad, potenciando la inclusión digital, al utilizar las TIC de forma efectiva y segura, reduciendo la brecha digital se amplían las oportunidades de educación digital, beneficiando a las comunidades indígenas del proyecto.

Objetivos

Objetivo general:

Evaluar los riesgos cibernéticos asociados a la brecha digital en las comunidades indígenas de San José de Fragua en el Caquetá frente a la falta de infraestructura tecnológica, evidenciando propuestas de resiliencia que promuevan una mayor inclusión tecnológica y fortalezcan su seguridad en el entorno digital de acuerdo con sus contextos culturales y sociales.

Objetivos específicos:

Caracterizar la brecha digital en comunidades indígenas considerando factores como el acceso a infraestructura tecnológica, la conectividad y habilidades digitales, teniendo en cuenta las principales vulnerabilidades cibernéticas que estas comunidades enfrentan, mediante una revisión sistemática de literatura.

Analizar los factores culturales, sociales y económicos que contribuyen a la brecha digital y aumentan la exposición a riesgos cibernéticos en las comunidades indígenas, generando estrategias que fortalezcan su resiliencia digital mediante la adopción de prácticas de ciberseguridad adaptadas a su contexto cultural.

Evaluar la efectividad de las estrategias propuestas, midiendo su impacto en la reducción de vulnerabilidades y en la mejora de la seguridad digital, en consonancia con su contexto cultural, mediante estudios de caso de los dos grupos seleccionados de la comunidad beneficiada.

Diseñar un plan de recomendaciones de resiliencia digital, que integre prácticas de ciberseguridad culturalmente pertinentes, sostenibles y replicables a otras comunidades indígenas, contribuyendo a la reducción de la brecha digital.

Marco Referencial

Antecedentes

Brecha digital y de ciberseguridad en las comunidades indígenas

La digitalización ha generado nuevas formas de inclusión y también de exclusión. En el caso de las comunidades indígenas, la brecha digital trasciende la falta de infraestructura o acceso físico a las tecnologías, es una problemática multidimensional atravesada por factores históricos, culturales, sociales y políticos[4]. El problema no solo limita el uso efectivo de las tecnologías de la información y la comunicación (TIC), sino que expone a estas comunidades a nuevos riesgos en materia de ciberseguridad, frente a los cuales suelen estar desprotegidas.

El trabajo de Huey y Ferguson [5] revela una preocupante desatención al impacto de la ciberseguridad en comunidades indígenas, identificando una escasa producción académica sobre el tema. A través de una revisión sistemática, hallaron solo 13 estudios relevantes, lo cual evidencia un rezago crítico en la investigación y formulación de respuestas adecuadas. Las formas más documentadas de ciber violencia incluyen el ciberacoso a jóvenes indígenas, el acoso a adultos y la trata de mujeres y niñas, siendo los jóvenes particularmente vulnerables frente a tasas de ciberacoso significativamente más altas que sus pares no indígenas. Sin embargo, las respuestas institucionales son limitadas y poco exploradas, dejando a estas poblaciones sin herramientas efectivas de prevención ni apoyo.

El estudio sobre las comunidades indígenas Batek y Semokberi en Malasia (Abadi, 2020) plantea que la brecha digital no puede entenderse únicamente como un déficit tecnológico. A través del concepto de "imaginarios digitales", se muestra cómo las experiencias de conectividad se configuran desde cosmovisiones y contextos culturales específicos. Para estas comunidades, estar

"conectado" o "desconectado" no tiene un significado universal, sino que reconfigura sus vínculos con el territorio, el tiempo y sus dinámicas sociales. Este enfoque plantea que cualquier estrategia de inclusión digital debe considerar las voces locales y reconocer la pluralidad de modos de habitar lo digital.

Complementando estas perspectivas, el estudio de (Oliver, 2022) expone cómo las políticas nacionales de ciberseguridad en países como Australia, Nueva Zelanda, Canadá y Estados Unidos han fallado en integrar los principios de soberanía de datos indígenas. A pesar del reconocimiento creciente sobre la importancia de empoderar digitalmente a las comunidades indígenas, las estrategias oficiales siguen ignorando sus derechos y valores. Esta omisión reproduce desigualdades estructurales y genera vulnerabilidades específicas en el entorno digital, en el cual los pueblos indígenas tienen escasa capacidad de decisión sobre el uso, almacenamiento y protección de sus datos.

En conjunto, estas investigaciones advierten sobre una forma emergente de exclusión digital, que va más allá del simple acceso a internet o a dispositivos tecnológicos. No basta con garantizar conectividad si esta no se acompaña de medidas de protección culturalmente pertinentes, políticas públicas que reconozcan la soberanía tecnológica de los pueblos indígenas y procesos educativos que fortalezcan su autonomía digital. La brecha existente en el acceso, uso y apropiación de tecnologías, recursos digitales y prácticas de ciberseguridad en las comunidades indígenas constituye, en esencia, una manifestación actual de una exclusión histórica continua. Esta situación demanda una atención gubernamental apoyada por la Estrategia Nacional de Seguridad Digital de Colombia 2025-2027, una sociedad incluyente, interseccionales y profundamente respetuosos de la diversidad cultural.

Riesgos cibernéticos y vulnerabilidades en comunidades Indígenas

Es indiscutible que el acelerado avance de las tecnologías emergentes y el perfeccionamiento de las ya existentes han transformado notablemente la manera en que las sociedades acceden a la información interactúa y ejercen sus derechos, es fundamental reconocer que este proceso de transformación no ha sido homogéneo ni equitativo. Las comunidades indígenas, tanto a nivel global como en contextos locales como el colombiano, enfrentan múltiples riesgos cibernéticos y vulnerabilidades que no solo reflejan, sino que también acentúan las desigualdades históricas que han padecido.

A nivel internacional, múltiples estudios han evidenciado cómo la inclusión digital de pueblos indígenas se ha centrado casi exclusivamente en mejorar el acceso a la infraestructura tecnológica, sin considerar los impactos que esta conectividad trae consigo, la falta de alfabetización digital, la falta de políticas públicas, y la ausencia de enfoques culturalmente pertinentes, han dejado a estas comunidades expuestas a nuevas formas de violencia, como el ciberacoso, la explotación en línea, la desinformación y la apropiación indebida de datos culturales y territoriales.

La vulnerabilidad empeora por la escasa protección legal de la soberanía de datos indígenas, un principio fundamental que reconoce el derecho de los pueblos a controlar el uso, almacenamiento y circulación de su información digital. Esta ausencia de protección se traduce en riesgos que van desde la recolección no consentida de datos por parte de empresas o gobiernos, hasta la pérdida de control sobre narrativas culturales y saberes ancestrales que pueden ser digitalizados y difundidos sin permiso ni contexto adecuado.

En Colombia, el censo nacional de población y vivienda realizado en el año 2018 identificó población perteneciente a 115 pueblos indígenas nativos distribuidos en diversas regiones del país, las amenazas digitales cada día son más recurrentes, no existen esfuerzos estatales y comunitarios orientados a reducir la brecha digital en zonas rurales o de difícil acceso, la conectividad no siempre va acompañada de procesos formativos adecuados en educación digital, ni de mecanismos de seguimiento que evalúen la efectividad y cumplimiento de las políticas públicas, que en la mayoría de los casos se limitan a planteamientos en el papel, persistiendo la ausencia de marcos regulatorios sólidos que garanticen la seguridad digital y los derechos culturales de estas comunidades.

En territorios indígenas colombianos, el ingreso de tecnologías de la información ha generado tensiones entre la preservación cultural y los nuevos riesgos. Casos de ciberacoso a jóvenes indígenas, campañas de desinformación que afectan sus procesos organizativos, o la suplantación de liderazgos comunitarios en redes sociales, son solo algunos ejemplos de cómo las amenazas cibernéticas pueden vulnerar la autonomía y cohesión de estas comunidades. Además, el uso de herramientas digitales por parte de organizaciones sociales indígenas para visibilizar sus luchas y denuncias sobre violaciones de derechos humanos también las expone a represalias digitales, ataques de denegación de servicio DDos, o campañas de desprestigio.

En este escenario, resulta fundamental adoptar un enfoque intercultural y territorial en las estrategias de ciberseguridad, que esté articulado con los gobiernos locales, sea legítimo y aceptado por las poblaciones indígenas, y responda a las particularidades regionales de departamentos como Caquetá. Esto implica reconocer que las comunidades indígenas no son totalmente usuarios digitales, sino sujetos colectivos con derechos diferenciados, saberes ancestrales y formas propias de relacionarse con el entorno digital. Proteger su integridad en el ciberespacio exige más que

soluciones técnicas: requiere voluntad política, procesos de formación contextualizados y un diálogo genuino entre el conocimiento tradicional y la innovación tecnológica.

Marco Conceptual

El análisis de la brecha digital y los riesgos cibernéticos en comunidades indígenas requiere comprender la interacción entre factores tecnológicos, sociales, culturales y educativos, la solución debe integrar enfoques de ciberseguridad, educación digital y pertinencia cultural, garantizando que las estrategias propuestas sean efectivas, sostenibles y adaptadas al contexto de la comunidad indígena Inga.

En este sentido, el marco conceptual se construye a partir de cuatro ejes fundamentales: brecha digital, ciberseguridad y riesgos digitales, vulnerabilidades digitales y resiliencia digital, los cuales se interrelacionan en el contexto de la comunidad indígena Inga.

Brecha digital y acceso a las TIC:

La brecha digital se entiende como la desigualdad en el acceso, uso y apropiación de las tecnologías de la información y la comunicación (TIC). Según autores como Van Dijk (2020), esta brecha no solo depende del acceso físico a dispositivos o conectividad, sino también de habilidades, uso significativo y contexto social.

En comunidades indígenas como la Inga, esta brecha se manifiesta en limitaciones de infraestructura tecnológica, baja conectividad y escasa formación digital, lo que restringe su participación en la sociedad digital y aumenta su exposición a riesgos.

La educación digital, en este contexto, cumple un papel fundamental al facilitar la apropiación tecnológica. Como lo plantea Area (2018), la alfabetización digital implica no solo saber usar herramientas tecnológicas, sino comprender sus riesgos y oportunidades.

Ciberseguridad y riesgos digitales:

La ciberseguridad se refiere al conjunto de prácticas, tecnologías y procesos diseñados para proteger sistemas, redes y datos frente a accesos no autorizados o ataques (ISO/IEC 27001, 2013). Este concepto se relaciona directamente con los riesgos cibernéticos, entendidos como la probabilidad de que una amenaza afecte la integridad, disponibilidad o confidencialidad de la información.

Las amenazas cibernéticas pueden materializarse en diversas formas como fraude en línea, phishing, malware o suplantación de identidad, especialmente en contextos donde el conocimiento digital es limitado.

Elementos técnicos como la autenticación y el uso de herramientas como antivirus constituyen mecanismos básicos de protección, sin embargo, su efectividad depende del nivel de conocimiento del usuario.

Vulnerabilidad digital en contextos rurales e indígenas:

La vulnerabilidad digital hace referencia a las debilidades que incrementan la exposición a riesgos cibernéticos. Según el enfoque de gestión de riesgos (ISO 27005), una vulnerabilidad es una debilidad que puede ser explotada por una amenaza.

En comunidades indígenas, estas vulnerabilidades están influenciadas por:

- Factores culturales (uso de lengua propia como el ingano)
- Factores sociales (nivel educativo)
- Factores económicos (limitado acceso a dispositivos y conectividad)

El uso compartido de dispositivos, la dependencia de redes públicas y la falta de formación en ciberseguridad incrementan la probabilidad de incidentes digitales. Los pueblos indígenas poseen características socioculturales propias que influyen en la adopción tecnológica. Como señala la

UNESCO (2019), la incorporación de TIC en comunidades indígenas debe respetar su cosmovisión, lengua y prácticas tradicionales.

En el caso del pueblo Inga, la lengua inga y sus dinámicas comunitarias influyen en la forma en que se perciben y utilizan las tecnologías. Esto implica que las estrategias de ciberseguridad deben ser culturalmente pertinentes, utilizando lenguaje accesible y metodologías participativas.

Resiliencia digital como respuesta estratégica

La resiliencia cibernética se define como la capacidad de una comunidad para prevenir, resistir, adaptarse y recuperarse de incidentes digitales (NIST, 2018). Este concepto integra tanto la prevención como la respuesta ante amenazas, la resiliencia digital se construye a partir de:

- Fortalecimiento de la alfabetización digital
- Implementación de prácticas seguras
- Desarrollo de capacidades comunitarias
- Adaptación cultural de estrategias de seguridad

El enfoque de resiliencia permite pasar de una visión reactiva a una visión preventiva y sostenible, en la cual la comunidad se convierte en un actor activo en su propia protección digital, los conceptos descritos se articulan de la siguiente manera:

- La brecha digital limita el acceso y conocimiento tecnológico.
- Esta limitación incrementa la vulnerabilidad digital.
- La vulnerabilidad facilita la materialización de riesgos cibernéticos.
- La educación digital y la ciberseguridad actúan como mecanismos de mitigación.

La resiliencia digital se consolida como una estrategia integral para fortalecer la seguridad y sostenibilidad tecnológica en la comunidad.

Marco teórico

La brecha digital en regiones rurales

La brecha digital es uno de los principales desafíos en la era de la información, esta problemática se manifiesta con mayor fuerza en las zonas rurales y comunidades indígenas, donde el acceso a las (TIC) es limitado o nulo, generando desigualdades en educación, participación ciudadana, desarrollo económico y acceso a la web.

En Colombia, el Departamento Administrativo Nacional de Estadística (DANE, 2024) junto con el Ministerio de Tecnologías de la Información y las Comunicaciones, han realizado estudios que muestran cómo la falta de conectividad en áreas rurales contribuye a una brecha digital amplia y persistente, especialmente en departamentos alejados como Caquetá. Estos informes destacan factores como la baja infraestructura tecnológica, la falta de capacitación y el acceso desigual a dispositivos tecnológicos. Estudios en América Latina han evidenciado que el acceso a internet y educación digital en regiones rurales aumenta la exclusión social y limita la equidad de oportunidades, exacerbando la pobreza y la marginalización en estas áreas.

Informes del MINTIC sobre conectividad digital en Colombia.

El MINTIC ha publicado múltiples informes sobre el estado de la conectividad digital en Colombia, las zonas alejadas como el municipio de San José del Fragua, exponen la existencia de barreras significativas para el acceso a internet y la baja alfabetización digital.

Principales hallazgos del MINTIC:

En muchas regiones de Caquetá, la conectividad es baja debido a las dificultades para llevar infraestructura de internet a zonas de difícil acceso, el MINTIC subraya que esto limita a la población rural en sus oportunidades de desarrollo personal y profesional.

Aunque existen programas de acceso a internet y alfabetización digital, muchos se enfocan en poblaciones urbanas o no logran alcanzar la continuidad necesaria para generar un cambio real, esto justifica la necesidad de iniciativas más focalizadas en comunidades indígenas del municipio de San José del Fragua, donde es necesario adaptar los contenidos y estrategias a las realidades locales.

Literatura sobre ciberseguridad comunitaria.

La Ciberseguridad: una mirada a los métodos y estrategias de anticipación al avance del cibercrimen en Colombia y la región (Jiménez, 2022). Frente a la creciente dependencia de la tecnología y el riesgo de amenazas en línea en comunidades vulnerables, la ciberseguridad comunitaria es una respuesta emergente que aborda la protección de datos y el uso seguro de las TIC, al igual también educa o capacita a los usuarios sobre las amenazas comunes en línea, la protección de información personal y el uso de prácticas seguras en internet.

En Europa y América Latina los proyectos en comunidades rurales han demostrado que, al fomentar la ciberseguridad con limitados conocimientos digitales, se reducen los riesgos de ataques cibernéticos y fraudes digitales, promoviendo una cultura de prevención.

En este contexto, el Instituto Nacional de Ciberseguridad de España (INCIBE, 2024), ha impulsado programas para capacitar a comunidades pequeñas en temas de ciberseguridad, señalando que estas iniciativas fomentan el autocuidado digital y protegen a los usuarios más vulnerables.

El desafío más complejo que enfrentan los pueblos indígenas en cuanto a transformación digital es superar las brechas digitales de una manera que sea culturalmente pertinente, aun cuando se lograra mejorar la cobertura acceso a servicios de internet y dispositivos tecnológicos, si no se promueve el desarrollo de habilidades digitales y si los contenidos existentes siguen siendo en los idiomas dominantes, sólo se acentuaría el riesgo de asimilación de su cultura, esta vez por medio de las tecnologías digitales.

Estudios sobre minimización de brechas digitales.

La alfabetización digital es clave para cerrar la brecha digital, especialmente en comunidades indígenas, la falta de conocimientos digitales básicos limita el uso efectivo de las TIC, dificultando la participación de la población en actividades económicas, educativas y sociales.

Proyectos de alfabetización digital en África (Unesco, 2024) y América Latina han resaltado que enseñar a las comunidades a utilizar dispositivos y plataformas digitales mejora no solo el acceso a la información, sino también la capacidad de autogestión y resolución de problemas de los habitantes. En Colombia, se han impulsado proyectos de alfabetización digital para capacitar a poblaciones vulnerables, incluyendo zonas rurales, en competencias básicas digitales, Sin embargo, estos programas a menudo carecen de continuidad, por lo cual un proyecto focalizado y a largo plazo tiene el potencial de crear un cambio duradero y significativo.

Propuestas educativas y contextuales para la ciberseguridad y la inclusión digital

El modelo educativo que mejor responde a las necesidades de las comunidades indígenas y con baja alfabetización digital es el de educación personalizada, en donde los contenidos se desarrollan tomando en cuenta las necesidades específicas de cada grupo, los proyectos

comunitarios de ciberseguridad deben ser aplicables y accesibles para la población, lo que significa adaptar el lenguaje, simplificar los conceptos y proporcionar recursos prácticos de fácil acceso.

La literatura destaca que una educación digital inclusiva y basada en las realidades de la comunidad indígena facilita la adopción y uso de la tecnología, estudios sobre proyectos de ciberseguridad en América Latina han demostrado que adaptar los contenidos y métodos a las características de la comunidad contribuye a una mejor comprensión y a un uso seguro de las TIC.

Marco legal

Ley 1273 de 2009, enero 5 (Publica, 2009)**,** cambia el código penal, proporciona un nuevo derecho legal protegido denominado "*protección de la información y los datos"*, y salvaguarda completamente los sistemas que hacen uso de las TIC.

Artículo 269A. *Uso no autorizado de un sistema informático*. Se impone una pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y una multa de 100 a 1.000 dólares a quien acceda total o parcialmente a un sistema informático sin autorización o fuera de lo acordado, o permanezca en él en contra de la voluntad de quien tiene el derecho legal de excluirlo.

Artículo 269B. *Intromisión no autorizada en un sistema informático o red de comunicaciones.* Se impondrá pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y multa de cien (100) a mil (1.000) salarios mínimos legales mensuales vigentes a quien, sin estar autorizado para ello, impida u obstruya el normal funcionamiento o el acceso a un sistema informático, a los datos informáticos contenidos en él o a una red de telecomunicaciones, siempre que la conducta no constituya delito sujeto a pena superior.

Artículo 269C. *Escucha de datos en los ordenadores*. Se impondrá una pena de prisión de treinta y seis (36) a setenta y dos (72) meses a quien intercepte ilegalmente datos informáticos en

su origen, destino, en el interior de un sistema informático o las emisiones electromagnéticas procedentes de un sistema informático que los transporta.

Artículo 269D. Daño a una computadora. El que, sin autorización, borre, corrompa, degrade, altere o suprima datos informáticos, un sistema de procesamiento de información o cualquiera de sus partes o componentes lógicos, será castigado con prisión de cuarenta y ocho (48) a noventa y seis (96) meses, además de una multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E. *uso de software perjudicial.* Se impone pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y/o multa de 100 a 1.000 dólares a quien, sin estar autorizado para ello, cree, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas informáticos con efectos nocivos.

Artículo 269F. *Violación de datos personales*. El que sin autorización obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o utilice códigos personales, datos personales contenidos en ficheros, archivos, bases de datos u otros medios análogos en beneficio propio o de terceros, será sancionado con prisión de cuarenta y ocho (48) a noventa y seis (96) meses y multa de 100 a 1.000 dólares, según los salarios mínimos legales mensuales vigentes.

Artículo 269G. Utilización de páginas web falsas para recabar información personal Se impondrá pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y/o multa de 100 a 1.000 dólares a quien, sin autorización y con un fin ilícito, cree, desarrolle, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, siempre que la conducta en cuestión no constituya un delito sancionado con una pena más grave (Diana, 2022).

Ley 1581 de 2012, octubre18, Por la cual se dictan disposiciones generales para la protección de datos personales.

Artículo 4°. Principios para el Tratamiento de datos personales. En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral.

Artículo 6°. ***Tratamiento de datos sensibles.*** Se prohíbe el Tratamiento de datos sensibles, excepto cuando:

Artículo 7°. ***Derechos de los niños, niñas y adolescentes.***

En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

Artículo 11. ***Suministro de la información*****.** La información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en un todo a aquella que repose en la base de datos.

Artículo 26. ***Prohibición*****.** Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos.

Decreto 767 de 2022 mayo 16. se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones**.**

Marco contextual

El municipio de San José del Fragua, ubicado en el sur del departamento del Caquetá, Colombia, caracterizado por un ecosistema de alta biodiversidad, predominando el bosque húmedo

tropical, se ubica en la zona de influencia del Parque Nacional Natural Alto Fragua Indi Wasi, su diversidad étnica de la época precolombina, fueron los indígenas pertenecientes a la cultura Inga, los cuales se han establecido en las márgenes de los ríos Fragua Grande y Yurayaco.

Territorio habitado por comunidades campesinas e indígenas, particularmente de los pueblos Inga y Coreguaje, manteniendo formas tradicionales de vida, limitaciones de acceso a infraestructura tecnológica, conectividad a Internet, servicios públicos adecuados y educación de calidad en competencias digitales, ubicándolos en una posición de vulnerabilidad frente a los riesgos del entorno digital.

La brecha digital en estas comunidades no solo se manifiesta en la falta de acceso físico a dispositivos o conectividad, sino también en la ausencia de habilidades digitales básicas, alfabetización tecnológica y conocimiento en ciberseguridad, limitando su participación plena en los beneficios que ofrecen las Tecnologías de la Información y la Comunicación (TIC), e incrementan su exposición a riesgos como el fraude digital, robo de datos personales, manipulación de información y otros tipos de ataques cibernéticos que afectan incluso a poblaciones rurales y vulnerables.

Los programas o capacitaciones del (MinTIC, 2025), han representado avances importantes, pero la mayoría no se adaptan a los contextos culturales específicos de estas comunidades indígenas ni consideran las barreras lingüísticas, sociales y geográficas que enfrentan. Esto refuerza la necesidad de un enfoque territorial, inclusivo y diferenciado, que promueva la resiliencia digital desde la cultura, el territorio y la educación digital propia.

Este proyecto propone un estudio profundo de las vulnerabilidades digitales en comunidades indígenas de San José del Fragua, a través de una revisión de literatura, estudios de caso y trabajo de campo, con el fin de construir propuestas pertinentes y culturalmente sensibles

para el fortalecimiento de la inclusión digital y la ciberseguridad, además responde algunos Objetivos de Desarrollo Sostenible (ONU, 2015), ODS 4 (Educación de calidad), ODS 9 (Industria, innovación e infraestructura), y ODS 10 (Reducción de las desigualdades), fortaleciendo procesos de equidad tecnológica en zonas rurales y promoviendo una ciudadanía digital activa, crítica y protegida.

Este proyecto se fundamenta en una necesidad territorial y cultural urgente que analice cómo las condiciones de acceso, apropiación tecnológica y cultura digital inciden en la vulnerabilidad cibernética, como fortalecer su resiliencia digital sin imponer modelos externos que desconozcan sus formas propias de vida, contribuyendo al diseño de estrategias de formación, conectividad y seguridad digital ajustadas al contexto sociocultural, apoyadas en metodologías participativas y adaptadas a las dinámicas del territorio, cerrando la brecha digital, evitar la exclusión tecnológica y la exposición a riesgos cibernéticos.

Diseño Metodológico

La metodología empleada en el estudio combina enfoques cuantitativos y cualitativos bajo un diseño exploratorio-descriptivo, orientado a comprender y mejorar la alfabetización digital y las prácticas de ciberseguridad en las comunidades indígenas del municipio de San José del Fragua, Caquetá. Se aplica un estudio de caso basado en el modelo de Runeson y Host con una población conformada por jóvenes estudiantes y comunidad indígena en general, utilizando muestreo por conveniencia con una muestra estimada de 30 a 40 personas.

Las variables consideradas incluyen la participación en un programa de ciberseguridad (independiente) y, como dependientes, el nivel de alfabetización digital, las prácticas de seguridad, la percepción tecnológica y la satisfacción con el programa. Se utilizan encuestas estructuradas, observación directa, entrevistas y talleres de capacitación para la recolección de datos, que luego

se analizan mediante estadística descriptiva e inferencial, y codificación temática para los datos cualitativos. La evaluación del impacto se centra en el cambio en el uso de TIC, adopción de buenas prácticas de ciberseguridad y satisfacción de los participantes. La revisión de literatura se apoya en estudios previos sobre brechas digitales en comunidades rurales e indígenas, alineando la propuesta con los Objetivos de Desarrollo Sostenible relacionados con la inclusión digital y el desarrollo equitativo.

Tipo y enfoque de Investigación.

El presente estudio adopta un enfoque cualitativo, orientado a comprender las dinámicas culturales, sociales y tecnológicas que configuran la brecha digital y los riesgos cibernéticos en las comunidades indígenas de San José del Fragua, Caquetá. Se emplea un diseño descriptivo-analítico, ya que busca caracterizar las vulnerabilidades existentes y analizar las estrategias que permitan fortalecer la resiliencia digital, respetando las particularidades culturales de las comunidades. Adicionalmente, se realizará un componente estudio de caso, enfocado en dos grupos indígenas seleccionados, para evaluar de manera detallada la efectividad de las propuestas de resiliencia.

Para la realización del estudio de casos se adopta el modelo metodológico propuesto por Runeson y Host (2009), conformado por cinco pasos fundamentales. La descripción operativa de estas fases ha sido retomada de Alonso (2013), quien sistematiza su aplicación en investigaciones empíricas.

Método de Investigación.

Se utilizará el método de investigación acción participativa (IAP), dado que promueve la colaboración directa con las comunidades objeto de estudio. Esta metodología permite identificar problemas reales, reflexionar conjuntamente y construir soluciones adaptadas al contexto cultural

de los participantes. La investigación acción participativa se fundamenta en principios de diálogo horizontal, respeto por el conocimiento tradicional y empoderamiento comunitario en el proceso de toma de decisiones.

Población y Muestra.

La población objeto de estudio está conformada por las comunidades indígenas del municipio de San José del Fragua, departamento del Caquetá. La muestra será intencional y estará compuesta por:

Una población indígena seleccionados en función de criterios de acceso tecnológico, disposición a participar y representatividad cultural.

Líderes comunitarios, jóvenes, adultos mayores y docentes de la institución educativa.

Variables.

Variable independiente:

- Participación en el programa de ciberseguridad y educación digital.

Variables dependientes.

- Nivel de alfabetización digital.
- Prácticas de ciberseguridad.
- Percepción de la tecnología y acceso a TIC.
- Satisfacción con el programa.

Hipótesis.

Hipótesis general.

La implementación de estrategias de ciberseguridad con encuesta estructurada sobre uso de las TIC y prácticas de seguridad digital reducirá la brecha digital en las comunidades indígenas del Municipio de San José del Fragua.

Hipótesis específica

La capacitación en alfabetización digital incrementará el nivel de uso y conocimiento de TIC en el sector estudiantil.

La implementación de estrategias de ciberseguridad reducirá la exposición a riesgos digitales.

La educación digital contextualizada mejorará la percepción y adopción de TIC en las comunidades indígenas.

Técnicas e instrumentos de recolección de información.

Para la recolección de información se utilizarán las siguientes técnicas e instrumentos:

Revisión sistemática de literatura. Se recopilarán estudios académicos, informes institucionales y documentos de organismos internacionales sobre brecha digital, riesgos cibernéticos y resiliencia digital en comunidades indígenas.

Entrevistas semiestructuradas. Dirigidas a líderes comunitarios, docentes locales, gestores de TIC y miembros de las comunidades seleccionadas. Se diseñarán guías de entrevista que permitan explorar percepciones, conocimientos y prácticas relacionadas con el uso seguro de las tecnologías. Grupos focales: Se organizarán espacios de diálogo con miembros de las comunidades para identificar necesidades, vulnerabilidades, riesgos percibidos y propuestas de acción. Observación participante: A través de visitas de campo se registrarán prácticas, dinámicas de acceso a tecnología, nivel de conectividad y situaciones cotidianas que reflejen la relación de las comunidades con el entorno digital. Estudio de caso: Se realizará un análisis profundo de dos

comunidades indígenas seleccionadas, evaluando el impacto de las estrategias propuestas en su resiliencia digital.

Procedimiento:

El procedimiento de la investigación se desarrollará en las siguientes fases:

Fase de diagnóstico inicial. Revisión documental y primer acercamiento a las comunidades para identificar la situación actual de la brecha digital y riesgos cibernéticos.

Fase de recolección de información. Aplicación de entrevistas, grupos focales y observación participante para identificar vulnerabilidades y factores culturales asociados.

Fase de diseño de estrategias de resiliencia. Construcción colectiva de propuestas de fortalecimiento digital basadas en los hallazgos, respetando los saberes y prácticas culturales.

Fase de implementación piloto. Aplicación de algunas estrategias seleccionadas en las dos comunidades escogidas.

Fase de evaluación. Análisis del impacto de las estrategias en términos de reducción de vulnerabilidades digitales y fortalecimiento de capacidades de resiliencia.

Análisis de la información: La información recolectada será analizada mediante técnicas de análisis de contenido, identificando categorías temáticas emergentes relacionadas con: Brecha digital, Riesgos cibernéticos, Factores culturales y sociales, Estrategias de resiliencia.

Técnicas para el análisis de los datos recopilados.

Análisis cuantitativo. Se utilizarán estadísticos descriptivos y pruebas de hipótesis (como la t de Student o ANOVA, según la muestra y distribución) para evaluar las diferencias en los niveles de alfabetización digital y ciberseguridad antes y después de la capacitación.

Análisis cualitativo. Las entrevistas y observaciones se analizarán mediante técnicas de codificación temática para identificar patrones y categorías emergentes que describan las percepciones y barreras de cada comunidad hacia la tecnología.

Medición de impacto y evaluación.

- Nivel de uso de TIC por la frecuencia y tipos de uso reportados en las encuestas.
- Evaluación en prácticas de ciberseguridad, aplicación de medidas de seguridad, el uso de contraseñas seguras en tecnologías emergentes.
- Encuestas de satisfacción para medir la percepción del programa y su aplicabilidad en la vida cotidiana.

Descripción de los métodos y herramientas utilizadas.

Se utilizó la metodología de Revisión Sistemática de Literatura (RSL), guiada por el modelo **SMS** (Systematic Mapping Study), empleando la estrategia **PICOC** (Población, Intervención, Comparación, Contexto y Resultados).

Bases de datos académicas:

- Scopus
- ScienceDirect
- IEEE Xplore

Fuentes institucionales.

- Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
- Bases de datos de la e-Biblioteca (UNAD).
- Departamento Administrativo Nacional de Estadística (DANE).
- Plan Nacional de TIC.

Criterios de inclusión:

- Publicaciones entre 2021-2026
- Idiomas: español e inglés
- Revistas o artículos de investigación
- Estudios centrados en comunidades indígenas, brecha digital, alfabetización digital, ciberseguridad, tecnologías inclusivas

Criterios de exclusión:

- Artículos en chino, alemán o ruso
- Estudios no académicos o sin revisión
- Fuentes con enfoque exclusivamente urbano o corporativo

Cadena de búsqueda usada:

("brecha digital" OR "educación digital") AND ("comunidades indígenas" OR "poblaciones rurales") AND (resiliencia OR "ciberseguridad")

Revisión sistemática de literatura.

Los estudios previos hechos por el grupo de investigación de Petersen, que se han centrado en el análisis de brechas digitales y el uso de tecnologías en comunidades rurales e indígenas en América Latina (Petersen, 2024).

En el marco del programa Iniciativas sustentables, promueven proyectos que aporten a los objetivos de desarrollo sostenible (ODS 2022) y sus metas. Las TIC están vinculado con varios de los ODS y tienen un impacto directo en la brecha digital, promoviendo la inclusión digital, el desarrollo sostenible y oportunidades. Estudios revisados y clasificados:

Brecha digital de zonas indígenas como factor de exclusión social. Disponible en: https://revistas.ort.edu.uy/inmediaciones-de-la-comunicacion/article/view/3557

Acceso a internet y pueblos indígenas en la Amazonía colombiana. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/DD_Amazonia_3_Colombia.pdf

Capítulo 1

Caracterización de la brecha digital en comunidades indígenas

La brecha digital es una problemática que afecta a muchas comunidades indígenas en el mundo y se manifiesta como una desigualdad en el acceso y uso de las tecnologías de la información y comunicación (TIC), las regiones rurales son las más vulnerables por falta de infraestructura tecnológica, acceso a internet y dispositivos obsoletos o limitados. Estudios ya realizados han demostrado que la brecha digital en estas comunidades no solo limita el acceso a la información, sino que también reduce oportunidades educativas, laborales y de inclusión social.

Las comunidades indígenas en Colombia han sido tradicionalmente consideradas como una minoría, según el Censo Nacional del DANE. (2019), el 13,6 % de la población del país equivalente a 4.671.160 millones de personas se reconoce como perteneciente a grupos étnicos, de este total, 1.905.617 millones de personas (4,4 %) hacen parte de pueblos indígenas, con presencia en 1.153 municipios de país, los departamentos con mayor concentración de pueblos indígenas son La Guajira, Cauca, Nariño, Córdoba, Sucre y Caquetá.

El Departamento del Caquetá, ubicado en la región amazónica de Colombia, presenta una geografía diversa, rica en recursos naturales y de una gran población indígena que habita principalmente en zonas rurales de difícil acceso, a pesar de la importancia cultural, ambiental y social de estas comunidades, su desarrollo se ha visto históricamente condicionado por el conflicto armado, el abandono estatal y la falta de inversión en infraestructura básica, especialmente en tecnologías de la información y la comunicación (TIC).

Con el desarrollo del primer objetivo específico, se busca identificar los principales factores que limitan el acceso, uso y apropiación de las tecnologías de la información y la comunicación (TIC), permitiendo explorar las vulnerabilidades cibernéticas derivadas de dicha

brecha, con el fin de sustentar estrategias resilientes que promuevan la inclusión digital y la protección frente a riesgos tecnológicos, documentando las herramientas utilizadas, resultados preliminares y la revisión sistemática de literatura.

Factores de la Brecha Digital.

- **Acceso a infraestructura tecnológica.**

Colombia ocupa la última posición en conexiones a internet por cada 100 habitantes entre los 38 países medidos por la Organización para la Cooperación y el Desarrollo Económicos (OCDE). La brecha de conectividad entre las áreas rurales y las áreas urbanas del país es considerable. El 52,9 % de los hogares en el área urbana y el 12,4 % (MinTIC, Cierre de la brecha digital , 2023) de los hogares en el área rural tienen acceso a internet fijo. Los menores niveles de conexión a internet se encuentran en la Amazonía colombiana.

La Conectividad es limitada en el acceso a internet a pueblos indígenas, evidenciando una infraestructura deficiente, en regiones como el departamento del Caquetá, menos del 3% (DANE, La información del DANE, 2022) de los hogares indígenas no cuentan con servicios básicos como el acceso a internet, electricidad y acueducto, evidenciando falencias para mejorar su bienestar y desarrollo.

La falta de inversión en infraestructura tecnológica en zonas rurales y apartadas perpetúa la exclusión digital en las comunidades indígenas.

En el municipio de San José del Fragua, se han presentado proyectos para comunidades indígenas como construir y dotar las salas de sistemas de la institución educativa Yachaikuri y sus sedes educativas, para que los niños, niñas y adolescentes indígenas puedan acceder a las tecnologías de la información y la comunicación. (ART, 2018).

- **La conectividad.**

La falta de infraestructura y acceso a Internet es significativa en las comunidades indígenas, especialmente en zonas rurales y remotas.

Los altos costos y disponibilidad de los servicios de Internet en las comunidades indígenas hacen que el acceso sea limitado.

Brecha cultural al acceso del Internet puede generar tensiones culturales y afectar las prácticas tradicionales de las comunidades indígenas.

Desconfianza hacia el acceso de la web, como una amenaza a la identidad cultural genera resistencia en algunos sectores de estas comunidades.

- **Habilidades Digitales.**

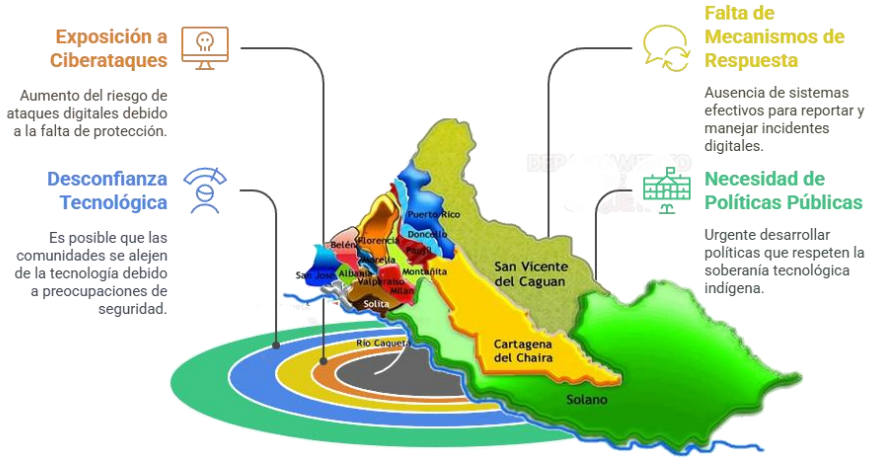
Desde una investigación de manera implícita la Desigualdad en el acceso, uso u manejo de las Tecnologías de la Información y la Comunicación (TIC).

Alfabetización digital insuficiente. La falta de programas de formación adaptados cultural y lingüísticamente limita el desarrollo de competencias digitales en estas comunidades.

Desconocimiento de riesgos cibernéticos. La ausencia de educación en ciberseguridad expone a las comunidades a amenazas como fraudes, desinformación y suplantación de identidad.

Resiliencia Digital

Fig 2. *Describe las implicaciones de la falta de conciencia sobre amenazas digitales en comunidades indígenas, evidenciando la necesidad de estrategias interculturales que fortalezcan la resiliencia digital.*



Fuente: elaboración propia

Actualmente, la brecha digital en las comunidades indígenas del Caquetá es evidente, se manifiesta principalmente el acceso al internet, la limitada disponibilidad de dispositivos tecnológicos y la casi nula capacitación en competencias digitales, lo que impide su participación en los procesos educativos, económicos, sociales y políticos del país. Esta exclusión digital incrementa su vulnerabilidad frente a riesgos cibernéticos como fraudes, manipulación de información, robo de datos y acceso no autorizado, dificultando su integración en el mundo digital de forma segura y autónoma.

Discusión y análisis:

Los resultados confirman la existencia de una brecha no solo tecnológica, sino también cultural y educativa entre las comunidades indígenas y el resto de la población colombiana en cuanto a inclusión digital.

Los estudios revisados muestran que la falta de conectividad, infraestructura básica y contenidos pertinentes que generan exclusión digital y a su vez, incrementa las vulnerabilidades

cibernéticas, pues las comunidades no cuentan con herramientas ni conocimientos para proteger su información o responder ante un ataque cibernético.

En comparación con otros países de América Latina o Europa, se identifican patrones similares como la desprotección normativa, centralismo tecnológico y la desarticulación entre gobierno, comunidad y academia.

En este contexto, el proyecto busca fortalecer la resiliencia digital de las comunidades indígenas mediante la implementación tecnológica adaptada a su entorno, el diseño de una plataforma web educativa, y la capacitación en ciberseguridad, con un enfoque intercultural que respete y valore sus saberes, lenguas y estructuras comunitarias.

Experiencias documentadas

Comunidades Indígenas en la Amazonía Colombiana. Solo en el departamento del Amazonas existen 22 pueblos indígenas que apenas representan el 57,7 % del total presente en la Amazonia Colombiana que abarca los departamentos de Caquetá, Guainía, Guaviare, Putumayo, Vaupés, la Bota Caucana, las vertientes amazónicas de Nariño y el sur del Meta.

Un estudio de Derechos Digitales destaca que, a pesar de las limitaciones en infraestructura, las comunidades indígenas del Vaupés buscan acceder a internet principalmente para mejorar la comunicación interna y preservar su cultura. Sin embargo, la falta de políticas públicas adecuadas y la ausencia de contenidos pertinentes limitan el aprovechamiento de las TIC. (SINCHI, 2022)

Pueblo Wayuu en La Guajira. Global Voices reporta que los hablantes de wayuunaiki enfrentan brechas digitales significativas que afectan su seguridad en línea. La falta de educación en ciberseguridad adaptada a su contexto cultural y lingüístico incrementa su vulnerabilidad ante amenazas digitales. (Organización Nacional Indígena de Colombia, 2022)

Informe de investigación y gestión del proyecto Tijitalü Wayuu - Wayuu Digital, es un proyecto que apoya procesos de alfabetización mediática e informacional, así como el fomento de acciones para la revitalización cultural y la promoción de derechos en escuelas pertenecientes a la comunidad indígena wayuu de Colombia y Venezuela. Esto es llevado a cabo mediante el aprovechamiento de la infraestructura tecnológica en contextos de difícil conectividad, mediante actividades que permitieron brindar apoyo a los procesos educativos. (Mónica Bonilla-Parra (redacción), 2022)

Comunidades Indígenas en Ecuador. Impacto de la conectividad digital en hogares liderados por mujeres, individuos de pueblos indígenas o afrodescendientes en Ecuador. Se observa una brecha digital significativa que afecta de manera desproporcionada a estas comunidades indígenas. El informe destaca que la falta de conectividad digital limita el acceso a oportunidades de educación, empleo, servicios de salud y participación cívica. Esto se traduce en una desventaja para estos hogares en términos de inclusión social y desarrollo económico. (Raúl Katz, 2024)

Análisis de las principales amenazas cibernéticas que estas comunidades presentan

La caracterización de la brecha digital en la comunidad indígena Inga, se identificó que la limitada infraestructura tecnológica, la conectividad intermitente y el bajo nivel de alfabetización digital generan un entorno altamente vulnerable frente a amenazas cibernéticas. A partir de la revisión de literatura y el trabajo de campo, se establece la relación directa entre vulnerabilidades existentes, amenazas potenciales y riesgos asociados, lo que permite comprender el nivel de exposición de la comunidad.

Principales amenazas cibernéticas

- Phishing (suplantación de identidad): Mensajes fraudulentos a través de WhatsApp, SMS o redes sociales que buscan engañar al usuario para obtener datos personales.
- Malware (software malicioso): Instalación de aplicaciones infectadas que pueden robar información o afectar el funcionamiento del dispositivo.
- Ingeniería social: Manipulación psicológica del usuario para obtener información confidencial, aprovechando la confianza o desconocimiento.
- Robo de identidad digital: Uso indebido de datos personales para suplantar al usuario en plataformas digitales.
- Desinformación digital: Circulación de noticias falsas o contenido engañoso que afecta la toma de decisiones.

Tabla 2 Riesgos Cibernéticos asociados

Riesgos económicos	-Pérdida de dinero por fraudes digitales. -Estafas en plataformas de comercio y transferencias.
Riesgos sociales	-Pérdida de confianza en el uso de tecnologías. -Aislamiento digital o rechazo a las TIC.
Riesgos culturales	-Uso indebido de conocimientos ancestrales o información cultural. -Pérdida de control sobre contenidos propios en entornos digitales.
Riesgos informacionales	-Exposición de datos personales o comunitarios. -Pérdida de información importante.
Riesgos operativos	-Interrupción del uso de dispositivos o servicios digitales. -Dependencia tecnológica sin capacidades de respuesta ante incidentes.

las comunidades indígenas del municipio de San José del Fragua presentan una **alta exposición a riesgos cibernéticos**, producto de la interacción entre vulnerabilidades tecnológicas, humanas y socioculturales. Las amenazas más relevantes, como el phishing, la ingeniería social y el malware, encuentran un entorno propicio para su materialización debido a la baja alfabetización

digital y la limitada infraestructura tecnológica, es fundamental diseñar estrategias que fortalezcan la capacidad de la comunidad para identificar, prevenir y responder ante amenazas, consolidando así un enfoque de resiliencia digital sostenible.

Resultados preliminares.

A partir del Anexo 2 - Matriz de Revisión Bibliográfica se consultaron 15 artículos y documentos relevantes, identificando los siguientes hallazgos:

Tabla 3 Resultados Preliminares

Dimensión	Hallazgos Relevantes	Fuente
Acceso a infraestructura	Conectividad inferior al 5% en comunidades indígenas	Derechos Digitales (2022)
Alfabetización digital	Ausencia de formación tecnológica en su lengua indígena	Global Voices (2023)
Factores culturales	Rechazo a tecnologías por temor a pérdida cultural	ISOC Colombia (2021)
Riesgos cibernéticos	Alta exposición a suplantación de identidad y desinformación	CrimRxiv (2022)

Fuente: Propia

Cierre del objetivo 1

Con el desarrollo del primer objetivo ha permitido establecer una caracterización sólida de la brecha digital en las comunidades indígenas del municipio de San José del Fragua, así como de las vulnerabilidades cibernéticas que se derivan de dicha condición.

El primer objetivo específico del proyecto se articula con el Objetivo nueve (ODS), (Industria, innovación e infraestructura), al promover la equidad en el acceso a las TIC y al conocimiento, la política pública nacional sobre transformación digital, inclusión social y protección de los derechos digitales de poblaciones históricamente marginadas.

La intervención planteada reconoce que la tecnología, por sí sola, no soluciona las desigualdades, se enfoca en un modelo de educación digital contextualizada y participativa, que permita a estas comunidades no solo acceder a internet, sino también usarlo de forma segura y provechosa para sus procesos organizativos, educativos, culturales y productivos. La revisión sistemática aporta un fundamento teórico y empírico para el desarrollo de estrategias de resiliencia digital culturalmente pertinentes.

Los métodos utilizados y herramientas empleadas para la revisión sistemática de literatura fueron artículos científicos, otras fuentes bibliográficas, como libros y tesis relacionadas con la brecha digital.

Capítulo 2

Análisis de factores culturales, sociales y económicos que aumentan la brecha digital y la exposición a riesgos cibernéticos

Describir y analizar cómo los factores culturales, sociales y económicos inciden en la brecha digital y en la exposición a riesgos cibernéticos en las comunidades indígenas Inga del municipio de San José del Fragua, con el fin de proponer estrategias que fortalezcan la resiliencia digital mediante prácticas de ciberseguridad culturalmente adaptadas. Partimos del entendimiento de que la brecha digital no es exclusivamente técnica, se articula con la lengua Inga, los modos de comunicación, las prácticas culturales, las estructuras indígenas, las condiciones económicas, y en su convergencia aumentan las vulnerabilidades frente a amenazas digitales (phishing, suplantación, fraude económico, acoso en línea, etc).

Metodología Aplicada

Enfoque: mixto (cualitativo, cuantitativo) con diseño explicativo, la comunidad esta integrada por 70 personas, la muestra se le realizo a 40 integrantes de la institución educativa de la comunidad indígena, estudiantes entre 14-17 años y los docentes de la institución educativa, aplicando instrumentos de campo acordados con la comunidad indígena.

Técnicas e instrumentos:

a. **Entrevista semiestructurada a líder de la comunidad Inga**

Link: https://www.youtube.com/watch?v=9PJAAnDj1pA

Objetivo de la entrevista:

Recopilar información cualitativa desde la perspectiva del liderazgo comunitario acerca de la situación actual de la infraestructura tecnológica (TIC) en la comunidad indígena, sus necesidades en materia de conectividad, capacitación y seguridad digital, así

como explorar los niveles de resiliencia digital y sostenibilidad alcanzados frente a los desafíos que plantea la brecha digital y los riesgos cibernéticos.

Población objetivo:

Líder de la comunidad indígena Inga, Rafael Soto Jacanamejoy, del Municipio de San José del Fragua, Caquetá, socialización del proyecto, para su comunidad.

Temas de la entrevista:

- Infraestructura TIC comunitaria: estado actual de los recursos tecnológicos, conectividad, acceso a internet, disponibilidad de dispositivos y servicios digitales.
- Resiliencia digital: estrategias comunitarias, saberes o prácticas que promueven el uso responsable y seguro de las tecnologías.
- Sostenibilidad: acciones o propuestas para mantener y fortalecer el acceso y uso de las TIC a largo plazo, alineadas con la identidad cultural de la comunidad.

Guion propuesto de la entrevista (preguntas orientadoras):

1. Infraestructura TIC comunitaria

- ¿Cómo describiría la infraestructura tecnológica actual de la comunidad (acceso a internet, equipos, redes, electricidad, etc.)?

2. Necesidades y desafíos tecnológicos

- ¿Qué limitaciones culturales o lingüísticas dificultan el uso de las TIC entre los miembros de la comunidad?

3. Ciberseguridad y resiliencia digital

- ¿De qué manera las tradiciones o valores del pueblo Inga pueden contribuir a promover una cultura de uso responsable de la tecnología?

4. Sostenibilidad y proyección futura

- ¿Qué acciones considera necesarias para garantizar que el uso de las TIC sea sostenible en el fortalecimiento cultural dentro de la comunidad?

5. Reflexión final

- Desde su experiencia como líder, ¿qué mensaje positivo enviaría a la comunidad que buscan reducir la brecha digital y exposición a riesgos Cibernéticos?

Descripción del análisis:

Con esta entrevista al líder de la comunidad indígena Rafael Soto Jacanamejoy, nos permitió identificar las condiciones reales de infraestructura tecnológica y las brechas más críticas en su comunidad, comprender las percepciones culturales sobre la tecnología y la seguridad digital, evaluando el grado de resiliencia y sostenibilidad alcanzado por la comunidad frente a los cambios tecnológicos y riesgos cibernéticos, así validamos las estrategias propuestas en el proyecto, asegurando que sean culturalmente pertinentes y sostenibles a largo plazo.

b. Encuesta estructurada sobre uso de las TIC y prácticas de Ciberseguridad.

La comunidad Inga está conformada por 70 personas, las encuestas se aplicaron a un total de 40 participantes matriculados a la institución educativa del pueblo Inga, distribuidos en dos grupos: estudiantes (70%) y docentes (30%). El propósito fue identificar el uso de las TIC y conocimientos básicos sobre ciberseguridad. Los formularios se diseñaron en Google Forms y estuvieron disponibles durante una semana.

Objetivo general:

Evaluar el nivel de conocimiento, uso responsable y prácticas de ciberseguridad entre estudiantes y profesores de la Institución Educativa del Pueblo Inga, para identificar vulnerabilidades y fortalecer la cultura digital segura dentro de la comunidad Inga.

Población objetivo:

- ✓ Estudiantes: entre 14 y 17 años (bachillerato).
- ✓ Docentes: de todas las áreas y edades.

Muestreo:

Dos grupos:

- ✓ Estudiantes 40,
- ✓ Docentes 10.

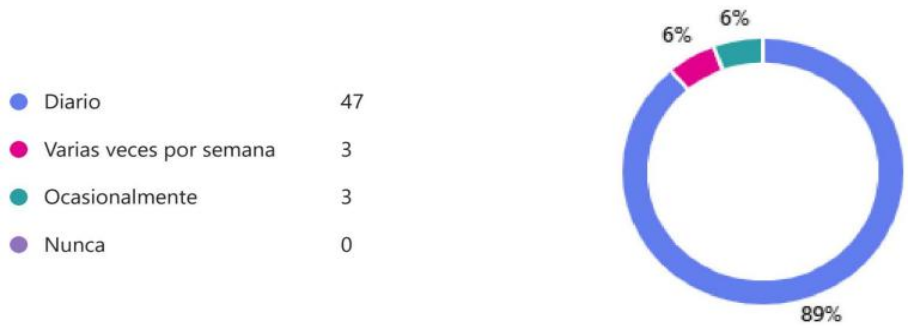
1. Uso de las TIC

https://forms.office.com/pages/responsepage.aspx?id=elQA_LskT06dYXP8peud86TJ3tUVhblKiccd8A7My4tUNFRWOENTVzA0Sjc1WkJFVjZNOERKV0lKRy4u&origin=lprLink&route=shorturl

Análisis de resultados

¿Con qué frecuencia utiliza dispositivos digitales (celular, computador, tablet)?

Figura 1Uso de Dispositivos Digitales



Fuente: elaboración propia a partir de resultados de encuesta.

El gráfico muestra que el 89% utiliza con frecuencia dispositivos digitales, mientras el 6% varias veces por semana y ocasionalmente, esto evidencia que el acceso a la tecnología depende en gran medida de los dispositivos móviles, lo cual están más expuestos a riesgos cibernéticos, (MinTic, 2025), La Estrategia Nacional de Seguridad Digital de Colombia 2025-2027 se presenta como una respuesta integral y proactiva a los desafíos y oportunidades que surgen en un entorno digital en constante evolución. Esta estrategia se construye sobre los cimientos establecidos por los documentos CONPES 3701 de 2011, 3854 de 2016 y 3995 de 2020, los cuales han guiado la política de seguridad digital del país en la última década. Reconociendo los avances logrados y las lecciones aprendidas, esta nueva estrategia busca fortalecer la postura de Colombia en materia de seguridad digital, adaptándose a las amenazas emergentes y aprovechando las innovaciones tecnológicas para crear un ciberespacio más seguro y resiliente.

Según el informe de análisis estadístico (LEE, 2025), de la Pontificia Universidad Javeriana, el acceso a dispositivos digitales con pantalla en el hogar constituye una condición

habilitante fundamental para el aprendizaje apoyado en tecnología, especialmente en contextos de transformación digital acelerada como el actual.

Para continuidad de la resiliencia digital se propone implementar una segunda encuesta complementaria, más detallada, con preguntas que profundicen en:

Percepción de riesgo y confianza digital.

- ✓ Experiencias previas con incidentes cibernéticos.
- ✓ Factores culturales que influyen en el uso de la tecnología.

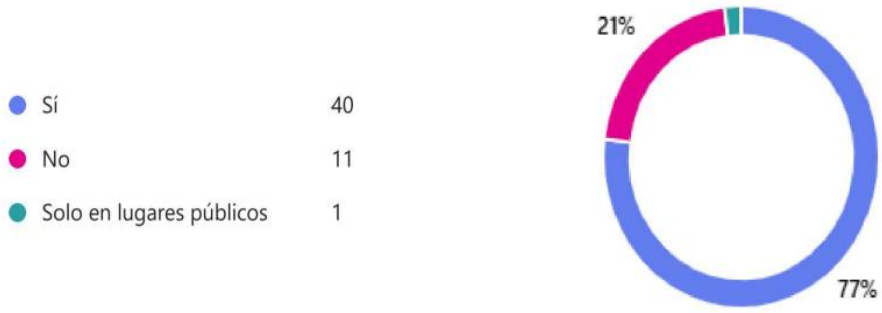
Esta segunda encuesta permitirá:

- ✓ Obtener información más precisa y cuantificable.
- ✓ Contrastar los datos con los resultados de la primera encuesta.
- ✓ Captar cambios generados tras las capacitaciones.

Se aclara en el informe que la encuesta original fue diagnóstica, y la complementaria funciona como instrumento de profundización y verificación del impacto.

¿Cuenta con acceso a internet?

Figura 2 Acceso a internet



Fuente: elaboración propia a partir de resultados de encuesta

El gráfico muestra el nivel de acceso regular a Internet, el 77%, un 21% indicó no tener conexión y el 2% en lugares públicos. Entre quienes sí tienen acceso, la mayoría utiliza datos móviles (75%), mientras que solo un 15% dispone de conexión institucional y 10% red Wi-Fi.

Para fortalecer el análisis del proyecto, es indispensable articular los resultados obtenidos con una reflexión profunda sobre las condiciones reales de conectividad en la comunidad indígena y cómo estas situaciones incrementan los riesgos cibernéticos, afectan su resiliencia digital y limitan la adopción de prácticas seguras, en zonas rurales donde se ubica la comunidad indígena del Municipio de San José del Fragua, la conectividad suele ser:

- Intermitente
- Basada en redes móviles de baja capacidad
- Sujeta a la falta de infraestructura y equipos adecuados
- En ocasiones realizada mediante redes públicas o compartidas.
- Articulación entre conectividad y riesgos de ciberseguridad.

Uno de los factores críticos identificados durante el análisis es la intermitencia en el acceso a internet y el uso frecuente de medios alternativos de conexión, como redes móviles de baja capacidad, puntos Wi-Fi comunitarios y conexiones compartidas entre varias familias. Estas condiciones no solo limitan la continuidad de las actividades formativas y el acceso regular a plataformas digitales, sino que incrementan significativamente los riesgos y amenazas de ciberseguridad a los que la comunidad está expuesta.

La inestabilidad de la conectividad provoca que los usuarios recurran a prácticas riesgosas como:

- ✓ Suplantación de redes Wi-Fi (ataques “Evil Twin”)
- ✓ Intercepción de datos (sniffing)

- Instalación de software malicioso en dispositivos compartidos

✓ Phishing y smishing,

✓ Robo de información personal debido a conexiones inseguras

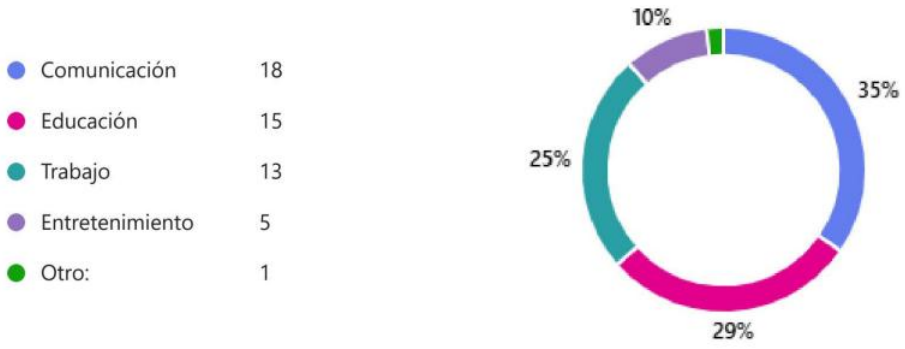
✓ Secuestro de cuentas por contraseñas débiles o reutilizadas

✓ Acceso no autorizado a dispositivos comunitarios

Estos riesgos deben integrarse al análisis de resultados, ya que afectan directamente la capacidad de la comunidad para adoptar las prácticas de ciberseguridad enseñadas durante el proyecto. Una formación adecuada no puede ser efectiva si las condiciones tecnológicas no permiten aplicarla de manera segura.

¿Para qué actividades usa principalmente la tecnología?

Figura 3 Uso de las TIC

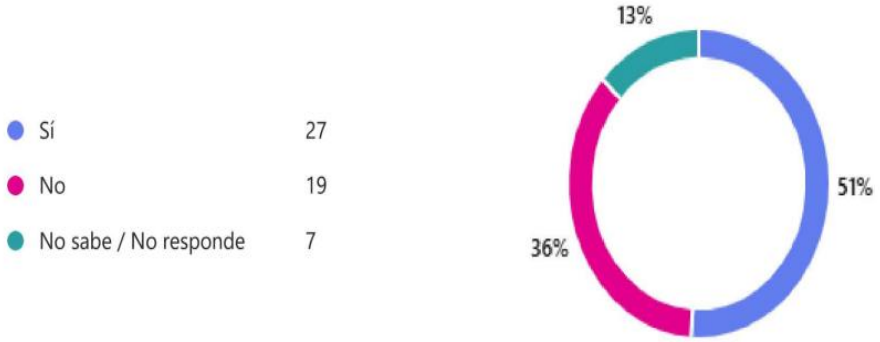


Fuente: elaboración propia a partir de resultados de encuesta

El gráfico muestra que el uso principal, es la comunicación como lo son las redes sociales (35%), Educación (29%) y en menor proporción como se observan actividades relacionadas trabajos (25%), entretenimiento (10%).

¿Ha sido víctima de algún ataque cibernético?

Figura 4 Víctima de ataques cibernéticos



Fuente: elaboración propia, resultados de encuesta

Los resultados evidencian que el 51% de la población ha experimentado algún tipo de ataque cibernético, lo cual demuestra un nivel significativo de exposición a riesgos digitales. Esto puede estar relacionado la carencia de medidas básicas de protección digital y capacitación en ciberseguridad.

Análisis de factores culturales

Percepción de la tecnología y la ciberseguridad: la tecnología es percibida mayoritariamente como herramienta instrumental, de comunicación, comercio local, acceso a trámites y educación. La noción de "ciberseguridad" aparece en el vocabulario popular como "cuidar el celular" o "no abrir links raros", lo cual indica una comprensión práctica pero parcial de riesgos más amplios (protección de identidad digital, privacidad de saberes, metadatos). Implicación: Las intervenciones deben traducir los conceptos técnicos a prácticas cotidianas relevantes y en protección de conocimientos propios.

Lengua, tradición y mediaciones culturales: el bilingüismo inga–español condiciona la recepción de mensajes técnicos, mensajes y materiales exclusivamente en español técnico tienen baja efectividad; la transmisión tradicional a través de autoridades (Gobernador, Taitas) es clave

para legitimidad. Además, existen protocolos culturales de reserva sobre saberes, prácticas y lugares sagrados que requieren protección frente a la divulgación digital como (fotografías, audios, geolocalización).

Barreras culturales identificadas:

- Normas culturales que restringen la difusión de ciertos saberes tradicionales, sin mecanismos digitales de control.
- Desconfianza hacia actores externos y plataformas comerciales.
- Autoridad del Cabildo como puerta de entrada a innovaciones

Diagnostico social:

La escolaridad presenta variabilidad, quienes alcanzaron educación secundaria muestran mayor manejo de herramientas básicas y mejores prácticas, mientras que quienes no completaron la primaria presentan barreras significativas para la lectura de mensajes técnicos o el uso seguro de APPS o plataformas digitales.

La comunidad estudiantil reporta uso intenso de redes sociales y plataformas digitales, también víctimas de ataques cibernéticos como el acoso, chantaje y fraude digital, los profesores influyen en tiempo disponible para formación, las estrategias deben mejorar, enseñando medidas de protección específicas.

Es necesario fortalecerla incorporando lineamientos de la ISO/IEC 27001:2022, especialmente aquellos controles relacionados con la cibercultura, concienciación y comportamiento seguro de los usuarios. Esta norma establece que la seguridad de la información no solo depende de tecnologías o infraestructuras, sino también del factor humano, señalando la necesidad de implementar controles orientados a la formación, sensibilización y establecimiento de prácticas seguras en los diferentes actores del entorno educativo.

Controles como el 5.1 (Políticas de seguridad de la información), 6.3 (Responsabilidades de seguridad en tareas específicas), 6.5 (Concienciación, educación y formación en seguridad de la información) y 8.28 (Gestión de vulnerabilidades técnicas) permiten darle rigor al análisis, ya que ofrecen un marco de referencia para evaluar el nivel de exposición de la comunidad educativa frente a riesgos asociados al uso de TIC, la navegación en internet, la protección de datos personales y el manejo seguro de dispositivos.

Integrar estos lineamientos permitirá argumentar con mayor profundidad cómo las brechas tecnológicas, la falta de cultura digital o las prácticas inseguras pueden incrementar la probabilidad de incidentes, tales como ciberacoso, suplantación de identidad, robo de información, accesos no autorizados o exposición a contenidos nocivos. Además, aporta claridad sobre la importancia de adoptar estrategias de resiliencia digital que preparen a estudiantes y docentes para identificar, prevenir y responder a amenazas, alineándose con un estándar internacionalmente reconocido.

Identificación de activos críticos

- ✓ Equipos tecnológicos computadores, celulares.
- ✓ Conectividad de la red Wi-Fi de la institución educativa
- ✓ Información digital de la institución educativa y comunidad Inga.
- ✓ Desconocimiento en TIC y ciberseguridad.

Identificación de amenazas

- ✓ Ataques de phishing o robo de contraseñas.
- ✓ Aplicaciones no seguras instaladas en dispositivos móviles.
- ✓ Suplantación de identidad en redes sociales.
- ✓ Pérdida de información Digital.
- ✓ Desinformación digital o manipulación de contenidos.

Vulnerabilidades encontradas:

La falta de recursos económicos limita la renovación de dispositivos tecnológicos, acceso a servicios digitales seguros, muchas familias comparten dispositivos, lo que aumenta la exposición ataques cibernéticos o suscripciones a servicios de protección digital.

La intermitencia de la red y el alto costo del dato provocan que las actualizaciones de seguridad y parches no se realicen oportunamente, incrementando el riesgo de explotación, el uso de Wi-Fi público o redes abiertas también amplifica vectores de ataque.

El uso de redes sociales WhatsApp y Facebook aumenta el riesgo de fraude y suplantación, si un mecanismo de verificación o de seguridad deja a las comunidades vulnerables a estafas.

Falta de cultura en ciberseguridad (cibercultura insuficiente)

Los estudiantes y docentes no cuentan con conocimientos sólidos sobre amenazas digitales, buenas prácticas de seguridad, protección de datos y navegación segura.

Cómo mitigarlo:

- ✓ Programas continuos de capacitación en ciberseguridad (ISO 27001).
- ✓ Campañas de sensibilización y charlas periódicas.
- ✓ Talleres prácticos sobre phishing, contraseñas, redes sociales.
- ✓ No utilizar contraseñas débiles o reutilizadas.
- ✓ Actualización de credenciales periódicamente.
- ✓ Falta de actualización de software y sistemas operativos.
- Riesgo alto en redes sociales
- Seguimiento con docentes orientadores de la institución educativa.
- No hay control del acceso físico y digital
- Supervisión adulta en menores de edad.

Estrategias para fortalecer la resiliencia Digital

- a. Campañas educativas sobre ciberseguridad.

Fecha: 5 de septiembre de 2025

Duración: 6 horas

Facilitador: Ingeniero Especialista en Seguridad Informática.

Participantes:

- ✓ Estudiantes: entre 14 y 17 años (bachillerato).
- ✓ Docentes de todas las áreas.

Muestreo:

Dos grupos:

- ✓ Estudiantes 40,
- ✓ Docentes 10.

Figura 5 Encuesta comunidad educativa Inga

Fuente: Propia

Descripción: En la figura 5 se observa el proceso de aplicación de estrategias para fortalecer la resiliencia digital en la Institución Educativa Inga, la actividad fue desarrollada con la participación de estudiantes entre 14 y 17 años y docentes, quienes colaboraron en un ambiente de aprendizaje participativo y de diálogo participativo.

Durante la jornada, los participantes respondieron preguntas orientadas a identificar sus hábitos digitales, nivel de conocimiento sobre ciberseguridad, acceso a internet y uso dispositivos tecnológicos. Esta actividad permitió recopilar información valiosa sobre las necesidades tecnológicas y la capacidad de respuesta digital de la población Inga, fortaleciendo así el proceso de diagnóstico del proyecto.

La escena refleja un espacio de intercambio de saberes y sensibilización del uso de las TIC, donde los estudiantes muestran interés en comprender cómo proteger su información personal, mientras los docentes acompañan y orientan la dinámica, fomentando una cultura de seguridad digital y uso responsable de las TIC, asimismo se evidencia la integración de estrategias pedagógicas culturalmente pertinentes, que promueven el uso consciente, ético y sostenible de la tecnología dentro del contexto educativo indígena, contribuyendo al cierre de la brecha digital y al fortalecimiento de la resiliencia comunitaria frente a los riesgos cibernéticos.

Link video: https://www.youtube.com/watch?v=1RkrdLnQQ3I

Link video: https://youtube.com/shorts/sLBTYeXdVfQ

- **b. Introducción a la Cibercultura y Riesgos Digitales.**

Fecha: 12 de septiembre de 2025

Duración: 2 horas

Participantes: 35 estudiantes de 14 y 17 años

Facilitador: Ingeniero Especialista en Seguridad Informática

Actividades:

- ✓ Exposición interactiva sobre amenazas comunes (phishing, ingeniería social, ciberacoso).
- ✓ Actividad grupal: “Detecta el riesgo” utilizando ejemplos de redes sociales.

Resultado esperado:

- ✓ Identificación básica de amenazas cibernéticas.

- **c. Uso Seguro de Internet y Redes Sociales**

Fecha: 26 de septiembre de 2025

Duración: 3 horas

Participantes: Estudiantes y docentes

Responsable: Equipo de Ciberseguridad del proyecto

Actividades:

- ✓ Configuración de privacidad en WhatsApp, Facebook e Instagram.
- ✓ Ejercicio práctico: creación de contraseñas robustas.
- ✓ Dinámica lúdica, “La cadena de seguridad”.

Resultado esperado:

- ✓ Reducir riesgos asociados a malas prácticas digitales.

Análisis de las estrategias implementadas de presaberes y fortalecimiento de la cibercultura en la comunidad Inga

El análisis evidencia que la brecha digital en la población Inga del Municipio de San José del Fragua es el resultado de una interacción compleja entre factores culturales (idioma,), sociales (educación, género) y económicos (pobreza, infraestructura tecnológica). Estas condiciones no solo limitan el acceso y la apropiación tecnológica, sino que amplifican la exposición a riesgos cibernéticos concretos.

Para fortalecer la resiliencia digital es imprescindible diseñar estrategias integrales y culturalmente adaptadas que combinen alfabetización bilingüe, gobernanza comunitaria, prácticas técnicas viables y mecanismos de economía digital segura, todo ello legitimado y liderado por las autoridades y redes de confianza locales.

Este proceso de intervención desarrollado en la comunidad indígena partió de los resultados obtenidos en las encuetas realizadas a la comunidad educativa Inga los conocimientos previos, experiencias y prácticas culturales que los participantes poseen en relación con el uso de las tecnologías de la información y la comunicación (TIC), permitiendo diseñar estrategias pedagógicas pertinentes, respetuosas de la cosmovisión indígena y alineadas con sus dinámicas sociales y culturales.

a) Análisis de los presaberes identificados

Durante la fase inicial, mediante encuestas, entrevistas y observación directa, se identificaron los siguientes aspectos:

✓ Conocimientos previos

- Uso básico de dispositivos móviles, principalmente para redes sociales y mensajería (WhatsApp, Facebook).
- Familiaridad con el acceso a internet a través de datos móviles o redes compartidas.
- Bajo conocimiento sobre conceptos de ciberseguridad (phishing, malware, privacidad digital).

✓ Prácticas culturales relacionadas con la tecnología

- Uso comunitario de dispositivos (compartición de celulares).

- Confianza en redes de comunicación cercanas (familia y comunidad).

✓ Limitaciones identificadas

- Falta de formación en seguridad digital.
- Desconocimiento de riesgos cibernéticos.
- Uso de contraseñas débiles o inexistentes.
- Baja apropiación de herramientas tecnológicas con fines educativos o productivos.

b) Estrategias implementadas para fortalecer la cibercultura

✓ Talleres formativos contextualizados

- Adaptación del lenguaje técnico a términos comprensibles.
- Uso de ejemplos reales del entorno comunitario.
- Integración de la cultura Inga en los contenidos digitales.

✓ Actividades didácticas y experienciales

- Juegos para identificar riesgos digitales.
- Simulación de ataques (phishing).
- Ejercicios prácticos de configuración de privacidad y contraseñas.

✓ Estrategias de aprendizaje colaborativo

- Trabajo en grupo y discusión de casos.
- Participación de líderes comunitarios como traductores.

- Espacios de diálogo y reflexión colectiva.

✓ Material pedagógico accesible

- Uso de infografías, imágenes y ejemplos visuales.
- Contenidos simplificados y adaptados al nivel educativo de la comunidad.

c) Impacto en el fortalecimiento de la cibercultura

✓ Mejora en conocimientos

- Mayor comprensión de conceptos básicos de ciberseguridad.
- Reconocimiento de amenazas digitales comunes.

✓ Cambio en comportamientos digitales

- Uso de contraseñas más seguras.
- Mayor precaución al abrir enlaces o mensajes desconocidos.

✓ Fortalecimiento de la conciencia digital

- Incremento en la percepción del riesgo digital.
- Mayor responsabilidad en el uso de las TIC.
- Interés en continuar procesos de formación digital.

✓ Apropiación cultural de la tecnología

- Integración del concepto de “cuidado del territorio” aplicado al entorno digital.
- Uso de las TIC como herramienta de desarrollo comunitario.

d) **Evaluación de las estrategias implementadas.**

- Su **adaptación al contexto cultural Inga**.
- El uso de metodologías participativas y prácticas.
- La incorporación de los presaberes como base del aprendizaje.
- La generación de confianza entre facilitadores y comunidad.

Esto permitió que la comunidad no solo adquiriera conocimientos, sino que también desarrollara habilidades y actitudes orientadas a una cibercultura responsable y resiliente.

El fortalecimiento de la cibercultura en la comunidad Inga demuestra que los procesos de formación en ciberseguridad son más efectivos cuando parten del reconocimiento de los presaberes y se adaptan al contexto sociocultural.

Las estrategias implementadas lograron generar cambios significativos en el conocimiento, las prácticas y la percepción del riesgo digital, contribuyendo a la construcción de una comunidad más informada, consciente y preparada frente a los desafíos del entorno digital.

Capítulo 3

Evaluación de la efectividad de las estrategias propuestas, resiliencia digital en comunidades indígenas.

Se evalúa la efectividad de las estrategias propuestas, seleccionando dos grupos de la población inga como objeto de estudio representativos de la comunidad estudiantil indígena y se aplicará un diagnóstico inicial sobre su nivel de vulnerabilidad digital y prácticas de ciberseguridad.

Posteriormente, se implementarán las estrategias de resiliencia adaptadas culturalmente (capacitaciones, campañas, etc.), se evaluará el impacto a través de encuestas, entrevistas y observaciones para medir los cambios en habilidades digitales y percepción de riesgos.

Los resultados pre y post intervención serán analizados comparativamente, sistematizando aprendizajes y documentando buenas prácticas, midiendo la efectiva del impacto en la población, se emplea el siguiente instrumento de evaluación centrados en el conocimiento y las habilidades prácticas con el fin de concluir sobre la efectividad de las estrategias y proponer recomendaciones para futuras intervenciones.

Instrumentos de evaluación

los instrumentos se realizarán a partir de la información recolectada en las fases anteriores, de modo que se garantice pertinencia cultural y aplicabilidad comunitaria, acciones estarán dirigidas principalmente a jóvenes y docentes de la institución educativa de la comunidad, como agentes multiplicadores del conocimiento digital.

Instrumentos Tipo Test o Evaluación:

Preguntas de Selección Múltiple con Múltiple Respuesta: Este formato requiere que el participante identifique varias opciones correctas para una sola pregunta, obligándolo a tener un conocimiento más profundo y matizado del tema, no solo una identificación superficial.

Talleres Temáticos y Evaluativos:

Diseño de ejercicios prácticos que requieran la aplicación de conceptos de ciberseguridad, identificar un correo de phishing, configurar contraseñas seguras, clasificar tipos de amenazas cibernéticas. La evaluación se centra en la ejecución correcta de la tarea.

Dinámicas de Grupo y Casos Reales:

Se presenta a los grupos escenarios de ciberseguridad que podrían enfrentar un ataque de ransomware, evaluando el proceso de toma de decisiones, la estrategia de mitigación y la respuesta comunicativa del equipo ante la crisis, esto mide la habilidad para aplicar el conocimiento bajo presión y en un contexto de equipo.

Las encuestas realizadas solo miden la sensación subjetiva del participante sobre su propio aprendizaje o la utilidad de la capacitación, no permite medir de verdad si el conocimiento fue impactado y si la persona es ahora capaz de actuar de manera más segura, los instrumentos propuestos, por el contrario, ofrecen datos cuantitativos y cualitativos sobre el dominio real del tema. "Considera que sabe más de ciberseguridad".

Para evaluar la efectividad del proceso fue necesario aplicar diversas metodologías activas que promovieran la participación comunitaria y permitieran medir cambios reales en las actitudes, conocimientos y comportamientos digitales.

a) Talleres formativos basados en el Objetivo 2

Los talleres desarrollados anteriormente no solo fueron actividades de capacitación, sino también insumos evaluativos donde se evaluó:

- ✓ Comprensión de conceptos clave.
- ✓ Cambio en las prácticas digitales.
- ✓ Nivel de participación individual y grupal.

b) Actividades didácticas para medir los conceptos de ciberseguridad

Cada taller incluyó dinámicas que permitieron evaluar la apropiación de conceptos mediante experiencias prácticas:

- ✓ Evaluación de la capacidad para identificar amenazas.
- ✓ Simulación de phishing: permitió medir cuántos participantes podían reconocer un ataque.
- ✓ Ejercicio evaluación de habilidades para crear claves robustas.
- ✓ Dinámica de privacidad en redes sociales.

c) Conversatorios y reflexiones comunitarias

- ✓ Debates guiados.
- ✓ Reflexiones grupales sobre experiencias previas de riesgo digital.
- ✓ Percepciones frente a su propio nivel de conocimiento.

Instrumentos de medición:

La efectividad se midió mediante tres fuentes principales:

a. Evidencias de participación y aprendizaje

- ✓ Listas de asistencia de cada taller.
- ✓ Actividades prácticas desarrolladas por los estudiantes.
- ✓ Productos entregados (instructivos).

b. Observación directa y retroalimentación comunitaria

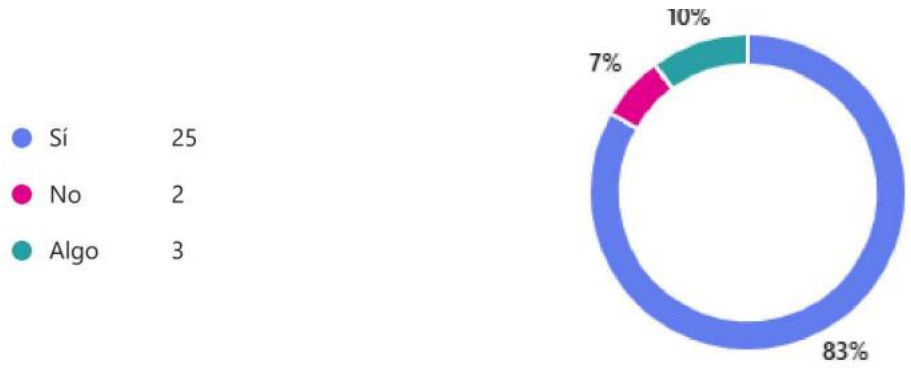
- ✓ Durante talleres y actividades prácticas se evaluó:
- ✓ Participación activa de los jóvenes.
- ✓ Preguntas y casos reales planteados por los estudiantes.
- ✓ Resultados de ejercicios de identificación de amenazas.
- ✓ Comentarios de docentes sobre continuidad de las prácticas seguras.

c. Encuesta Formulario Google Forms - Practicas de Ciberseguridad

- https://forms.office.com/pages/responsepage.aspx?id=elQA_LskT06dYXP8peud86TJ3tUVhblKiccd8A7My4tUOFFORlZCVkZPR1o5MUdJVE05RU5KQlYzRC4u&origin=lprLink&route=shorturl

¿ahora si entiende la definición de ciberseguridad?

Figura 6 Definición de Ciberseguridad



Fuente: elaboración propia, resultados de encuesta.

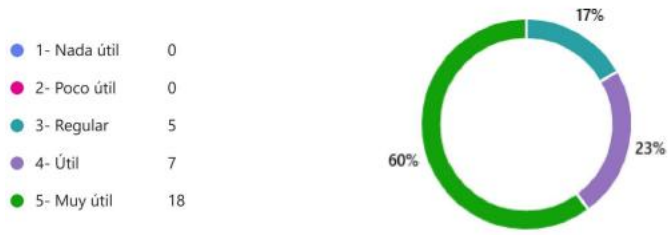
Después de las campañas sobre ciberseguridad, los resultados reflejan que el 83% de los encuestados, afirmó comprender claramente el concepto de ciberseguridad tras la estrategia implementada, el 10% manifestó tener una comprensión parcial, mientras que un 7% aún no logra identificar con claridad el significado del término.

Estos resultados indican que las estrategias implementadas —como las campañas educativas sobre ciberseguridad fueron efectivas para mejorar el conocimiento y la apropiación del concepto de ciberseguridad dentro de la comunidad educativa indígena.

El alto porcentaje de comprensión (83%) evidencia un avance significativo en la resiliencia digital, demostrando que, cuando los contenidos se explican con ejemplos cercanos a la vida cotidiana y se adaptan a la cultura local, los participantes logran interiorizar las nociones clave de seguridad digital.

¿considera importante el proceso de formación para prevenir ataques cibernéticos?

Figura 7 Proceso de Formación Ciberseguridad



Fuente: elaboración propia, resultados de encuesta.

Los datos reflejan que el 60% considera que la formación en ciberseguridad es muy importante como mecanismo de prevención frente a ataques digitales dentro de la comunidad educativa Inga, lo que demuestra una conciencia creciente sobre la necesidad de aprender a protegerse en el entorno digital.

El hecho de que seis de cada diez participantes valoren altamente estos procesos indica que las acciones pedagógicas implementadas en el marco del proyecto han sido bien recibidas y comprendidas.

¿Las estrategias para fortalecer la resiliencia digital fueron adaptadas a la comunidad?

Figura 8 Resiliencia Digital

Fuente: elaboración propia, resultados de encuesta

Los resultados reflejan que un 97% considera que sí fueron adaptadas adecuadamente, un 3% manifiesta que las estrategias no fueron completamente acordes a las necesidades culturales o tecnológicas de la comunidad, estos resultados indican que más de la mitad de los encuestados percibe positivamente la adaptación de las estrategias digitales, lo cual sugiere que las actividades implementadas como las campañas en ciberseguridad y uso responsable de las TIC lograron conectar con la realidad sociocultural del pueblo Inga.

Indicadores:

- Reducción de incidentes reportados.
- Incremento en adopción de prácticas seguras.
- Cumplimiento de protocolos culturales en el uso de TIC.

Resultados

Para el cumplimiento de este objetivo, se procederá a estructurar un conjunto de estrategias pedagógicas, tecnológicas y organizativas orientadas a fortalecer la resiliencia digital de la comunidad Inga en el municipio de San José del Fragua. Dichas estrategias contemplan la alfabetización digital, campañas en ciberseguridad adaptadas a la realidad cultural Inga.

Se propone la aplicación de talleres presenciales y virtuales enfocados en:

- Uso básico de herramientas tecnológicas (Internet, correo electrónico, redes sociales).
- Identificación de riesgos cibernéticos más frecuentes (phishing, ciberacoso, robo de identidad).
- Implementación de medidas preventivas de seguridad digital (uso de contraseñas seguras, respaldo de información, autenticación en dos pasos).

Efectividad de estrategias implementadas en la comunidad Inga

Los resultados permitieron ajustar los contenidos de las capacitaciones para responder de manera específica a las necesidades detectadas en la comunidad.

La simulación de un ciberataque fue la estrategia más efectiva porque logró transformar el conocimiento en acción, fortaleciendo la resiliencia digital de la comunidad Inga mediante el desarrollo de habilidades prácticas, conciencia del riesgo y toma de decisiones seguras en entornos digitales, permitió pasar del conocimiento teórico a la práctica, generando cambios reales en el comportamiento digital de los participantes. Su enfoque experiencial, contextualizado y participativo facilitó la apropiación de prácticas seguras.

La simulación consistió en recrear escenarios reales de amenazas digitales a los que la comunidad está expuesta, tales como:

- Mensajes falsos de WhatsApp solicitando información personal

- Enlaces fraudulentos (phishing)
- Solicitudes engañosas de códigos o contraseñas
- Descarga de aplicaciones no seguras

Durante la actividad, los participantes debían identificar el riesgo, tomar decisiones y justificar su respuesta, lo que permitió evaluar su comportamiento en tiempo real.

Impacto en la reducción de vulnerabilidades

- Disminuir vulnerabilidades principalmente por errores humanos
- Reducción del uso de enlaces desconocidos
- Disminución de la confianza en mensajes sospechosos
- Mayor uso de contraseñas seguras
- Incremento en la verificación de información

Esto evidencia que la estrategia contribuyó directamente a cerrar brechas de conocimiento y comportamiento digital inseguro dejando cambios significativos en la comunidad:

- Mayor capacidad para identificar amenazas como phishing
- Incremento en la confianza para enfrentar riesgos digitales
- Adopción de prácticas básicas de seguridad (no compartir datos)
- Uso más consciente y responsable de dispositivos móviles
- Mejora en la seguridad digital individual y colectiva.

Se observó una mejora inmediata en la toma de decisiones digitales, como no abrir enlaces desconocidos o no compartir información personal, demostraron mayor seguridad y confianza al enfrentar situaciones simuladas, generando aprendizaje significativo fortaleciendo la resiliencia digital al permitir que la comunidad:

- Anticipe posibles ataques

- Reaccione de forma adecuada ante amenazas
- Aprenda de los errores en un entorno controlado
- Desarrolle autonomía en el uso seguro de las TIC
- Empoderamiento comunitario.

La pertinencia cultural fue el factor que más potenció la adopción, la traducción a lengua Inga, la participación de líderes traductores garantizaron legitimidad y comprensión.

La evaluación de la efectividad permitió comprobar que las estrategias implementadas sí generaron un impacto real, formativo y medible en la comunidad indígena participante, la comunidad no solo respondió encuestas, sino que participó activamente en procesos formativos, experimentó actividades prácticas y recibió materiales educativos que fortalecieron su resiliencia digital, una comunidad más consciente, preparada y protegida frente a los riesgos cibernéticos, cumpliendo satisfactoriamente con los resultados esperados.

Capítulo 4

Diseñar un plan de recomendaciones en resiliencia digital, que integre prácticas de ciberseguridad culturalmente pertinentes, sostenibles y replicables a otras comunidades indígenas, contribuyendo a la reducción de la brecha digital.

Este capítulo presenta un conjunto de recomendaciones prácticas y lineamientos estratégicos para fortalecer la resiliencia digital en comunidades indígenas del municipio de San José del Fragua, dicho plan hace parte de los resultados obtenidos en lo objetivos del proyecto.

La implementación de prácticas de ciberseguridad culturalmente pertinentes, sostenibles y replicables, que contribuyan a reducir la brecha digital y promuevan el uso seguro, responsable y autónomo de las TIC.

El objetivo no es solo cerrar brechas tecnológicas, sino también empoderar a la comunidad indígena para la incorporación de prácticas de seguridad digital y evitar las amenazas cibernéticas que se presentan a diario, respetando sus tradiciones culturales.

Ejes estratégicos del plan de resiliencia digital.

Diseñar, implementar y mantener un plan Integral de Fortalecimiento de la Resiliencia Digital Comunitaria, que consolide los resultados obtenidos en las fases anteriores del proyecto, asegurando su continuidad y adaptación a lo largo plazo. Este plan contempla:

- **Capacitación periódica en ciberseguridad y uso ético de las TIC.**

Es un proceso de formación continua dirigido a estudiantes, docentes, líderes y miembros de la comunidad indígena Inga, busca fortalecer competencias en el uso seguro, responsable y ético de las tecnologías, integrando elementos culturales y prácticas comunitarias.

Etapa 1: Diagnóstico previo

- ✓ Identificación del nivel actual de conocimientos.

- ✓ Reconocimiento de prácticas digitales inseguras predominantes.
- ✓ Detección de brechas culturales o lingüísticas que deban ser adaptadas.

Etapa 2: Diseño del programa de formación

- ✓ Construcción de módulos basados en las necesidades detectadas.
- ✓ Adaptación del contenido a la cultura Inga (lenguaje).
- ✓ Elaboración de material didáctico.

Etapa 3: Ejecución de los talleres

- ✓ Sesiones mensuales de 4 horas, presenciales.
- ✓ Actividades prácticas:
- ✓ talleres sobre contraseñas seguras.
- ✓ simulaciones de phishing.
- ✓ Ejercicios sobre privacidad.

Etapa 4: Evaluación inmediata

- ✓ Aplicación de cuestionarios cortos.
- ✓ Ejercicios prácticos para medir competencias adquiridas.

- **Actualización constante de los contenidos formativos según nuevas amenazas digitales.**

Este componente garantiza que el material utilizado en capacitaciones se mantenga vigente frente a nuevas ciber amenazas, técnicas de fraude, vulnerabilidades tecnológicas y tendencias globales, en concordancia con normas como ISO 27001 e ISO 27002 (controles A.5, A.6, A.7 y A.12 asociados a cibercultura y concienciación).

Etapa 1: Monitoreo de amenazas

-Identificación de amenazas emergentes relevantes para zonas rurales:

- ✓ Fraudes por WhatsApp
- ✓ Robo de datos por redes WiFi-públicas
- ✓ Virus mediante memorias USB
- ✓ Suplantación de identidad para subsidios o ayudas

Etapa 2: Actualización del contenido

- ✓ Revisión del Manual de Resiliencia Digital.
- ✓ Actualización de guías, infografías y talleres.
- ✓ Inclusión de nuevos ejercicios prácticos.

- **Seguimiento y evaluación mediante indicadores de impacto y sostenibilidad.**

Se trata de un sistema formal para medir la evolución del proyecto, la apropiación comunitaria y la reducción de riesgos digitales. Incluye indicadores cuantitativos, cualitativos y de sostenibilidad cultural.

Etapa 1: Definición de indicadores

- ✓ Adopción de prácticas seguras.
- ✓ Reducción de incidentes de ciberseguridad.
- ✓ Participación estudiantil.
- ✓ Actualización del material.

Etapa 2: Recolección de información

- Encuestas semestrales.
- Entrevistas con docentes y líderes.
- Observación de hábitos digitales en los talleres.
- Registro de incidentes reportados.

Etapa 3: Análisis de resultados

- Identificación de avances en resiliencia digital.
- Detección de nuevas vulnerabilidades.

- Ajustes necesarios al programa de capacitación.

Etapa 4: Retroalimentación y mejora

- Presentación de resultados a toda la comunidad.
- Aplicación de mejoras en contenidos y metodologías.
- Articulación con entidades externas según los resultados.

Documento o producto clave:

a) Manual de Resiliencia Digital Comunitaria

- Documento principal que incluirá:
- Buenas prácticas de ciberseguridad adaptadas a contextos rurales e indígenas.
- Protocolos de respuesta ante incidentes cibernéticos.
- Lineamientos para la sostenibilidad tecnológica y cultural.
- Herramientas prácticas (guías, infografías y recursos visuales).

b) Plan de capacitación continua en ciberseguridad

- **Duración total:** 40 horas.
- **Modalidad:** Presencial con apoyo virtual (plataforma Moodle o Google Classroom).
- **Módulos propuestos:**

    1. Introducción a las TIC y seguridad digital (8 horas)
    2. Ciber amenazas comunes en contextos educativos e indígenas (8 horas)
    3. Buenas prácticas de seguridad digital (8 horas)
    4. Herramientas para la protección de datos personales (8 horas)
    5. Cultura digital y resiliencia comunitaria (8 horas)

Cada módulo incluirá actividades prácticas, dinámicas participativas y materiales en lenguaje accesible y culturalmente pertinente.

Plan específico de ejecución y seguimiento:

Tabla 4 Plan de ejecución

Etapa	Actividad principal	Periodicidad	Responsable	Producto o evidencia
Implementación	Talleres y capacitaciones sobre resiliencia digital	Trimestral	Instructores TIC y líderes comunitarios	Listas de asistencia, materiales y reportes
Seguimiento	Evaluación de adopción de prácticas seguras	Semestral	Comité de Resiliencia Digital	Informes de avance y encuestas de seguimiento
Actualización	Revisión y mejora de contenidos de formación	Anual	Coordinador del proyecto + aliados TIC	Versión actualizada del manual y plan
Evaluación	Medición del impacto en reducción de vulnerabilidades	Final del ciclo anual	Entidad ejecutora + apoyo académico	Informe de resultados con indicadores

Fuente: Propia

Roles y Entidades responsables:

Tabla 5 Roles y responsables

Entidad o actor	Rol dentro del proyecto	Responsabilidad principal
Institución Educativa Inga	Coordinador educativo local	Facilitar espacios, convocar docentes y estudiantes.
Comunidad Indígena Inga	Participante y multiplicador	Participar en la formación, aplicar prácticas seguras y replicar el conocimiento.
Gobernación del Caquetá / Secretaría de Educación	Entidad aliada	Acompañamiento técnico y validación de contenidos.
Ministerio TIC	Apoyo institucional	Proveer recursos y asesoría técnica en inclusión digital.
Sector privado (aliado tecnológico)	Socio estratégico	Donación o préstamo de infraestructura tecnológica (routers, software educativo, etc.).
Comité Comunitario de Seguridad Digital	Coordinador local de resiliencia	Monitorear la aplicación de prácticas y garantizar sostenibilidad.

Fuente: Propia

Indicadores de medición:

Tabla 6 Roles de Medicion

Indicador	Meta esperada	Medio de verificación
Porcentaje de participantes que adoptan prácticas seguras en línea	70% de los capacitados	Encuestas de evaluación post-capacitación
Reducción de incidentes cibernéticos reportados	40% respecto al diagnóstico inicial	Registro comunitario de incidentes
Niveles de participación en capacitaciones	90% de asistencia promedio	Listas de asistencia
Actualización anual de materiales y contenidos	100% cumplimiento anual	Versión revisada del manual
Creación de comités de resiliencia digital	2 comités activos	Actas de conformación y reuniones periódicas

Fuente: Propia

Articulación y sostenibilidad:

La sostenibilidad del proyecto se garantizará mediante la **articulación interinstitucional** entre la comunidad, las entidades gubernamentales y aliados del sector privado.

- **Mecanismo de articulación:**

Se establecerá una **mesa intersectorial de resiliencia digital**, integrada por representantes de la comunidad indígena, docentes, autoridades locales y expertos TIC, con reuniones trimestrales de seguimiento.

- **Acciones concretas:**
    - Monitoreo constante de los avances y retroalimentación comunitaria.
    - Renovación anual de compromisos mediante cartas de intención.
    - Inclusión del plan dentro del Proyecto Educativo Institucional (PEI).
    - Gestión de recursos ante el Ministerio TIC y programas de inclusión digital.

Eje cultural: Pertinencia y apropiación comunitaria:

- ✓ Diseñar material pedagógico (español e inga) en ciberseguridad.

- ✓ Incorporar a los líderes del cabildo con los estudiantes como mediadores digitales para transmitir prácticas seguras.
- ✓ Establecer mecanismos de articulación entre comunidad, gobierno y sector privado para la sostenibilidad de las estrategias.

Eje social: Inclusión y participación comunitaria

- ✓ Implementar programas comunitarios de ciberseguridad, liderados por los docentes de la comunidad educativa.
- ✓ Vincular la participación de toda la comunidad, garantizando que sea inclusiva y equitativa.

Eje económico: Acceso y sostenibilidad

- ✓ Gestionar con entes territoriales y ONG la dotación de dispositivos nuevos.
- ✓ Fomentar el uso de software libre y herramientas gratuitas de ciberseguridad (antivirus).

Articulación entre Actores:

- ✓ SENA, MinTIC, Secretaría de Educación Departamental
- ✓ Policía Cibernética, universidades aliadas (UNAD).
- ✓ Gobernación del Caquetá, Alcaldía Municipal de Sanjosé del Fragua,
- ✓ ONG, Empresas privadas (Claro, Movistar, Tigo), cooperación internacional.

Estrategias de Sostenibilidad:

- ✓ Vincular proyectos a convocatorias del MinTIC y fondos de cooperación internacional.
- ✓ Empoderar a los jóvenes como multiplicadores del lenguaje (Embajadores Digitales).
- ✓ Integrar los valores y cosmovisiones indígenas en las prácticas de ciberseguridad.

Lineamientos de ciberseguridad adaptados al contexto indígena

Protección de la identidad digital comunitaria:

- ✓ Evitar la difusión no autorizada de símbolos, rituales o información cultural sensible en plataformas públicas.
- ✓ Crear protocolos internos para publicaciones en redes sociales.

Gestión segura de dispositivos y cuentas:

- ✓ Uso de contraseñas robustas explicadas con analogías culturales.
- ✓ Promoción del bloqueo de dispositivos y copias de seguridad periódicas.
- ✓ Prevención frente a amenazas externas:
- ✓ Campañas de detección de estafas digitales (phishing, fraudes financieros) adaptadas a ejemplos cotidianos.

Propuestas de Acciones a corto, mediano y largo plazo

Corto plazo (6 meses):

- ✓ Talleres bilingües de ciberseguridad básicos.
- ✓ Creación de grupo comunidad educativa de apoyo digital.

Mediano plazo (1-2 años):

- ✓ Implementación de escuelas comunitarias TIC.
- ✓ Inclusión de toda la comunidad en procesos de alfabetización digital.
- ✓ Protocolos internos de seguridad digital en redes sociales.

Largo plazo (3-5 años):

- ✓ Integración de la resiliencia digital en el Plan de Vida indígena.
- ✓ Replicación del modelo en otras comunidades amazónicas.
- ✓ Establecimiento de alianzas con universidades y entes territoriales con pertinencia cultural indígena.

Recomendaciones

Los resultados evidencian que las estrategias aplicadas sí contribuyeron a reducir vulnerabilidades digitales, principalmente en el control de contraseñas, autenticación y uso responsable de dispositivos, la adopción de prácticas avanzadas como respaldo frecuente en la nube o antivirus de pago sigue limitada por factores económicos y de conectividad.

El componente cultural jugó un papel central: cuando las prácticas de ciberseguridad se transmitieron mediante metáforas culturales, lengua Inga y la mediación del Cabildo, se generó mayor apropiación.

Asegurar que los procesos de formación estén integrados en el proyecto educativo institucional (PEI) del colegio, fomentando la cooperación con universidades para proyectos de investigación aplicada en ciberseguridad intercultural.

- ✓ Utilizar instructores bilingües (español–quechua/inga) cuando sea necesario.
- ✓ Aplicar una pedagogía basada en la oralidad y ejemplos cotidianos.
- ✓ Incorporar líderes indígenas como referentes para legitimar el proceso.
- ✓ Actualizar los módulos cada seis meses según las nuevas amenazas detectadas.
- ✓ Actualización constante de los contenidos formativos según nuevas amenazas digitales.
- ✓ Seguimiento y evaluación mediante indicadores de impacto y sostenibilidad.

Reflexiones derivadas del análisis

La resiliencia digital en comunidades indígenas no depende únicamente de la tecnología, sino de la articulación entre cultura, educación y economía comunitaria.

Los lineamientos diseñados permiten respetar la identidad cultural al mismo tiempo que promueven la seguridad digital.

El plan propuesto ofrece un modelo replicable y sostenible, que puede ser implementado en otros territorios con características similares.

La participación activa de líderes, jóvenes y mujeres será determinante para garantizar la apropiación y continuidad de estas prácticas de ciberseguridad.

Conclusiones

El estudio permitió identificar las principales amenazas cibernéticas en la comunidad indígena Inga, el acceso limitado a internet, el uso de redes compartidas, la falta de infraestructura tecnológica y la ausencia de políticas de seguridad digital, incrementan la exposición de vulnerabilidades, la suplantación de identidad, el fraude en línea y la desinformación, respondiendo así a la pregunta problema planteada.

Los hallazgos obtenidos a partir del estudio preliminar permiten reflexionar sobre la importancia de diseñar estrategias de ciberseguridad que se acoplen a la cultura y región en donde se debe reconocer las particularidades sociales, lingüísticas y tecnológicas de las comunidades indígenas del municipio de San José del Fragua, en el departamento de Caquetá.

La investigación evidenció que la brecha digital en la comunidad indígena Inga no solo está relacionada con el acceso a infraestructura tecnológica, sino principalmente con limitaciones en la alfabetización digital, lo que incrementa significativamente la exposición a riesgos cibernéticos como el phishing, la suplantación de identidad y la desinformación.

La alfabetización digital es un factor determinante en la reducción de vulnerabilidades, ya que las debilidades identificadas (uso de contraseñas inseguras, desconocimiento de amenazas, baja verificación de información) están directamente asociadas a la falta de formación en el uso seguro de las TIC, El análisis de factores culturales, sociales y económicos permitió establecer que la alfabetización digital debe ser contextualizada, considerando aspectos como la lengua inga, las condiciones de acceso, para lograr una apropiación real del conocimiento tecnológico, finalmente la alfabetización digital no debe ser vista únicamente como una herramienta educativa, sino como un mecanismo de inclusión social, empoderamiento comunitario y protección frente a riesgos digitales, especialmente en las comunidades indígenas.

La investigación evidenció una brecha significativa en el acceso y uso de tecnologías de la información y la comunicación (TIC), así como en la comprensión de los riesgos digitales y la adopción de prácticas de seguridad básica, especialmente entre los sectores de jóvenes estudiantes y adultos de la comunidad indígena.

El enfoque metodológico mixto permitió no solo cuantificar el nivel de alfabetización digital y las prácticas de ciberseguridad, sino también interpretar las percepciones, temores y barreras que enfrentan estas comunidades frente al entorno digital. Los resultados cualitativos revelan que la confianza en las TIC aún está mediada por experiencias previas, baja infraestructura tecnológica y escasa formación especializada. En cuanto a la intervención mediante talleres de capacitación, se observó una mejora progresiva en el uso de TIC, así como una mayor conciencia sobre la importancia de proteger la información personal y comunitaria en entornos digitales.

Con el primer Objetivo nos permitió confirmar que la comunidad indígena Inga presenta brechas significativas en el acceso, uso y apropiación segura de las TIC, derivadas de factores culturales, económicos, de infraestructura y de falta de formación específica, evidenciando la necesidad de intervenciones sostenidas y culturalmente pertinentes para fortalecer su resiliencia digital.

Objetivo 2, el análisis de factores culturales, sociales y económicos evidenció que la brecha digital es multifactorial y se relaciona con la intermitencia de la conectividad, la dependencia de redes comunitarias inestables, el uso compartido de dispositivos, las limitaciones económicas y la ausencia de contenidos formativos adaptados al contexto indígena., aportando un marco descriptivo profundo que permite comprender la relación entre vulnerabilidad digital y condiciones territoriales.

Objetivo 3, las estrategias implementadas (talleres, campañas educativas, ejercicios prácticos, actividades lúdicas y material audiovisual adaptado culturalmente) demostraron un impacto positivo en la percepción y adopción de prácticas seguras, la comparación entre las evaluaciones iniciales y finales mostró una mejora en la comprensión del concepto de ciberseguridad, mayor identificación de riesgos como el phishing o el robo de información, incremento en la aplicación de medidas básicas como contraseñas seguras, verificación de enlaces y bases de datos.

Objetivo 4, El diseño del Plan Integral de Resiliencia Digital constituye un aporte estructural y sostenible, que consolida procedimientos, roles, herramientas pedagógicas y mecanismos de evaluación replicables en otras comunidades indígenas., y se convierte en una guía metodológica útil para instituciones educativas, autoridades locales y organizaciones que trabajen temas de inclusión digital y seguridad comunitaria.

Es importante continuar promoviendo políticas públicas y proyectos académicos que garanticen el acceso inclusivo, ético y seguro a las TIC, especialmente en zonas rurales y vulnerables, como una vía para avanzar en el cumplimiento de los Objetivos de Desarrollo Sostenible, particularmente en lo relativo a la educación de calidad, la reducción de desigualdades y el empoderamiento comunitario.

Recomendaciones

Mejorar los procesos de alfabetización digital de manera continua y contextualizada, implementando programas de formación periódicos que incluyan contenidos de ciberseguridad adaptados a la realidad cultural, social y lingüística de la comunidad indígena Inga, con alianzas institucionales, universidades, ONG y entes gubernamentales para garantizar recursos

técnologicos, humanos y económicos que permitan el desarrollo de propuestas de inclusión digital sostenibles.

Fortalecer la infraestructura tecnológica de las comunidades indígenas con la instalación de centros digitales con conectividad garantizada, energía sostenible (como paneles solares) y dispositivos modernos, con formación y capacitación básica, las buenas prácticas digitales como parte de los programas de formación para los jóvenes, líderes comunitarios y profesores indígenas en el diseño, ejecución y evaluación de los proyectos tecnológicos, asegurando su pertinencia cultural y su sostenibilidad.

Referencias Bibliográficas

Arias Chávez, D. & Cangalaya Sevillano, L. M. (2022). La tesis: mitos y errores. 1. Universidad Peruana de Ciencias Aplicadas (UPC). (pp. 35-41). https://elibronet.bibliotecavirtual.unad.edu.co/es/ereader/unad/217042

Congreso de Colombia. (2009, enero 5). *Ley 1273 de 2009 por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – la protección de la información y de los datos – y se preservan los sistemas que utilicen las tecnologías de la información y las comunicaciones*. Diario Oficial No. 47.223. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Guía de actividades Etapa 2 – Documentación de procesos de investigación

Fresno Chávez, C. (2019). Metodología de la investigación: así de fácil. El Cid Editor. (pp. 13-36). https://elibronet.bibliotecavirtual.unad.edu.co/es/ereader/unad/98278

García García, G. L. (2019). ¿Quieres hacer Tesis?. PACJ. (pp. 51- 62). https://elibronet.bibliotecavirtual.unad.edu.co/es/ereader/unad/173769

MAWIL. (2022). Lectura y escritura académica y creativa: Instrumentos que aportan al desarrollo humano. (pp. 72-82) https://doi.org/10.26820/978-9942-602-31-2

Mónica Bonilla-Parra (redacción), G. P. D. L. C. y D. V. (diseño y diagramación). (2022). *Tijitaalü Wayuu-Wayuu Digital Informe de investigación y gestión del proyecto Tijitaalü Wayuu-Wayuu Digital*. https://centroisur.co/wp-content/uploads/2024/03/wayuu_digital_libro_01_web.pdf

Organización Nacional Indígena de Colombia. (2022). *Escuela de comunicaciones Wayuu: caminando la palabra*. https://www.onic.org.co/noticias/653-escuela-de-comunicaciones-wayuu-caminando-la-palabra#:~:text=Hoy%20la%20Red%20de%20Comunicaciones,contado%20por%20los%20mismos%20Wayuu

Perez, L. Perez, R. & Seca, M. V. (2020). Metodología de la investigación científica. Editorial Maipue. (pp. 281-327). https://elibronet.bibliotecavirtual.unad.edu.co/es/ereader/unad/138497

Raúl Katz, R. V. F. C. P. P. G. A. G. Z. E. I. R. y M. D. (2024, April 2). *Impacto de la conectividad digital en hogares liderados por mujeres, individuos de pueblos indígenas o afrodescendientes en Ecuador*. https://colombiainteligente.org/es_co/tendencias/impacto-de-la-conectividad-digital-en-hogares-liderados-por-mujeres-individuos-de-pueblos-indigenas-o-afrodescendientes-en-ecuador/

Santos Valencia, R. A. Barroso Tanoira, F. G. & Chuc Canul, F. A. (2020). Cómo elaborar un proyecto de investigación. Instituto Mexicano de Contadores Públicos. (pp. 49-67). https://elibronet.bibliotecavirtual.unad.edu.co/es/ereader/unad/130921

Sarikhani, M., & Wendelborn, A. (2018). Mechanisms for provenance collection in scientific workflow systems. Computing: Archives for Scientific Computing, 100(5), 439–472. https://doiorg.bibliotecavirtual.unad.edu.co/10.1007/s00607-017-0578-1

SINCHI, I. (2022). *Comunidades indígenas de la Amazonia ya tienen sus propios indicadores de bienestar y calidad de vida*. https://sinchi.org.co/comunidades-indigenas-de-la-amazonia-ya-tienen-sus-propios-indicadores-de-bienestar-y-calidad-de-vida

Scott Berinato. (2019). Good Charts Workbook : Tips, Tools, and Exercises for Making Better Data Visualizations. Harvard Business Review Press.(130-170) https://research-ebscocom.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=f48fd728-55cf-3e17-b0d1d5619f378147

UNAD. (2023). Instructivo para el uso de Normas APA 7a Edición. https://repository.unad.edu.co/static/pdf/Norma_APA_7_Edicion.pdf

UNAD. (2024). Lineamientos para el uso de la IA en el Sello Editorial UNAD. Sello Editorial UNAD. 3 https://selloeditorial.unad.edu.co/images/2024/02/19/Lineamient osIAr.pdf

Anexos

PRIMERA ENCUESTA CIBERSEGURIDAD-.pdf

SEGUNDA ENCUESTA-.pdf