UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: **RPC-SO-02-No.053-2021**

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
Esquema de seguridad de la información para comunidades indígenas en las zonas rurales de Otavalo: alineación con las normas ISO 27002, el Código Orgánico Integral Penal (COIP) y la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador.
Línea de Investigación:
Ciencias de la Ingeniería Aplicadas a la Producción, Sociedad y Desarrollo Sustentable
Campo amplio de conocimiento:
Tecnologías de la Información y Comunicación
Autor:
Jimy Alejandro Enríquez Guerron
Tutores:
PhD. Renato Toasa PhD. Maryory Urdaneta

Quito – Ecuador

2025

APROBACIÓN DEL TUTOR

Yo, PHD Renato Mauricio Toasa Guachi con C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado: Esquema de Seguridad de la Información para Comunidades Indígenas en las Zonas Rurales de Otavalo: Alineación con las Normas ISO 27002, el Código Orgánico Integral Penal (COIP) y la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador.

Elaborado por: Jimy Alejandro Enríquez Guerrón, de C.I: 1002848123, estudiante de la Maestría: Seguridad de la Información, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2025

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

_____

Firma

APROBACIÓN DEL TUTOR

Yo, PhD. Maryory Urdaneta Herrera con C.I: 1759316126 en mi calidad de Tutor del proyecto de investigación titulado: Esquema de Seguridad de la Información para Comunidades Indígenas en las Zonas Rurales de Otavalo: Alineación con las Normas ISO 27002, el Código Orgánico Integral Penal (COIP) y la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador.

Elaborado por: Jimy Alejandro Enríquez Guerrón, de C.I: 1002848123, estudiante de la Maestría: Seguridad de la Información, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2025

MARYORY URDANETA HERRERA

Firmado digitalmente por MARYORY URDANETA HERRERA
Fecha: 2025.03.14 11:17:22 -05'00'

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Jimy Alejandro Enríquez Guerron con C.I: 1002848123, autor del proyecto de titulación denominado: Esquema de Seguridad de la Información para Comunidades Indígenas en las Zonas Rurales de Otavalo: Alineación con las Normas ISO 27002, el Código Orgánico Integral Penal (COIP) y la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador. Previo a la obtención del título de Magister en Seguridad de la Información

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2025

Firmado electrónicamente por:
JIMY ALEJANDRO ENRIQUEZ GUERRON

Firma

Tabla de contenidos

APROBACIÓN DEL TUTOR....2
APROBACIÓN DEL TUTOR....3
DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE....4
INFORMACIÓN GENERAL....8
Contextualización del tema....8
Problema de investigación....9
Objetivo general....9
Objetivos específicos....9
Vinculación con la sociedad y beneficiarios directos:....10
CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO....11
1.1. Contextualización general del estado del arte....11
1.2. Proceso investigativo metodológico....12
1.3. Análisis de resultados....15
CAPÍTULO II: PROPUESTA....23
2.1. Fundamentos teóricos aplicados....23
2.2 Descripción de la propuesta....24
2.3. Validación de la propuesta....28
2.4 Matriz de articulación de la propuesta....30
CONCLUSIONES....32
RECOMENDACIONES....33
BIBLIOGRAFÍA....34
ANEXOS....35

Índice de tablas

Tabla 4. Detalle de Propuesta de Buenas Prácticas.....25
Tabla 5. Matriz de articulación de propuesta.....30

Índice de figuras

Figura 1. Pregunta 1 15
Figura 2. Pregunta 2 15
Figura 3. Pregunta 3 16
Figura 4. Pregunta 4 17
Figura 5. Pregunta 5 18
Figura 6. Pregunta 6 18
Figura 7. Pregunta 7 19
Figura 8. Pregunta 8 20
Figura 9. Pregunta 9 21
Figura 10. Pregunta 10..... 21
Figura 11. Estructura general de la propuesta..... 26

INFORMACIÓN GENERAL

Contextualización del tema

En la actualidad proteger la información se ha vuelto fundamental para evitar pérdidas de datos, accesos no autorizados y riesgo digitales. A medida que la tecnología avanza y las conexiones en línea incrementan también aumentan las amenazas cibernéticas. Estas afectan tanto a grandes instituciones como a comunidades con menor acceso a medidas de seguridad permitiendo que se expongan a riesgos de fraude, robo de identidad y manipulación de información.(Siponen, 2000).

Las comunidades indígenas han encontrado diversas dificultades para gestionar su información para acceder a herramientas de ciberseguridad. En Ecuador, la digitalización ha permitido que se acceda a servicios financieros, educativos y administrativos en zonas rurales. Sin embargo, la falta de conocimientos en seguridad informática y la limitada infraestructura tecnológica han dejado a estas comunidades desprotegidas, expuestas a posibles filtraciones de datos personales y uso indebido de sus conocimientos.(Howard y Mazaheri, 2009).

El uso de estándares internacionales, como la ISO/IEC 27002, ha demostrado ser un enfoque eficaz para mejorar la ciberseguridad en muchos ámbitos. Esta norma, en forma de marco, ha permitido proteger los datos contra nuevos riesgos y guiar la gestión de la seguridad de la información (Calder y Watkins, 2017). A nivel nacional. La Ley Orgánica de Protección de Datos Personales (LOPDP) de Ecuador establece directrices para la recopilación, así como su almacenamiento y tratamiento, con el fin de garantizar la privacidad y los derechos. de los ciudadanos digitales(Asamblea Nacional del Ecuador, 2021)

Las investigaciones actuales han determinado que las comunidades indígenas nativas de América latina muestran una brecha significativa en términos de acceso y conocimiento sobre protección de datos. Por lo tanto, la digitalización desprovista de las medidas de seguridad adecuadas podría exponer a estos grupos a la explotación de su información cultural y geográfica a estos grupos a la explotación de su información cultural y geográfica. (Calder y Watkins, 2017). Además, los elementos importantes que restringen la aplicación de políticas de seguridad de la información en estos entornos han sido la falta de conocimiento en ciberseguridad y la escasez de herramientas técnicas (Idme et al., 2022).

Problema de investigación

En muchas comunidades indígenas rurales el acceso a conocimientos y herramientas para proteger su información sigue siendo limitado, lo que las deja expuestas a diversos riesgos en el entorno digital. A medida que la tecnología avanza y el uso de herramientas digitales se expande, también aumentan las amenazas relacionadas con la privacidad y la seguridad de los datos. En el caso de las comunidades indígenas de Otavalo, la ausencia de medidas de protección adecuadas puede comprometer su identidad cultural, su conocimiento tradicional y sus derechos en el ámbito digital.

A pesar de que normas como la Ley Orgánica de Protección de Datos Personales (LOPDP) y estándares internacionales como la ISO/IEC 27002 existen en Ecuador, su aplicación en zonas rurales e indígenas sigue siendo un reto. La imposibilidad de poner estas medidas en acción proviene de la falta de recursos financieros, la diferencia de cultura e incluso las limitaciones tecnológicas. Estas personas son más vulnerables a ataques cibernéticos y al uso indebido de la información o incluso a la explotación del conocimiento, ya que no cuentan con una protección suficiente.

El tema de esta investigación se configura en torno a la ausencia de un esquema de seguridad de la información que contemple las particularidades culturales, así como el marco normativo vigente para las comunidades indígenas rurales de Otavalo. Por lo cual es necesario un modelo que contemple la efectiva protección de la información en cuestión sin perjuicio de la autonomía y la cosmovisión de estas comunidades.

Objetivo general

Desarrollar una propuesta para la implementación de un esquema de Seguridad de la Información para comunidades indígenas de las zonas rurales de Otavalo bajo la norma ISO 27002, COIP y LOPDP

Objetivos específicos

- Analizar la norma ISO 27002 y la normativa ecuatoriana en seguridad de la información.
- Identificar los riesgos y vulnerabilidades en la gestión de información en comunidades indígenas.
- Diseñar políticas de seguridad alineadas con ISO 27002, COIP y LOPDP.
- Validar el esquema con expertos en seguridad, derecho digital y cultura indígena.

Vinculación con la sociedad y beneficiarios directos:

Los principales beneficiarios de este proyecto son las comunidades indígenas rurales de Otavalo, quienes recibirán esquemas de seguridad de la información diseñados a medida que les permitirán proteger su información personal y cultural, reducir los riesgos digitales y fortalecer su autonomía sobre la gestión de la información. Entre otros beneficiarios indirectos, se encuentran oficinas gubernamentales, ONG y centros de investigación que podrán utilizar este modelo en otras comunidades. Además, el proyecto ayudará a construir seguridad digital en Ecuador.

Esta investigación busca mejorar la seguridad digital de las comunidades indígenas rurales mediante el desarrollo de un marco de protección de datos modelado según su realidad socioeconómica basado en la norma ISO 27002, el Código Orgánico Integral Penal (COIP) y la Ley de Protección de Datos Personales (LOPDP). Estas regulaciones hacen posible implementar este modelo en áreas con infraestructura tecnológica mínima.

Esta investigación también busca promover la inclusión digital con un grado de seguridad considerando los factores de riesgo que enfrentan estas comunidades al gestionar su información. Sin embargo, el modelo es útil no solo para las personas que trabajan en estas comunidades, sino también para investigadores, especialistas en ciberseguridad y formuladores de políticas para las poblaciones más en riesgo.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

La implementación de esquemas de seguridad de la información en comunidades indígenas rurales, como las de Otavalo, requiere de un análisis detallado de trabajos previos que han abordado temas similares. Diversas investigaciones han explorado la alineación de normativas internacionales como la ISO 27002 con marcos legales nacionales, así como su aplicación en entornos específicos, incluyendo instituciones públicas y privadas en Ecuador y otros países.

Basado en la ISO 27002, De la Cruz (2016), quien en su estudio "Propuesta de políticas, basadas en mejores prácticas, para la gestión de la seguridad de la información en la Municipalidad Provincial de Paita," examina la aplicación de controles de seguridad en el ámbito gubernamental local. Este estudio se encuentra entre los más relevantes en este campo. Su sugerencia subraya la necesidad de implementar políticas adaptadas a la infraestructura y la cultura organizacional de cada institución, lo cual es un factor fundamental en la consideración de las comunidades indígenas sobre la aplicación de estas normas (De la Cruz 2016).

Por el contrario, el "Plan de Seguridad Informática basado en las normas ISO 27001 y 27002 para la Empresa Pública Municipal de Telecomunicaciones, Agua Potable, Alcantarillado y Saneamiento Ambiental de Santo Domingo" de Aguasanta y Lozada (2023) ofrece a las empresas públicas ecuatorianas una estructura útil para implementar políticas de seguridad. Si bien el enfoque está dirigido a entidades municipales, el trabajo resalta la importancia de estructurar un plan de seguridad de la información que contemple normativas internacionales, algo que puede extrapolarse al contexto de las comunidades indígenas que buscan fortalecer la protección de sus datos (Aguasanta y Lozada 2023)

En un contexto más general sobre la seguridad de la información en Ecuador, el estudio de Romo y Valarezo (2018) "Análisis e implementación de la norma ISO 27002 para la protección de los activos de información en la Universidad Politécnica Salesiana sede Guayaquil", evidencia cómo la aplicación de esta norma ha permitido mejorar la gestión de riesgos y la protección de la información en el ámbito académico. Este estudio es significativo para la investigación actual ya que la Universidad Politécnica Salesiana tiene una estrecha relación con los pueblos indígenas que permite deducir la relevancia de estas normas en tales entornos (Romo y Valarezo 2018).

Desde una perspectiva más particular sobre las comunidades indígenas, López y Ramírez (2022) en su "Aplicación del Control Interno en los Procesos Administrativos de las Comunidades Indígenas en Ecuador," subrayan la necesidad de crear mecanismos de control que permitan la adecuada gestión

de la información en estos sectores. Aunque la investigación no aborda específicamente la ISO 27002, ofrece un marco para comprender cómo las comunidades gestionan la información y qué problemas de seguridad les afectan (López y Ramírez, 2022).

Por último, Comunidades indígenas, economía de mercado y democracia en Ecuador ofrece una perspectiva sobre la transformación social y la integración, aborda el uso de nuevas tecnologías en estos sectores, lo que ayuda a comprender mejor el contexto socioeconómico y organizativo en el que se desarrollan estas comunidades. Comprender cómo los pueblos indígenas están cambiando las reglas de seguridad de la información y cuáles son las principales dificultades en su aplicación depende de este estudio (Korovkin 2018).

1.2. Proceso investigativo metodológico

En esta investigación, se optó por un enfoque cuantitativo, ya que permite comprender en profundidad las percepciones, vivencias y problemáticas relacionadas con la gestión de la seguridad de la información en comunidades indígenas rurales. Dado que estas comunidades enfrentan desafíos únicos en términos de protección de datos, acceso a la tecnología y cumplimiento normativo, este enfoque facilita la identificación de factores clave que afectan la implementación de medidas de ciberseguridad en su contexto sociocultural

El método cuantitativo resulta particularmente útil para analizar las barreras socioculturales económicas que limitan la adopción de normativas como la Ley Orgánica de Protección de Datos personales (LOPD) y la ISO/IEC 27002. Para ello, se llevan a cabo entrevistas, observación participativa y análisis documental, se busca obtener una visión integral de los riesgos y vulnerabilidades en materia de seguridad. Este enfoque permite:

- Explorar las percepciones y experiencias de los miembros de la comunidad en relación con la seguridad en el ámbito digital.
- Identificar vacíos en la protección de datos y en la aplicación de normativas.
- Proponer soluciones adaptadas a la realidad de las comunidades indígenas, respetando su y derechos digitales.

Al centrarse en un análisis profundo y contextualizado, esta metodología garantiza que los hallazgos sean relevantes y aplicables en el diseño de un esquema de seguridad de la investigación sean relevantes y aplicables en el diseño de un esquema de seguridad, que se alinea con las necesidades de estas comunidades.

Enfoque de investigación

La elección del enfoque cuantitativo en esta investigación responde a la necesidad de comprender de la seguridad de la información desde una perspectiva sociocultural y tecnológica en comunidades indígenas rurales en comunidades indígenas rurales. Este enfoque permite analizar las percepciones, prácticas y desafíos relacionados con la gestión y protección de datos en estos entornos relacionados con la gestión y protección de datos en estos entornos, y ofrece una visión global integral del problema.

Para recopilar información, se utilizaron entrevistas semiestructuradas, ya que permitieron que los participantes hablaran con libertad. directamente con líderes comunitarios, miembros de organizaciones indígenas y expertos en seguridad y obtener información. Gracias a estas conversaciones fue posible entender mejor:

- ¿Cuáles son los mayores riesgos en el manejo de la información dentro de la comunidad?
- ¿Qué saben y cómo aplican la ciberseguridad en su día a día?
- ¿Qué estrategias podrían ayudar a mejorar la seguridad de sus datos, tomando en cuenta la ISO/IEC 27002, la LOPDP y el COIP?

El enfoque cuantitativo permite comprender mejor la realidad de estas comunidades. Así, las soluciones propuestas en la investigación pueden contextualizarse y aplicarse. Respetando su identidad cultural y promoviendo la inclusión digital segura.

Diseño de la investigación

Se utilizó un enfoque cualitativo exploratorio para identificar las dificultades y requerimientos específicos de las comunidades indígenas en relación con la seguridad de información. Este tipo de estudio permite analizar el contexto sociocultural, tecnológico y normativo, en el que se desarrollan las prácticas de gestión de datos dentro de estas comunidades, lo que facilita identificar riesgos y estrategias de mitigación adaptadas a su realidad.

Muestra

La investigación se centró en realizar entrevistas a miembros de la comunidad de la zona de Otavalo, incluidos estudiantes, trabajadores locales y pequeños comerciantes con acceso a herramientas digitales herramientas digitales. Estos participantes fueron seleccionados por su uso cotidiano de la tecnología, y por su exposición a riesgos de seguridad de la información.

Se priorizó la participación de personas que pudieran aportar información sobre:

- Uso de tecnologías digitales en la vida cotidiana.
- Nivel de conocimiento en ciberseguridad y protección de datos.

- Experiencias personales relacionadas con riesgos digitales como fraudes o pérdida de información.

Este enfoque permitió obtener una visión más amplia sobre los desafíos en seguridad de la información dentro de la comunidad sin limitarse a la perspectiva de líderes o expertos.

Criterios de Selección

Los entrevistados fueron seleccionados en función de su uso cotidiano de la tecnología y su nivel de exposición a riesgos digitales dentro de la comunidad. Se priorizó la participación de:

- Estudiantes y docentes que utilizan herramientas digitales en su educación o trabajo.
- Trabajadores y pequeños comerciantes que manejan información digital en sus actividades diarias.
- Usuarios de tecnología en la comunidad que han experimentado problemas de seguridad digital o que buscan mejorar su protección en línea

Procedimiento

Esta investigación incluyó la aplicación de encuestas, las cuales se llevaron a cabo de forma virtual para garantizar la participación de los encuestados según su disponibilidad. Las encuestas, compuestas por 18 preguntas, exploraron diversos aspectos relacionados con la seguridad de la información en la comunidad de Otavalo. A través de este instrumento, se recopilaron datos de estudiantes, trabajadores locales y pequeños comerciantes, permitiendo identificar patrones y tendencias en el uso de la tecnología y los desafíos en materia de seguridad. Los resultados obtenidos se analizarán en detalle en la siguiente sección, “Análisis de resultados”.

Análisis de datos

Para el análisis de datos se utilizó la técnica de exploración temática permitiendo categorizar las respuestas entorno a aspectos importantes como:

- La gestión de acceso a la información en comunidades indígenas.
- La concienciación y capacitación en seguridad digital.
- Los mecanismos de protección de datos y aplicación de normativas como la ISO/IEC 27002 y la LOPDP.

Para garantizar que los resultados fueran confiables se comparó la información obtenida en las entrevistas con datos de documentos y observaciones dentro de la comunidad. Esto permitió tener una visión más completa y precisa de la situación.

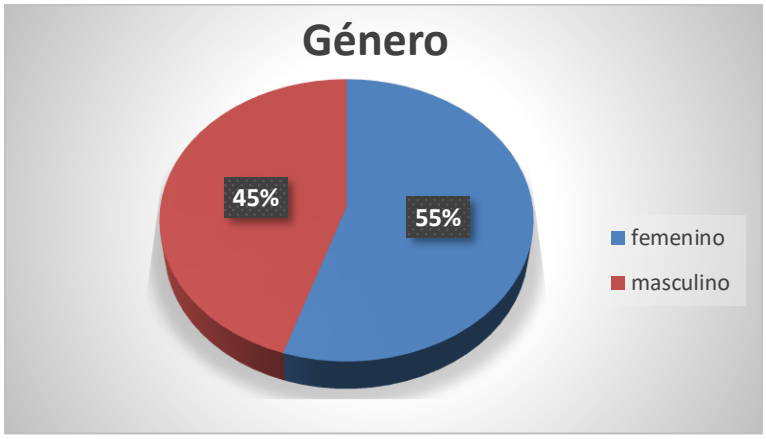
1.3. Análisis de resultados

Para lograr evaluar el nivel de conocimiento, percepción y prácticas de seguridad de la información en la comunidad indígena de Otavalo, se aplicó una encuesta a participantes. A continuación, se presentan los resultados obtenidos.

Pregunta 1: ¿Género?

Figura 1

Respuesta Pregunta 1



Nota. Esto indica una participación equilibrada entre hombres y mujeres en la encuesta

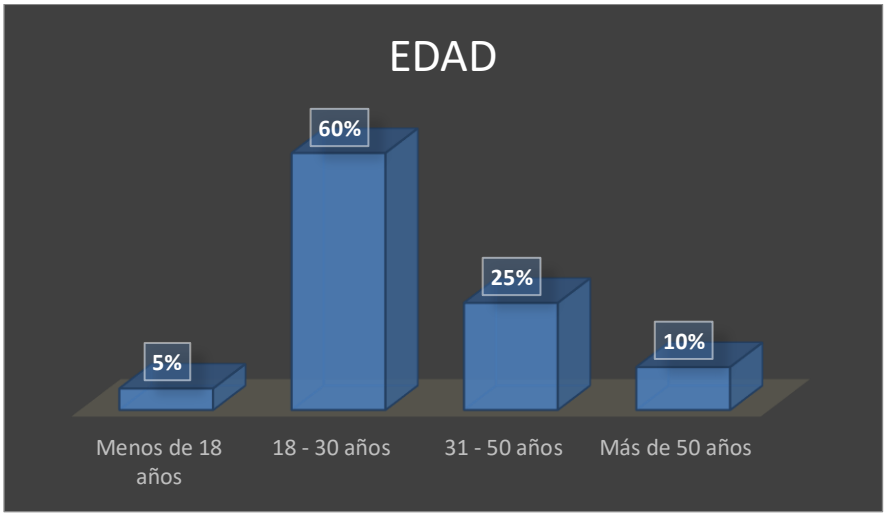
Análisis: Los resultados de la encuesta muestran una participación bastante equilibrada entre hombres y mujeres dentro de la comunidad de Otavalo. En total, el 55% de los encuestados se identificó como femenino y el 45% como masculino, lo que indica que ambos géneros estuvieron bien representados en el estudio.

Este balance es importante porque permite obtener una perspectiva más amplia y diversa sobre la seguridad de la información en la comunidad. Además, aunque hay una ligera mayoría de mujeres en la muestra, la diferencia no es tan grande como para influir significativamente en los resultados.

Pregunta 2: ¿Edad?

Figura 2

Respuesta Pregunta 2



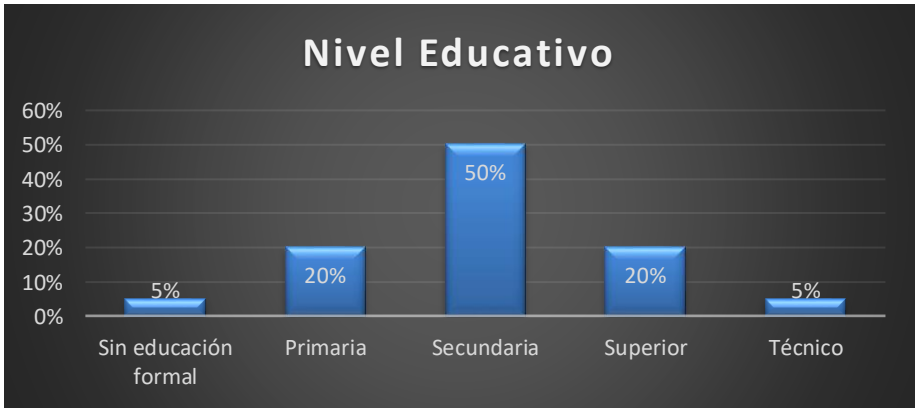
Nota. El porcentaje calculado indica que la población joven adulta es la más interesada en este tipo de estudios.

Análisis: Los resultados muestran que la mayoría de los encuestados, un 60%, tiene entre 18 y 30 años, lo que indica que la población joven adulta es la más participativa en este tipo de estudios. Un 25% de los participantes se encuentra en el rango de 31 a 50 años, mientras que solo un 10% supera los 50 años esto refleja que los jóvenes tienen un mayor interés o disponibilidad para responder encuestas sobre seguridad de la información. También podría reflejar que este grupo está más familiarizado con la tecnología y, por lo tanto, siente una mayor conexión con el tema. Por otra parte, la menor participación de personas mayores de 50 años podría deberse a distintos factores, como menor acceso a la tecnología o menor interés en estos temas. Esto resalta la importancia de incluir estrategias que ayuden a involucrar a todas las edades en la seguridad de la información, garantizando que nadie quede fuera de esta conversación.

Pregunta 3: ¿Nivel educativo?

Figura 3

Respuesta Pregunta 3



Nota. Representación gráfica de los resultados de la pregunta 3, dando favorable el 50% en nivel educativo

Análisis: Los resultados reflejan que la mayoría de los encuestados (50%) ha terminado la educación secundaria, lo que significa que es el grupo más representativo en la comunidad. Un 20% ha accedido a educación superior, mientras que otro 20% solo llegó hasta la educación primaria. Además, un pequeño grupo (5%) no tiene educación formal. Este nivel educativo influye en el acceso y el manejo de herramientas digitales, así como en el conocimiento sobre seguridad de la información. Las personas con mayor escolaridad pueden estar más familiarizadas con la tecnología y sus riesgos mientras que aquellas con menos educación podrían tener más dificultades para proteger sus datos en línea. Estos resultados muestran la importancia de ofrecer información clara y accesible para todos asegurando que cualquier persona, sin importar su nivel educativo, pueda aprender a protegerse en el mundo digital.

Pregunta 4: ¿Ocupación?

Figura 4

Respuesta Pregunta 4

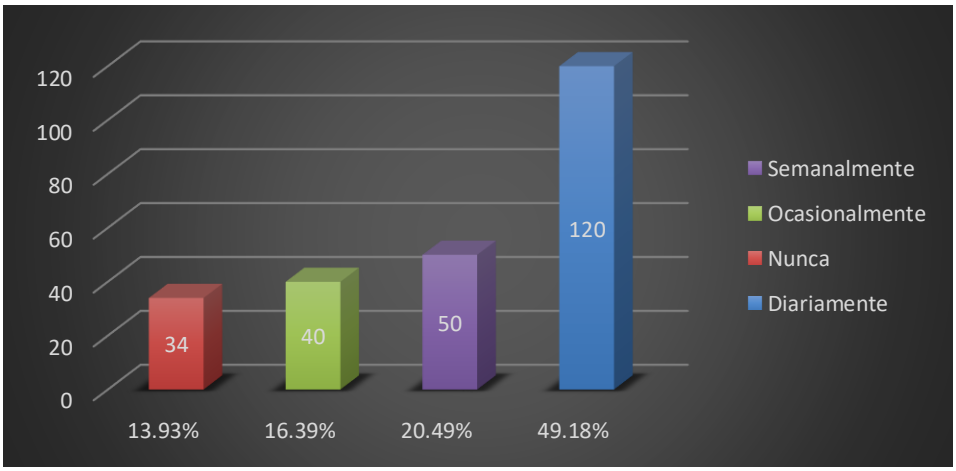
Nota. Representación gráfica de los resultados de la pregunta 4, dando favorable el 30% en la ocupación artesanía

Análisis: Los resultados reflejan que la artesanía (30%) y el comercio (25%) son las principales actividades económicas dentro de la comunidad. Además, un 20% de los encuestados trabaja en la agricultura, mientras que el 15% son estudiantes y el 10% empleados en distintos sectores. Esto nos muestra que la comunidad se caracteriza por su espíritu emprendedor y su fuerte vínculo con la producción artesanal y el comercio. La agricultura sigue siendo una fuente importante de sustento y la presencia de estudiantes indica un interés por la educación y el crecimiento personal hay que tener en cuenta estas ocupaciones es clave para adaptar iniciativas sobre seguridad de la información a las necesidades reales de la comunidad.

Pregunta 5: ¿Con qué frecuencia utiliza dispositivos electrónicos (computadora, teléfono móvil) para acceder a información personal o comunitaria?

Figura 5

Respuesta Pregunta 5



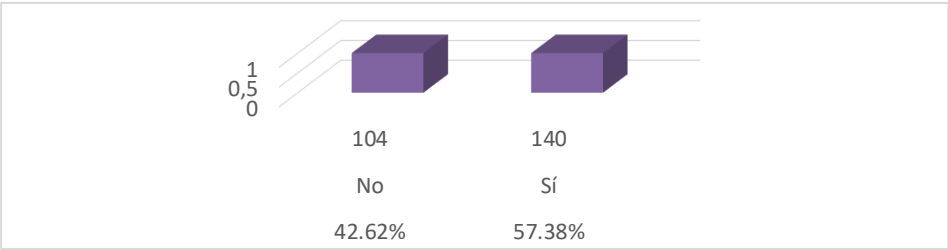
Nota. Representación gráfica de los resultados de la pregunta 5, dando favorable el 49.18% en la respuesta diariamente.

Análisis: Los resultados muestran que el uso de dispositivos electrónicos para acceder a información personal o comunitaria varía significativamente entre los encuestados. La mayoría, un 49.18% (120 personas), utiliza estos dispositivos diariamente, lo que indica una fuerte dependencia tecnológica en la comunidad. Un 20.49% (50 personas) los usa semanalmente, mientras que un 16.39% (40 personas) accede ocasionalmente. Además, un 13.93% (34 personas) nunca los utiliza. Estos datos reflejan que la tecnología juega un papel importante en la vida cotidiana de la mayoría de los encuestados, aunque todavía hay un grupo que tiene un acceso limitado o no la usa en absoluto. Esto puede deberse a factores como la edad, el nivel educativo o la disponibilidad de dispositivos y conexión a internet.

Pregunta 6: ¿Está familiarizado(a) con el concepto de "seguridad de la información"?

Figura 6

Respuesta Pregunta 6



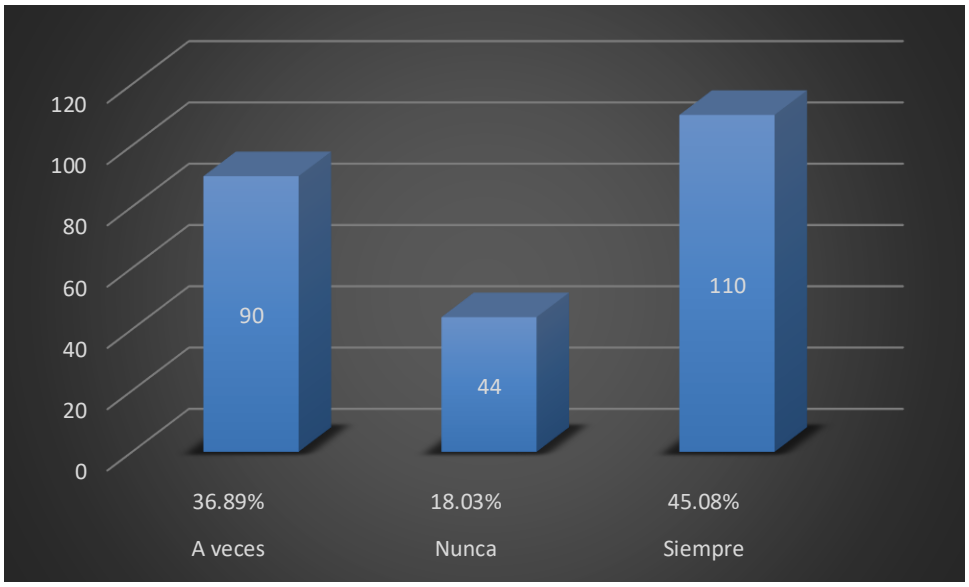
Nota. Representación gráfica de los resultados de la pregunta 6, dando favorable el 57.38% en la respuesta Si

Análisis: Los resultados indican que un 57.38% de los encuestados (140 personas) afirma estar familiarizado con el concepto de seguridad de la información, mientras que un 42.62% (104 personas) no lo está. Esto sugiere que, aunque una mayoría tiene cierta noción sobre el tema, todavía existe una parte significativa de la comunidad que desconoce este concepto, lo que puede representar un riesgo en cuanto a la protección de sus datos personales y digitales. El hecho de que más de un 40% de los encuestados no esté familiarizado con la seguridad de la información destaca la necesidad de realizar campañas de concienciación y educación en la comunidad. Con el aumento del uso de dispositivos electrónicos y la constante exposición a riesgos digitales, es fundamental que todas las personas, independientemente de su nivel de conocimiento, adquieran herramientas básicas para proteger su información.

Pregunta 7: ¿Utiliza contraseñas seguras para proteger sus dispositivos y cuentas?

Figura 7

Respuesta Pregunta 7



Nota. Representación gráfica de los resultados de la pregunta 7, dando favorable el 45.08% en la respuesta Siempre

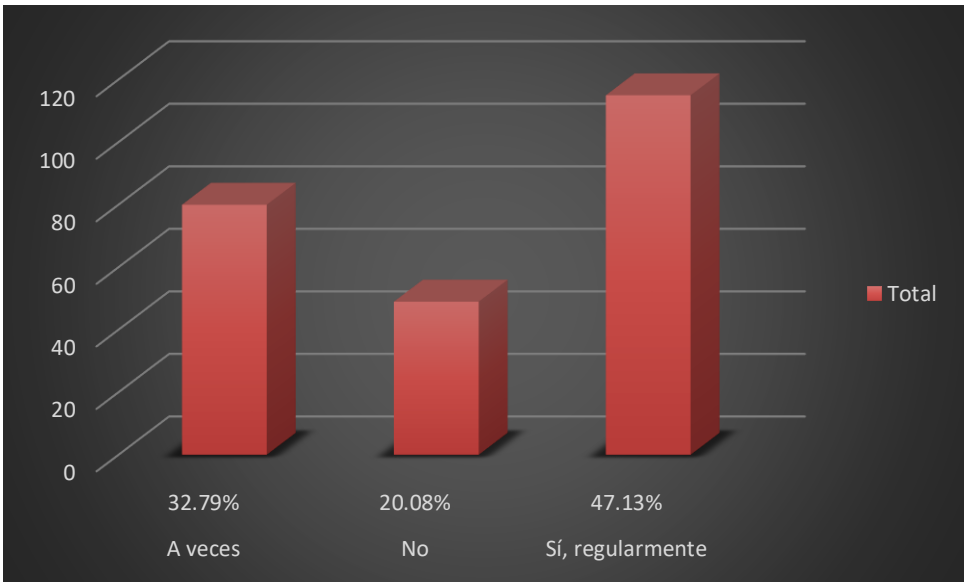
Análisis: Los resultados muestran que el 45.08% de los encuestados (110 personas) siempre usa contraseñas seguras para proteger sus dispositivos y cuentas, lo que indica que una parte importante de la comunidad es consciente de la importancia de la seguridad digital. Sin embargo, un 36.89% (90 personas) solo lo hace a veces, lo que sugiere que aún hay hábitos de seguridad que pueden mejorar. Preocupantemente, un 18.03% (44 personas) nunca utiliza contraseñas seguras lo que los deja vulnerables a riesgos como el robo de información o el acceso no autorizado a sus cuentas. Estos datos reflejan la necesidad de promover mejores prácticas en seguridad digital dentro de la comunidad. Aunque casi la mitad de los encuestados protege sus cuentas adecuadamente, hay un porcentaje

significativo que aún no lo hace de manera constante, en algunos casos no lo hace en absoluto. Establecer campañas de concienciación y educación sobre la importancia de contraseñas seguras y cómo crearlas de manera efectiva podría ayudar a reducir estas vulnerabilidades y fortalecer la protección de la información personal y comunitaria.

Pregunta 8: ¿Realiza copias de seguridad de información importante?

Figura 8

Respuesta Pregunta 8



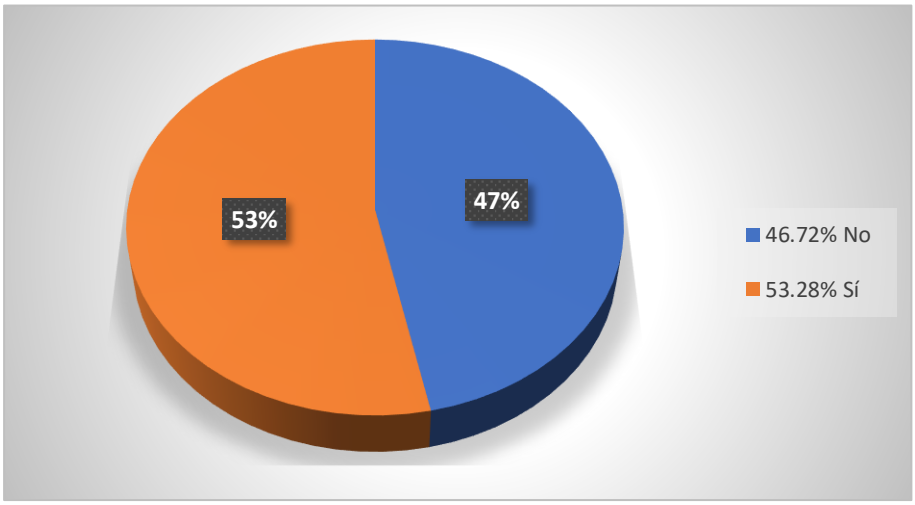
Nota. Representación gráfica de los resultados de la pregunta 8, dando favorable el 47.13% en la respuesta Sí, regularmente

Análisis: Los resultados muestran que el 47.13% de los encuestados (115 personas) realiza copias de seguridad de su información importante de manera regular, lo que indica que casi la mitad de la comunidad tiene este buen hábito de protección de datos. Sin embargo, un 32.79% (80 personas) solo lo hace de vez en cuando lo que significa que aún hay margen de mejora en la frecuencia y constancia de estas prácticas. Además, existe un 20.08% (49 personas) nunca respalda su información, lo que los deja en riesgo de perder datos valiosos en caso de algún problema técnico, robo o ciberataque. Estos resultados reflejan que, aunque muchas personas comprenden la importancia de hacer copias de seguridad, todavía hay quienes lo hacen de manera irregular o no lo hacen en absoluto. Es fundamental seguir promoviendo la importancia de este hábito, ya que guardar una copia de la información en un lugar seguro puede prevenir la pérdida de datos personales y laborales. Fomentar el uso de herramientas accesibles, como el almacenamiento en la nube o discos externos, podría ayudar a que más personas adopten esta práctica de forma regular.

Pregunta 9: ¿Sabe identificar mensajes de correo o enlaces sospechosos (phishing)?

Figura 9

Respuesta Pregunta 9



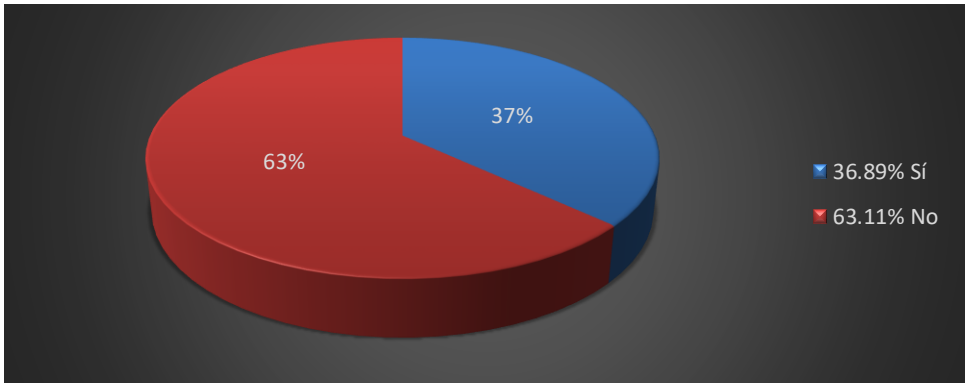
Nota. Representación gráfica de los resultados de la pregunta 9, dando favorable el 53% en la respuesta Sí

Análisis: Los resultados muestran que un 53.28% de los encuestados (130 personas) sabe identificar mensajes de correo o enlaces sospechosos, mientras que un 46.72% (114 personas) no tiene esta habilidad. Esto significa que poco más de la mitad de la comunidad está atenta a posibles intentos de fraude en línea, pero aún hay un número considerable de personas que podrían ser vulnerables a estafas digitales. El hecho de que casi la mitad de los encuestados no sepa reconocer correos o enlaces fraudulentos es preocupante ya que el phishing es una de las formas más comunes de engaño en internet. Las personas que no tienen este conocimiento pueden ser más propensas a caer en fraudes, exponiendo su información personal y financiera.

Pregunta 10: ¿Conoce la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador?

Figura 10

Respuesta Pregunta 10



Nota. Representación gráfica de los resultados de la pregunta 10, dando favorable el 63% en la respuesta No

Análisis: Los resultados muestran que solo el 36.89% de los encuestados conoce la Ley Orgánica de Protección de Datos Personales en Ecuador, mientras que el 63.11% no sabe sobre su existencia. Esto significa que la mayoría de las personas no está informada sobre sus derechos y deberes en cuanto a la protección de su información personal. El desconocimiento de esta ley puede hacer que muchas personas no tomen las precauciones necesarias para resguardar sus datos o no sepan qué hacer en caso de que su información sea utilizada sin su consentimiento. Es importante que se difunda más información sobre esta ley para que la comunidad entienda cómo proteger sus datos y qué acciones puede tomar si sus derechos son vulnerados.

CAPÍTULO II: PROPUESTA

2.1. Fundamentos teóricos aplicados

La implementación de un esquema de seguridad de la información en comunidades indígenas de las zonas rurales de Otavalo requiere un enfoque basado en normativas internacionales y nacionales que regulen la protección de datos y la seguridad digital.

Seguridad de la información en comunidades indígenas

Las comunidades indígenas enfrentan desafíos particulares en la protección de su información debido a la brecha digital, el acceso limitado a infraestructura tecnológica y la falta de capacitación en ciberseguridad (Williamson, 2024).La digitalización ha permitido el acceso a servicios gubernamentales, educativos y financieros, pero también ha incrementado los riesgos de apropiación indebida de información cultural y datos personales (Heeks y Renken, 2016). La seguridad de la información en estos entornos debe tener en cuenta factores socioculturales para garantizar la protección de datos sin menoscabar la autonomía de la comunidad. (Howard y Mazaheri, 2009).

Ciclo de Deming (PDCA)

El ciclo de Deming, también conocido como PDCA (Planificar, Hacer, Verificar, Actuar), es un método de mejora continua que se puede aplicar al sistema de gestión de la seguridad Es un medio de progreso continuo que se puede aplicar al sistema de gestión de seguridad de información. Esta etapa implica planificar acciones, implementarlas, verificar sus resultados y tomar medidas correctoras medidas correctivas para mejorar continuamente el SGSI. (Ramírez y Ortiz, 2021).

Principio de Menor Privilegio

Este principio se basa en la teoría del control de acceso, que se centra en cómo se otorgan y gestionan los permisos de acceso a recursos en un sistema. La implementación del principio de menor El privilegio se alinea con la norma ISO 27001, que hace hincapié en la importancia de controlar y limitar el acceso a la información El acceso a la información. (Torres y Herrera, 2019).

Separación de Funciones (Segregación de Tareas)

La segregación de tareas se basa en la teoría del control interno, que busca garantizar que las funciones críticas se ejecuten de manera independiente para evitar la concentración de poder funciones críticas se ejecuten de manera independiente para evitar la concentración de poder, así como la posibilidad de manipulación. Este principio se corresponde con la norma ISO 27002, que aborda el control de acceso y gestión de privilegios. (Castro y Méndez, 2020).

Modelo de Amenazas y Vulnerabilidades

Este modelo está orientado en la teoría de seguridad e identificación de riesgos de la información. Se puede utilizar en grupo con la modalidad de evaluación de riesgos de la norma ISO 27005 para identificar las amenazas y vulnerabilidades más probables que enfrenta la organización, lo que permite la implementación de controles adecuados (Velasco y Gutiérrez, 2019).

Gestión de Incidentes de Seguridad

La gestión de percances de seguridad es un mecanismo que engloba la respuesta, identificación, recuperación y contención de incidentes asociados con la seguridad de la información en el organismo. Esta perspectiva se basa en la teoría de gestión de incidentes y respuesta a emergencias. Se puede aplicar junto con las pautas de la norma ISO 27035 para garantizar que la organización esté preparada para rebatir eficazmente a los incidentes de seguridad y minimizar el impacto en caso de que ocurran (Pérez y López, 2022).

2.2 Descripción de la propuesta

Esta propuesta tiene como objetivo poder ayudar a las comunidades indígenas de Otavalo a proteger su información evitando riesgos como accesos no autorizados, uso indebido de su conocimiento de medios de comunicación y problemas de seguridad digital. La idea es implementar buenas prácticas basadas en normas y leyes que ya existen como la ISO 27002, el COIP y la Ley de Protección de Datos Personales pero adaptadas a su realidad.

Para lograr este objetivo se trabajará en cinco áreas clave que son las siguientes:

1. Identificación de riesgos: Se analiza los principales peligros que enfrenta la comunidad en cuanto a su información tomando en cuenta su cultura y su forma de manejar la tecnología y las leyes que pueden ayudarles.
2. Creación de normas claras: Se establece reglas y procedimientos que sirvan para proteger sus datos personales y comunitarios asegurando que las leyes sean aplicables en su entorno.
3. Capacitación a la comunidad: Se organiza talleres y charlas para que líderes y miembros de la comunidad aprendan sobre seguridad digital y cómo proteger su información.
4. Control en el acceso a la información: Se define mecanismos para que solo las personas que cuenten con autorización las mismas que puedan acceder a ciertos datos importantes de la comunidad.
5. Revisar y mejorar constantemente: Se realiza evaluaciones constantes para asegurarse de que todo funcione correctamente permitiendo realizar los cambios necesarios en caso de nuevas amenazas digitales.

El objetivo final es que la comunidad indígena tenga más control sobre sus datos e información permitiendo manejarla de forma segura evitando problemas que pongan en riesgo su cultura y conocimientos.

Estructura general

La propuesta está diseñada con un enfoque integral de seguridad de la información alineado con la ISO/IEC 27002 y normativas nacionales como la LOPDP y el COIP. A continuación, se presentan las principales fases del esquema:

Tabla 1

Detalle de Propuesta de Buenas Prácticas

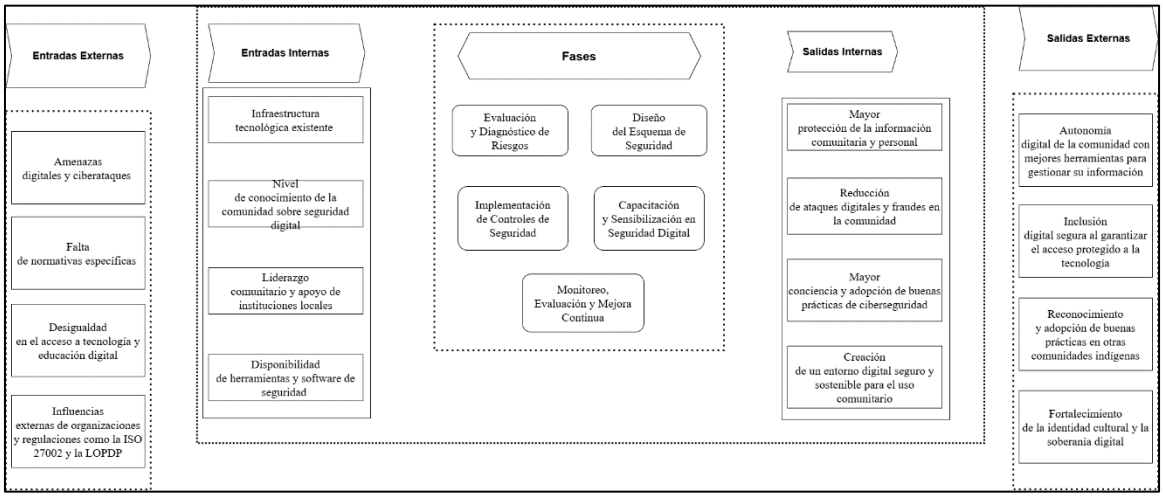
Fase	Descripción	Acciones clave
Evaluación inicial y diagnóstico	Identificación de riesgos y debilidades en el acceso a la información.	Análisis de cumplimiento con ISO/IEC 27002 y regulaciones locales.
Definición de normativas y controles	Establecimiento de reglas claras para la protección de datos en la comunidad indígena.	Creación y elaboración de políticas de control de acceso y protección de datos.
Capacitación constante sobre la seguridad digital	Concientización y educación en la comunidad sobre protección de información.	Talleres, guías y capacitaciones adaptadas al contexto cultural.
Implementación de herramientas tecnológicas	Aplicación de soluciones de seguridad para gestionar accesos y monitoreo.	Uso de autenticación multifactor, auditorías y detección de anomalías.
Evaluación y mejora continua	Revisiones periódicas para optimizar la protección de la información.	Auditorías de seguridad y actualización de estrategias.

Nota. La figura muestra la estructura general de la propuesta de buenas practicas

A continuación, la figura 11 muestra la estructura general de la propuesta de buenas practicas

Figura 11

Estructura general de la propuesta



Nota. La figura muestra la estructura general de la propuesta de buenas prácticas.

Componentes Claves de la Propuesta

1. Conocer la situación actual

Antes de hacer cualquier cambio, es importante entender cómo manejan la seguridad de su información las comunidades indígenas. Para eso:

- Se evaluará qué tan protegida está su información en este momento.
- Se identificarán los puntos débiles y los problemas en el acceso a los datos.
- Se revisará qué tan alineados están con las normas y leyes actuales.

2. Crear estrategias de protección

Una vez detectadas las debilidades, el siguiente paso es desarrollar soluciones prácticas que realmente sirvan en su contexto. Esto incluye:

- Definir reglas claras para proteger la información.
- Implementar controles para que solo las personas autorizadas puedan acceder a ciertos datos.
- Crear normas internas que permitan manejar la información de forma segura sin afectar su uso en la comunidad.

3. Enseñar y concienciar a la comunidad

No basta con poner reglas, también hay que asegurarse de que todos las comprendan y sepan aplicarlas en su día a día. Para esto:

- Se realizarán talleres prácticos donde se explicará cómo cuidar la información digital.
- Se diseñarán programas de formación pensados para su cultura y su forma de aprender.
- Se crearán materiales educativos en formatos fáciles de entender y en su propia lengua.

4. Evaluar y mejorar constantemente

La seguridad no es algo que se hace una vez y ya, hay que revisarla constantemente para asegurarse de que funcione bien. Por eso:

- Se evaluará periódicamente cómo está funcionando el esquema.
- Se harán simulaciones de ataques digitales para ver si hay fallos y corregirlos.
- Se harán ajustes según la retroalimentación de la comunidad y de expertos en el tema.

Con estas acciones, se busca que las comunidades indígenas puedan proteger su información de forma efectiva, sin perder el control sobre sus datos y su conocimiento ancestral.

Estrategias y Técnicas Aplicadas

1. ***Análisis de Brechas y Diagnóstico:***

- Identificación de debilidades en la seguridad de la información dentro de las comunidades.
- Evaluación del nivel de madurez en la gestión de datos.

2. ***Investigación de Buenas Prácticas:***

- Análisis de marcos de referencia internacionales como el NIST y la ISO 27002.

- Adaptación de normativas a contextos socioculturales específicos.

3. Implementación Iterativa con PDCA:

- Aplicación del ciclo de mejora continua (Planificar, Hacer, Verificar, Actuar).
- Revisión constante de la efectividad de los controles de seguridad.

4. Pruebas y Simulaciones de Seguridad:

- Realización de auditorías y pruebas de penetración para validar la efectividad del esquema.
- Uso de escenarios reales para evaluar la preparación de la comunidad frente a incidentes.

5. Capacitación y Sensibilización Comunitaria:

- Programas de formación para fortalecer el conocimiento en seguridad digital.
- Estrategias de difusión en redes comunitarias para garantizar la adopción de buenas prácticas.

Este enfoque busca garantizar la protección de la información de las comunidades indígenas promoviendo una cultura de seguridad digital adaptada a sus necesidades y contexto.

2.3. Validación de la propuesta

Para asegurarse de que esta propuesta realmente funcione y sea útil para las comunidades indígenas de Otavalo se trabajó con Especialistas en seguridad de la información, derecho digital y cultura indígena para esto se tomaron en cuenta sus opiniones y sugerencias para hacer los ajustes necesarios. (Ver Anexo 1).

Se hicieron evaluaciones tanto dentro como fuera de la comunidad para comprobar que las medidas de seguridad sean prácticas y aplicables a su realidad.

Con este proceso, se confirmó que la propuesta sigue lo establecido en la norma ISO 27002, el Código Orgánico Integral Penal (COIP) y la Ley de Protección de Datos Personales (LOPDP). Más allá de cumplir con las leyes lo más importante fue asegurarse de que realmente sirva a la comunidad y se adapte a su forma de manejar la información y la tecnología.

1. Revisión del esquema de seguridad

Lo primero que se realizó fue un análisis detallado del esquema propuesto para ver si realmente este cubría las necesidades de las mejores prácticas de seguridad de la información y lo más importante si era factible y útil en la comunidad.

2. Pruebas en la comunidad y simulaciones de riesgos

Para asegurase de que el esquema funcionara en la práctica se realizaron pruebas piloto dentro de la comunidad, se hicieron simulaciones de posibles ataques digitales y se revisaron vulnerabilidades. Durante este proceso, se identificaron dificultades técnicas y sociales lo que ayudó a hacer ajustes antes de su aplicación definitiva.

3. Evaluación de su adaptación a la comunidad

No basta con que el esquema sea seguro, también tiene que integrarse bien en la vida diaria de la comunidad. Se evaluó si era fácil de usar si respetaba sus costumbres y si se adaptaba a la tecnología que tienen disponible. El objetivo era que su implementación fuera realmente útil y funcional en su entorno.

4. Ajustes y mejoras finales

Después de revisar todo lo aprendido en las fases anteriores, se hicieron cambios para mejorar la propuesta, se adaptaron los materiales de capacitación para que fueran más accesibles se simplificaron algunos procesos y se reforzó el monitoreo de accesos.

Gracias a este proceso, se logró que el esquema no solo protegiera la información de la comunidad, sino que fuera práctico fácil de usar y bien recibido. De esta manera se aseguró su aplicación a largo plazo sin afectar la dinámica de la comunidad.

2.4 Matriz de articulación de la propuesta

En la siguiente matriz se resume la conexión del producto desarrollado con los fundamentos metodológicos, teóricos, tecnológicos y estratégicos-técnicos utilizados. A continuación, la Tabla 2 detalla la matriz de articulación de la propuesta:

Tabla 2

Matriz de articulación de propuesta

Ejes o Partes Principales	Sustento Teórico	Sustento Metodológico	Estrategias / Técnicas	Descripción de Resultados	Instrumentos Aplicados
Análisis de riesgos y diagnóstico inicial	ISO 27001 – A9 Control de Acceso LOPDP (Ley Orgánica de Protección de Datos Personales)	Evaluación cuantitativo de vulnerabilidades y amenazas	Análisis de brechas Revisión documental Entrevistas con especialistas	Identificación de riesgos en la gestión de accesos y control de datos	Documentos normativos Entrevistas Cuestionarios
Definición de políticas y controles de acceso	Principio de Menor Privilegio Segregación de funciones ISO 27002	Revisión documental y análisis comparativo	Diseño de políticas de control de acceso Aplicación de normativa de seguridad	Establecimiento de procedimientos para la gestión segura de accesos y roles	Documentación de políticas Normativas internas
Capacitación y concienciación en seguridad	Educación en ciberseguridad	Análisis de percepciones del personal Encuestas	Talleres de capacitación Simulaciones de ataques de ingeniería social	Fortalecimiento de la cultura organizacional en	Encuestas Simulaciones

	Factores humanos en seguridad de la información			seguridad de la información	
Implementación de herramientas tecnológicas	ISO 27001 Gestión de Identidades y Accesos (IAM)	Análisis técnico de soluciones de seguridad	Evaluaciones periódicas Aplicación de autenticación multifactor (MFA) Monitoreo y auditoría de accesos	Mayor control y trazabilidad en la gestión de accesos	Talleres Herramientas de monitoreo
Evaluación, validación y mejora continua	Modelo de gestión de seguridad de la información	Validación de controles de acceso mediante pruebas prácticas	Simulaciones de ataques y pruebas de penetración Evaluación de aplicabilidad operativa	Optimización del esquema de seguridad según vulnerabilidades identificadas	Auditorías de seguridad Reportes de pruebas Evaluación de expertos

Nota. La tabla muestra las partes principales de la matriz de articulación de la propuesta

CONCLUSIONES

Este proyecto permitió comprender de manera más cercana los problemas que hoy en dia enfrentan las comunidades indígenas de Otavalo para proteger su información. A través de entrevistas y análisis se evidenció que muchas personas tienen poco acceso a herramientas de seguridad digital y que en su mayoría desconocen leyes como la Ley Orgánica de Protección de Datos Personales lo que las deja en una situación de vulnerabilidad.

Se probó que la norma ISO 27002 puede ser de gran ayuda para mejorar la seguridad de la información, pero su aplicación en comunidades rurales e indígenas debe adaptarse a su contexto para que sea realmente útil. No se trata solo de establecer medidas técnicas sino también de asegurarse de que la comunidad entienda por qué es importante proteger su información y cómo puede hacerlo de manera sencilla y efectiva.

Por esta razón se diseñó un esquema de seguridad pensado para sus necesidades, combinando regulaciones internacionales con educación y prácticas acordes a su cultura. Se establecieron reglas claras para el control de acceso a la información se propusieron capacitaciones y se implementaron mecanismos de monitoreo que ayuden a resguardar sus datos personales y comunitarios.

Para garantizar que este modelo sea realmente funcional y bueno para la comunidad se realizaron pruebas en la comunidad y se contó con la opinión de expertos. Los resultados demostraron que combinar medidas técnicas con educación ayuda a que las personas adopten mejores hábitos de seguridad digital. Asimismo, se resaltó la importancia de que este esfuerzo sea sostenible en el tiempo, para que las comunidades puedan proteger su información sin depender de terceros.

RECOMENDACIONES

Es evidente al examinar cómo los pueblos indígenas de Otavalo manejan sus datos que se deben tomar medidas para protegerlos mejor y prevenir los peligros del mundo digital. Establecer directrices claras sobre quién puede acceder a qué tipo de información disponible en la sociedad es lo primero. Particularmente en los casos que involucran información privada o sensible, no todo el material debería estar fácilmente disponible para todos.

Es esencial implementar un sistema en el que todos tengan acceso únicamente a la información que les corresponda necesario, para evitar así la filtración o explotación de datos privados. Además, se destacó el hecho de que muchas personas aún carecen de conocimiento sobre los riesgos involucrados en el uso de las nuevas tecnologías plataformas de Internet y dispositivos modernos. Por lo tanto, es importante planificar cursos de capacitación sencillos y útiles donde las personas de la comunidad puedan aprender a proteger sus datos sencillos y útiles en los que las personas de la comunidad puedan aprender a proteger sus datos. Estos cursos deben incluir, por ejemplo, cómo elegir contraseñas seguras y detectar correos electrónicos fraudulentos y prevenir el fraude en línea.

Además de evitar problemas, es importante saber qué hacer en caso de que se produzca un evento inesperado de seguridad. Se aconseja crear una estrategia que permita a la sociedad hacer frente a cualquier peligro relacionados con la tecnología digital, como el robo de datos o el acceso ilegal a sus recursos. Para ello, se pueden realizar simulaciones y también se puede evaluar el éxito de esta estrategia y proporcionar correcciones cuando sea necesario De este modo, se garantizará su viabilidad, se debe garantizar a las personas el acceso a herramientas digitales seguras y de fácil navegación seguras y de fácil navegación.

El fomento de los líderes locales puede ser muy importante para ayudar a las personas a adoptar estas precauciones de seguridad. La seguridad digital no es algo que se instala una vez y ya está, sino que es algo que hay que ir manteniendo, Por el contrario, es vital construir entornos donde las personas puedan hacer preguntas y recibir orientación sobre el uso seguro de la tecnología y obtener orientación sobre el uso seguro de la tecnología. Este es un procedimiento que tiene que estar en constante cambio para enfrentar nuevos peligros y problemas. Las evaluaciones regulares nos ayudarán a identificar qué políticas son efectivas y qué áreas necesitan cambios, asegurando así que la comunidad se mantenga protegida a largo plazo.

BIBLIOGRAFÍA

Aguasanta, Pablo, y Edwin Lozada. 2023. *PLAN DE SEGURIDAD INFORMÁTICO BASADO EN LAS NORMAS ISO 27001 Y 27002 PARA EL COMERCIAL "EL FERRETERO" DE LA CIUDAD DE TENA*.

Asamblea Nacional del Ecuador. 2021. *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*.

Calder, Alan, y Steve Watkins. 2017. *IT Governance i*.

Heeks, Richard, y Jaco Renken. 2016. "Data justice for development: What would it mean?" *Information Development* 34. doi: 10.1177/0266666916678282.

Howard, y Mazaheri. 2009. "Telecommunications Reform, Internet Use and Mobile Phone Adoption in the Developing World". *World Development* 37:1159–69. doi: 10.1016/j.worlddev.2008.12.005.

Howard, Philip, y Nimah Mazaheri. 2009. "Telecommunications Reform, Internet Use and Mobile Phone Adoption in the Developing World". *World Development* 37:1159–69. doi: 10.1016/j.worlddev.2008.12.005.

Idme, Jorge, Jhon García, Shalóm Morales, y Laberiano Andrade-Arenas. 2022. "The Implementation of Information Security for the Inventory System in a Municipality of Lima-Perú". *International Journal on Advanced Science, Engineering and Information Technology* 12:101. doi: 10.18517/ijaseit.12.1.13914.

Korovkin, Tanya. 2018. "Comunidades indígenas, economía de mercado y democracia en los Andes ecuatorianos".

De la Cruz, Vargas. 2016. *PROPUESTA DE POLÍTICAS, BASADAS EN BUENAS PRÁCTICAS, PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DE PAITA*.

Romo, Daniel, y Joffre Valarezo. 2018. *Análisis e implementación de la norma ISO 27002 para la protección de los activos de información en la Universidad Politécnica Salesiana sede Guayaquil.*

Siponen, Mikko. 2000. "Conceptual foundation for organizational information security awareness". *Information Management and Computer Security* 8:31–41.

Williamson, Ben. 2024. "Geographies of Digital Exclusion: Data and Inequality". *The AAG Review of Books* 13:1–3. doi: 10.1080/2325548X.2024.2389793.

ANEXOS

Anexo 1

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"ESQUEMA DE SEGURIDAD DE LA INFORMACIÓN PARA COMUNIDADES INDÍGENAS EN LAS ZONAS RURALES DE OTAVALO: ALINEACIÓN CON LAS NORMAS ISO 27002, EL CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP) Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (LOPDP) EN ECUADOR"**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

AUTOR: JIMY ALEJANDRO ENRIQUEZ GHUERRON

Datos informativos

Validado por: PAÚL BALDEÓN
Título obtenido: DOCTORADO EN PROYECTO - TIC
C.I.: 1002807814
E-mail: pbaldeon@uisrael.edu.ec
Institución de Trabajo: Universidad Tecnológica Israel
Cargo: Director de Sistematización
Años de experiencia en el área: 15 años

Universidad Israel

ESPOG | Escuela de Posgrados

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "ESQUEMA DE SEGURIDAD DE LA INFORMACIÓN PARA COMUNIDADES INDÍGENAS EN LAS ZONAS RURALES DE OTAVALO: ALINEACIÓN CON LAS NORMAS ISO 27002, EL CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP) Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (LOPDP) EN ECUADOR"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	X				
Aplicabilidad		X			
Factibilidad		X			
Novedad	X				
Fundamentación pedagógica		X			
Fundamentación tecnológica	X				
Indicaciones para su uso	X				
TOTAL	**20**	**12**			

Observaciones: Se debería fortalecer a la ISO 27002 con por lo menos alguna característica del marco referencia internacional de la NIST.

Recomendaciones: Generar estrategias de concienciación para los beneficiarios.

Lugar, fecha de validación: Quito, 25 de febrero de 2025

PAUL FRANCISCO BALDEON EGAS

Firmado digitalmente por PAUL FRANCISCO BALDEON EGAS
Fecha: 2025.02.25 12:53:55 -05'00'

Firma del especialista
Paúl Baldeón

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"ESQUEMA DE SEGURIDAD DE LA INFORMACIÓN PARA COMUNIDADES INDÍGENAS EN LAS ZONAS RURALES DE OTAVALO: ALINEACIÓN CON LAS NORMAS ISO 27002, EL CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP) Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (LOPDP) EN ECUADOR"**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Marco Cazar
Título obtenido: Msc. Ciencia de Datos
C.I.: 1718449166
E-mail: mcazar@telconet.ec
Institución de Trabajo: Telconet S.A
Cargo: Jefe nacional de Procesos
Años de experiencia en el área: 16 años

Universidad Israel
ESPOG | Escuela de Posgrados

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "ESQUEMA DE SEGURIDAD DE LA INFORMACIÓN PARA COMUNIDADES INDÍGENAS EN LAS ZONAS RURALES DE OTAVALO: ALINEACIÓN CON LAS NORMAS ISO 27002, EL CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP) Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (LOPDP) EN ECUADOR"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	X				
Aplicabilidad		X			
Factibilidad		X			
Novedad	X				
Fundamentación pedagógica	X				
Fundamentación tecnológica	X				
Indicaciones para su uso	X				
TOTAL	33				

Observaciones: El tema es muy importante tomando en cuenta que esto era poco probable que por iniciativa propia las comunidades adopten quedado susceptibles a escenarios de robo o mal uso de su información.

Recomendaciones: Al tratar con comunidades rurales se recomendaría que poder llegar de forma adecuada a cualquier integrante de la misma, se podría recurrir a expertos pedagogos que ayuden a mejorar la posibilidad de éxito del proyecto.

Lugar, fecha de validación: Quito 21 de febrero 2025

Firma del especialista
Marco Cazar

Universidad Israel

ESPOG | Escuela de Posgrados

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"ESQUEMA DE SEGURIDAD DE LA INFORMACIÓN PARA COMUNIDADES INDÍGENAS EN LAS ZONAS RURALES DE OTAVALO: ALINEACIÓN CON LAS NORMAS ISO 27002, EL CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP) Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (LOPDP) EN ECUADOR"**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Ismael Andrade Winingther
Título obtenido: Abogado
C.I.: 0801798216
E-mail: miandrade@telconet.ec
Institución de Trabajo: Telconet S.A
Cargo: Jefe Técnico Sucursal Esmeraldas
Años de experiencia en el área: 15 años

Universidad Israel

ESPOG | Escuela de Posgrados

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "ESQUEMA DE SEGURIDAD DE LA INFORMACIÓN PARA COMUNIDADES INDÍGENAS EN LAS ZONAS RURALES DE OTAVALO: ALINEACIÓN CON LAS NORMAS ISO 27002, EL CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP) Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (LOPDP) EN ECUADOR"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	X				
Aplicabilidad	X				
Factibilidad		X			
Novedad	X				
Fundamentación pedagógica	X				
Fundamentación tecnológica	X				
Indicaciones para su uso	X				
TOTAL	34				

Observaciones generales

1. **Alta pertinencia y necesidad social:**
   El tema abordado representa una necesidad concreta en comunidades rurales e indígenas, tradicionalmente desatendidas en temas de ciberseguridad y protección de datos.
2. **Enfoque normativo sólido:**
   La alineación con la norma ISO 27002, el COIP y la LOPDP refuerza la base jurídica y técnica de la propuesta. Esto la vuelve sólida en términos de cumplimiento normativo y adaptable a contextos institucionales.
3. **Factibilidad y aplicabilidad validadas desde la experiencia técnica:**
   Se destaca la factibilidad y aplicabilidad del proyecto, lo cual es clave, considerando la experiencia adquirida en implementación de soluciones tecnológicas en distintas

realidades del Ecuador. Esto indica que la propuesta tiene condiciones reales de ejecución si se abordan adecuadamente los desafíos locales.

Recomendaciones específicas

1. **Incluir acompañamiento pedagógico intercultural:**
   Para facilitar la adopción del esquema de seguridad en las comunidades indígenas, se recomienda integrar a pedagogos interculturales o facilitadores comunitarios que puedan traducir los conceptos técnicos a un lenguaje accesible y culturalmente pertinente.
2. **Elaborar materiales de apoyo didáctico:**
   Desarrollar guías visuales, infografías, talleres prácticos o videos en idioma originario (por ejemplo, kichwa) puede mejorar significativamente la comprensión y apropiación del proyecto.
3. **Estrategia de implementación colaborativa:**
   Diseñar un plan de implementación participativa, que incluya a líderes comunitarios, jóvenes locales y actores institucionales, para asegurar sostenibilidad del esquema.

Resumen Final

La propuesta evaluada muestra un enfoque técnico-normativo sólido, viable, innovador y pertinente. La observación más relevante gira en torno al acompañamiento pedagógico adecuado para garantizar el éxito de su implementación en zonas rurales e indígenas.

Lugar, fecha de validación: Esmeraldas 11 de marzo 2025

Firma del especialista
Ismael Andrade W.

Universidad Israel

ESPOG | Escuela de Posgrados

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"ESQUEMA DE SEGURIDAD DE LA INFORMACIÓN PARA COMUNIDADES INDÍGENAS EN LAS ZONAS RURALES DE OTAVALO: ALINEACIÓN CON LAS NORMAS ISO 27002, EL CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP) Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (LOPDP) EN ECUADOR"**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: MARIA BLANCA RUIZ GUAJAN
Título obtenido: INGENIERA EN ADMINISTRACION
C.I.: 1003172408
E-mail: blanki_h@hotmail.com
Institución de Trabajo: PEGUCHE -PARROQUIA MIGUEL EGAS CABEZAS
Cargo: VOCAL DIRECTIVA BARRIO IMBAQUI
Años de experiencia en el área: 15 AÑOS

Universidad Israel

ESPOG | Escuela de Posgrados

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "ESQUEMA DE SEGURIDAD DE LA INFORMACIÓN PARA COMUNIDADES INDÍGENAS EN LAS ZONAS RURALES DE OTAVALO: ALINEACIÓN CON LAS NORMAS ISO 27002, EL CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP) Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (LOPDP) EN ECUADOR"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	X				
Aplicabilidad	X				
Factibilidad		X			
Novedad		X			
Fundamentación pedagógica	X				
Fundamentación tecnológica	X				
Indicaciones para su uso	X				
TOTAL	25	8			

Observaciones:

Muchas organizaciones en Ecuador aún no han implementado programas de concienciación y formación adecuados para sus empleados sobre los riesgos de seguridad de la información en el trabajo remoto. Esto incluye la falta de conocimiento sobre phishing, malware, uso seguro de contraseñas y la protección de datos sensibles.

Recomendaciones:

Las organizaciones deben desarrollar e implementar programas de concienciación y formación periódicos sobre seguridad de la información para todos los empleados. Estos programas deben cubrir temas como la identificación de amenazas, el uso seguro de dispositivos y aplicaciones, y la protección de datos confidenciales.

Las empresas deben invertir en la infraestructura de seguridad necesaria para proteger los datos en entornos de trabajo remoto. Esto incluye la implementación de firewalls, software

antivirus actualizado, VPNs y sistemas de cifrado. También es crucial establecer políticas claras sobre el uso de dispositivos personales y la seguridad de las redes domésticas de los empleados.

Lugar, fecha de validación: Otavalo 11 de marzo del 2025

Firma del especialista
MARIA BLANCA RUIZ GUAJAN

Universidad Israel

ESPOG | Escuela de Posgrados

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital **"ESQUEMA DE SEGURIDAD DE LA INFORMACIÓN PARA COMUNIDADES INDÍGENAS EN LAS ZONAS RURALES DE OTAVALO: ALINEACIÓN CON LAS NORMAS ISO 27002, EL CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP) Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (LOPDP) EN ECUADOR"**. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: WALTER MAURICIO AYALA ALMEIDA
Título obtenido: Abogado de los Tribunales de la República del Ecuador, Especialista en Derecho Penal, Mgs. En Derecho Procesal Penal, Mgs. En Derecho Procesal Constitucional
C.I.: 1002691242
E-mail: abg.walterayala@hotmail.com
Institución de Trabajo: Fiscalía General del Estado
Cargo: Analista Provincial de Gestión Procesal 2
Años de experiencia en el área: 17

Universidad Israel

ESPOG | Escuela de Posgrados

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "ESQUEMA DE SEGURIDAD DE LA INFORMACIÓN PARA COMUNIDADES INDÍGENAS EN LAS ZONAS RURALES DE OTAVALO: ALINEACIÓN CON LAS NORMAS ISO 27002, EL CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP) Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (LOPDP) EN ECUADOR"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	X				
Aplicabilidad	X				
Factibilidad	X				
Novedad	X				
Fundamentación pedagógica	X				
Fundamentación tecnológica	X				
Indicaciones para su uso	X				
TOTAL	35				

Observaciones: El tema es muy importante tomando en cuenta que esto era poco probable que por iniciativa propia las comunidades adopten quedado susceptibles a escenarios de robo o mal uso de su información.

Recomendaciones: Al tratar con comunidades rurales se recomendaría que poder llegar de forma adecuada a cualquier integrante de la misma, se podría recurrir a expertos pedagogos que ayuden a mejorar la posibilidad de éxito del proyecto.

Lugar, fecha de validación: Quito 07 de marzo 2025

Firma del especialista

Anexo 2

Los resultados de esta encuesta serán analizados con absoluta reserva y su tratamiento será de manera estadística y exclusivamente para los fines investigativos.

1.. Género:
[ ] Femenino
[ ] Masculino
[ ] Prefiero no decirlo

2. Edad:
[ ] Menos de 18 años
[ ] 18 - 30 años
[ ] 31 - 50 años
[ ] Más de 50 años

3. Comunidad o sector donde reside: _____

1.4. Nivel educativo:
[ ] Sin educación formal
[ ] Primaria
[ ] Secundaria
[ ] Superior
[ ] Técnico
[ ] Otro: _____

4. Ocupación principal:
[ ] Agricultura
[ ] Artesanía
[ ] Comercio
[ ] Estudiante
[ ] Empleado
[ ] Otro: _____

5. ¿Con qué frecuencia utiliza dispositivos electrónicos (computadora, teléfono móvil) para acceder a información personal o comunitaria?
[ ] Diariamente
[ ] Semanalmente
[ ] Ocasionalmente
[ ] Nunca

6. ¿Está familiarizado(a) con el concepto de "seguridad de la información"?
[ ] Sí
[ ] No

7. ¿Utiliza contraseñas seguras para proteger sus dispositivos y cuentas?
[ ] Siempre
[ ] A veces
[ ] Nunca

8. ¿Realiza copias de seguridad de información importante?
[ ] Sí, regularmente
[ ] A veces
[ ] No

9. ¿Sabe identificar mensajes de correo o enlaces sospechosos (phishing)?
[ ] Sí
[ ] No

10. ¿Conoce la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador?
[ ] Sí
[ ] No

Comentarios adicionales o sugerencias:

_____
_____
_____
_____

Gracias por su tiempo y colaboración!
Su participación es fundamental para mejorar la seguridad de la información y la protección de datos en las comunidades indígenas rurales de Otavalo.

Anexo 3

GUÍA PARA LA IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD DE LA INFORMACIÓN EN COMUNIDADES INDÍGENAS RURALES DE OTAVALO

Subtítulo: Alineación con las Normas ISO 27002, el Código Orgánico Integral Penal (COIP) y la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador

Autor: Jimy Alejandro Enríquez Guerrón

Universidad Tecnológica Israel

Quito, Ecuador - 2025

Contenido

Introducción 52

Contextualización del Tema 52

Objetivo de la Guía 52

Público Objetivo 53

Metodología 53

Cómo Utilizar la Guía 54

1.Fundamentos Teóricos y Conceptuales 55

Seguridad de la información en comunidades indígenas 55

Ciclo de Deming (PDCA) 55

Principio de Menor Privilegio 55

Separación de Funciones (Segregación de Tareas) 55

Modelo de Amenazas y Vulnerabilidades 56

Gestión de Incidentes de Seguridad 56

2.Procedimiento, Pasos y Estrategias de Implementación 56

2.1. ..... Explicación detallada de los procesos, estrategias y metodologías recomendadas 56

2.1.1. ..... Fase 1: Evaluación y Diagnóstico de Riesgos 56

2.1.2. ..... Fase 2: Diseño del Esquema de Seguridad 57

2.1.3. ..... Fase 3: Implementación de Controles y Herramientas de Seguridad 57

2.1.4. ..... Fase 4: Capacitación y Sensibilización en Seguridad Digital 57

2.1.5. ..... Fase 5: Monitoreo, Evaluación y Mejora Continua 58

2.2. ..... Ejemplos y Casos de Aplicación 58

3.Herramientas Tecnológicas Aplicadas 58

3.1. ..... Materiales Adicionales 61

3.1.1. ..... Formularios de Evaluación de Seguridad 61

3.1.2. ..... Plantillas de Políticas de Seguridad 61

3.1.3. ..... Checklists de Seguridad 61

3.1.4. ..... Infografías Educativas 62

3.2. Recomendaciones Prácticas 62
3.2.1. Uso de Herramientas de Cifrado 62
3.2.2. Control de Accesos a la Información 62
3.2.3. Protección contra Amenazas Digitales 63
3.2.4. Educación y Concienciación en Ciberseguridad 63
4.Buenas Prácticas y Consideraciones Finales 63
4.1. Errores Comunes a Evitar 63
4.2. Sugerencias para una Mejor Implementación 64
4.3. Factores de Éxito 65
5.Conclusiones y Recomendaciones 66
Bibliografía 68

Introducción

1.4. Contextualización del Tema

En la era digital, la seguridad de la información se ha convertido en una prioridad global. Sin embargo, las comunidades indígenas en zonas rurales, como las de Otavalo, enfrentan desafíos únicos en la protección de sus datos personales y culturales. La adopción de tecnologías digitales ha crecido en estos entornos debido a la necesidad de acceder a servicios gubernamentales, financieros y educativos. No obstante, esta digitalización no ha sido acompañada por estrategias adecuadas de ciberseguridad, dejando a las comunidades expuestas a amenazas como el robo de identidad, fraudes en línea y el uso indebido de su conocimiento ancestral.

La carencia de infraestructura tecnológica segura y la limitada capacitación en ciberseguridad han generado un entorno vulnerable en el que la información personal y colectiva puede ser explotada sin consentimiento. Además, la falta de políticas locales enfocadas en la protección de datos en comunidades rurales acentúa esta problemática. Frente a este escenario, es fundamental implementar un esquema de seguridad de la información que no solo proteja los datos de estas comunidades, sino que también respete sus prácticas culturales y su autonomía en la gestión de la información.

Este documento tiene como finalidad proporcionar una guía clara y técnica para la implementación de un esquema de seguridad de la información en comunidades indígenas, alineado con normativas nacionales e internacionales como **la ISO 27002, el Código Orgánico Integral Penal (COIP) y la Ley Orgánica de Protección de Datos Personales (LOPDP).** La adopción de estas normas permitirá establecer controles de acceso, mecanismos de protección de datos y estrategias de concienciación que contribuyan a fortalecer la seguridad digital en estos entornos.

1.5. Objetivo de la Guía

El objetivo principal de esta guía es proporcionar un marco metodológico y técnico para la **implementación de un esquema de seguridad de la información** en comunidades indígenas rurales, garantizando la protección de sus datos personales y colectivos. Esta guía se centra en:

- Identificar los principales riesgos y amenazas que enfrentan las comunidades indígenas en términos de ciberseguridad.
- Establecer lineamientos y buenas prácticas basadas en normas internacionales como **ISO 27002**.
- Implementar herramientas y tecnologías accesibles para proteger la información en entornos rurales.
- Diseñar estrategias de formación y concienciación en seguridad digital adaptadas a la realidad de las comunidades.

- Crear un plan de evaluación y mejora continua que garantice la sostenibilidad del esquema de seguridad de la información.

Con esta guía, se busca empoderar a las comunidades indígenas para que gestionen de manera autónoma su información, reduciendo su vulnerabilidad ante amenazas digitales y promoviendo un uso seguro y responsable de la tecnología.

1.6. Público Objetivo

Esta guía está dirigida a diversos actores que pueden desempeñar un papel clave en la protección de la información en comunidades indígenas. Entre ellos se incluyen:

- **Líderes comunitarios y autoridades locales**: Responsables de implementar políticas de seguridad y protección de datos en la comunidad.
- **Instituciones gubernamentales y ONGs**: Entidades que trabajan en el desarrollo de estrategias digitales para comunidades rurales y buscan asegurar que la información se maneje de manera segura.
- **Docentes y centros educativos comunitarios**: Involucrados en la alfabetización digital y la formación en ciberseguridad.
- **Miembros de la comunidad indígena**: Personas que utilizan herramientas digitales y necesitan conocer cómo proteger su información personal y colectiva.
- **Expertos en ciberseguridad y desarrolladores tecnológicos**: Profesionales que pueden contribuir con soluciones tecnológicas adaptadas a la realidad de estas comunidades.

El impacto de esta guía va más allá de la protección de datos individuales, ya que también promueve la **seguridad digital colectiva**, asegurando que el conocimiento cultural y la identidad de las comunidades sean resguardados ante posibles abusos o manipulaciones externas.

1.7. Metodología

La construcción de esta guía se ha basado en un enfoque **cuantitativo y normativo**, tomando en cuenta estudios previos, normativas internacionales y entrevistas con miembros de comunidades indígenas, expertos en ciberseguridad y profesionales del sector tecnológico.

Para garantizar que el esquema de seguridad propuesto sea **efectivo y aplicable**, se han seguido los siguientes pasos metodológicos:

1. **Investigación documental**: Revisión de normativas internacionales como **ISO 27002**, la **LOPDP** en Ecuador y el **COIP**, así como estudios previos sobre ciberseguridad en entornos rurales.
2. **Análisis de riesgos**: Identificación de las principales amenazas y vulnerabilidades que afectan la seguridad de la información en comunidades indígenas.

3. **Diseño del esquema de seguridad**: Desarrollo de un modelo basado en controles de acceso, cifrado de datos, autenticación y concienciación en ciberseguridad.
4. **Validación del modelo**: Evaluación del esquema de seguridad con expertos en tecnología y miembros de la comunidad para asegurar su viabilidad y adecuación a la realidad local.
5. **Propuesta de implementación**: Desarrollo de un plan de acción con herramientas, estrategias y métricas de evaluación para monitorear su efectividad a largo plazo.

Esta metodología permite que la guía sea aplicada de manera flexible en distintas comunidades indígenas, adaptándose a sus necesidades y limitaciones tecnológicas.

1.8. Cómo Utilizar la Guía

La presente guía ha sido estructurada de manera modular para que pueda ser utilizada por distintos actores según sus necesidades específicas. A continuación, se describe cómo sacarle el máximo provecho:

Para líderes comunitarios y autoridades locales

- Revisar la sección de **normativas y regulaciones** para comprender las leyes aplicables a la protección de datos en Ecuador.
- Aplicar los **procedimientos y estrategias** descritos en la guía para fortalecer la seguridad de la información en su comunidad.
- Promover la **capacitación y formación** en ciberseguridad dentro de la comunidad.

Para instituciones gubernamentales y ONGs

- Utilizar la sección de **herramientas tecnológicas** para identificar soluciones viables en la gestión de la información.
- Apoyar la implementación de las estrategias propuestas mediante la dotación de recursos tecnológicos.
- Evaluar la **efectividad del esquema de seguridad** a través de auditorías y revisiones periódicas.

Para miembros de la comunidad indígena

- Seguir las recomendaciones sobre **buenas prácticas en seguridad digital** para evitar fraudes y ataques cibernéticos.
- Aplicar los métodos de **autenticación y cifrado de datos** en sus dispositivos personales.
- Participar en **talleres de formación en ciberseguridad** para mejorar sus conocimientos sobre protección de datos.

Para docentes y educadores

- Utilizar la sección de **concienciación y formación** para diseñar materiales didácticos sobre seguridad de la información.

- Implementar ejercicios prácticos con estudiantes sobre detección de phishing y creación de contraseñas seguras.

Para expertos en ciberseguridad y desarrolladores tecnológicos

- Revisar la sección de **evaluación y mejora continua** para optimizar las estrategias de protección de datos.
- Adaptar herramientas tecnológicas a la realidad de la comunidad para maximizar su impacto.

En resumen, esta guía ha sido diseñada para ser un **recurso práctico y aplicable**, proporcionando estrategias claras y herramientas accesibles para fortalecer la seguridad de la información en comunidades indígenas. Siguiendo sus recomendaciones, se podrá reducir significativamente el riesgo de exposición a amenazas digitales y fortalecer la autonomía de la comunidad en la gestión de su información.

1. Fundamentos Teóricos y Conceptuales

1.9. Seguridad de la información en comunidades indígenas

Las comunidades indígenas enfrentan desafíos particulares en la protección de su información debido a la brecha digital, el acceso limitado a infraestructura tecnológica y la falta de capacitación en ciberseguridad (Williamson, 2024).La digitalización ha permitido el acceso a servicios gubernamentales, educativos y financieros, pero también ha incrementado los riesgos de apropiación indebida de información cultural y datos personales (Heeks y Renken, 2016). La seguridad de la información en estos entornos debe considerar factores socioculturales, garantizando la protección de datos sin afectar la autonomía de la comunidad (Howard & Mazaheri, 2009).

1.10. Ciclo de Deming (PDCA)

El Ciclo de Deming, también nombrado como PDCA (Planificar, Hacer, Verificar, Actuar), es un medio de progreso continuo que se puede destinar en el sistema de gestión de seguridad de la información. Esta etapa implica planificar acciones, implementarlas, verificar sus resultados y tomar medidas correctivas para mejorar continuamente el SGSI (Mas y otros, 2018).

1.11. Principio de Menor Privilegio

Este principio se fundamenta en la teoría de control de acceso, que se enfoca en cómo se otorgan y gestionan los permisos de acceso a recursos en un sistema. La implementación del principio de menor privilegio se alinea con la norma ISO 27001, que hace hincapié en la importancia de controlar y limitar el acceso a la información (Aguasanta & Lozada, 2023).

1.12. Separación de Funciones (Segregación de Tareas)

La segregación de tareas se basa en la teoría de control interno, que busca garantizar que las

funciones críticas se ejecuten de manera independiente para evitar la concentración de poder y la posibilidad de manipulación. Este principio se alinea con la norma ISO 27002, que aborda el control de acceso y la gestión de privilegios (Aguasanta & Lozada, 2023).

1.13. Modelo de Amenazas y Vulnerabilidades

Este modelo está orientado en la teoría de seguridad e identificación de riesgos de la información. Se puede utilizar en grupo con la modalidad de evaluación de riesgos de la norma ISO 27005 para identificar las amenazas y vulnerabilidades más probables que enfrenta la organización, lo que permite la implementación de controles adecuados (Aguasanta & Lozada, 2023).

1.14. Gestión de Incidentes de Seguridad

La gestión de percances de seguridad es un mecanismo que engloba la respuesta, identificación, recuperación y contención de incidentes asociados con la seguridad de la información en el organismo. Esta perspectiva se basa en la teoría de gestión de incidentes y respuesta a emergencias. Se puede aplicar junto con las pautas de la norma ISO 27035 para garantizar que la organización esté preparada para rebatir eficazmente a los incidentes de seguridad y minimizar el impacto en caso de que ocurran (Aguasanta & Lozada, 2023).

2. Procedimiento, Pasos y Estrategias de Implementación

Aqui describe los procedimientos, metodologías y estrategias necesarias para implementar un esquema de seguridad de la información en comunidades indígenas rurales de Otavalo. Se establecen pasos detallados que pueden ser adaptados a diferentes contextos, priorizando la facilidad de implementación y la compatibilidad con los recursos tecnológicos disponibles.

2.1. Explicación detallada de los procesos, estrategias y metodologías recomendadas

Para la implementación de un esquema de seguridad de la información en comunidades indígenas, se sigue un modelo estructurado basado en cinco fases clave:

- Evaluación y Diagnóstico de Riesgos
- Diseño del Esquema de Seguridad
- Implementación de Controles y Herramientas de Seguridad
- Capacitación y Sensibilización en Seguridad Digital
- Monitoreo, Evaluación y Mejora Continua

Cada una de estas fases se desarrolla a continuación en detalle.

2.1.1. Fase 1: Evaluación y Diagnóstico de Riesgos

El primer paso en la implementación del esquema de seguridad es la identificación de riesgos y vulnerabilidades en la comunidad. Este análisis permite conocer qué problemas de seguridad afectan a los miembros de la comunidad y qué nivel de conocimiento tienen sobre protección de datos.

Metodología aplicada:

Aplicación de encuestas a miembros de la comunidad para evaluar su conocimiento en ciberseguridad.

Análisis de infraestructura tecnológica disponible en la comunidad.

Identificación de amenazas comunes (phishing, robo de identidad, acceso no autorizado a datos personales).

2.1.2. Fase 2: Diseño del Esquema de Seguridad

Tras identificar los riesgos, se diseña un esquema de seguridad adaptado a la realidad tecnológica y cultural de la comunidad. Este esquema debe contemplar políticas de acceso, gestión de información y control de incidentes.

Estrategias recomendadas:

Aplicación del principio de menor privilegio, limitando el acceso a información sensible solo a personas autorizadas.

Uso de contraseñas seguras y autenticación multifactor (MFA) para proteger el acceso a cuentas comunitarias.

Definición de procedimientos de respuesta ante incidentes de seguridad.

2.1.3. Fase 3: Implementación de Controles y Herramientas de Seguridad

En esta fase, se aplican herramientas tecnológicas y controles de seguridad definidos en el esquema. La implementación debe considerar la facilidad de uso y accesibilidad para los miembros de la comunidad.

Herramientas y tecnologías recomendadas:

Uso de firewalls como pfSense para proteger redes comunitarias contra accesos no autorizados.

Implementación de software de cifrado AES-256 para resguardar documentos digitales de la comunidad.

Instalación de antivirus y filtros de contenido en computadoras comunitarias para evitar infecciones por malware.

2.1.4. Fase 4: Capacitación y Sensibilización en Seguridad Digital

No basta con implementar tecnología; es crucial capacitar a los miembros de la comunidad en buenas prácticas de ciberseguridad. La educación es clave para prevenir ataques y asegurar la correcta aplicación del esquema de seguridad.

Estrategias de capacitación:

Talleres sobre creación de contraseñas seguras y detección de correos fraudulentos (phishing).

Simulaciones de ataques cibernéticos para enseñar cómo reconocer amenazas.

Elaboración de guías digitales y físicas en idioma local sobre protección de datos.

2.1.5. Fase 5: Monitoreo, Evaluación y Mejora Continua

Una vez implementado el esquema de seguridad, se requiere un monitoreo constante para detectar nuevas amenazas y ajustar las estrategias conforme evolucionen los riesgos.

Métodos de monitoreo recomendados:

Uso de herramientas como OpenVAS para escanear vulnerabilidades en redes comunitarias.

Auditorías periódicas para evaluar el cumplimiento de políticas de seguridad.

Encuestas de seguimiento para medir el impacto de la capacitación en la comunidad.

2.2. Ejemplos y Casos de Aplicación

A continuación, se presentan algunos casos prácticos donde la implementación de estas estrategias ha mejorado la seguridad digital en comunidades rurales:

Caso 1: Implementación de una Red Local Inalámbrica en la Comunidad Indígena de Otavalo

En 2018, se llevó a cabo un proyecto para establecer una red local inalámbrica en una comunidad indígena de Otavalo, Ecuador. Este proyecto tuvo como objetivo facilitar la divulgación de la historia, el sistema legal y otros datos relevantes de la comunidad, permitiendo una fácil actualización sin requerir conocimientos técnicos especializados. (Mas y otros, 2018)

Caso 2: Seguridad Comunitaria y Pueblos Indígenas

Este documento aborda la identificación de herramientas y prácticas para ayudar a suministrar información, promover y apoyar a las asociaciones comunitarias locales dedicadas a la prevención de la criminalidad y la violencia. Se centra en cómo las comunidades indígenas pueden fortalecer su seguridad comunitaria mediante la colaboración y el uso de prácticas tradicionales y modernas. (Capobianco, 2009)

Caso 3: Comunidades Indígenas y su Combate Diario ante la Discriminación

Este estudio se centra en las luchas diarias de las comunidades indígenas de Ecuador contra el racismo, la exclusión social y las violaciones de sus derechos. Aunque no se enfoca exclusivamente en la seguridad de la información, proporciona contexto sobre los desafíos que enfrentan estas comunidades en su vida diaria, lo que es relevante para comprender el entorno en el que se implementan las estrategias de seguridad. (Puma, 2023)

3. Procedimiento, Pasos y Estrategias

Entradas Externas

Estas son los factores externos que influyen en la necesidad de establecer un esquema de seguridad de la información en la comunidad.

- Amenazas digitales y ciberataques (phishing, malware, robo de identidad).

- Falta de normativas específicas en comunidades indígenas sobre protección de datos.
- Desigualdad en el acceso a tecnología y educación digital.
- Influencias externas de organizaciones y regulaciones como la ISO 27002 y la LOPDP.

Entradas Internas

Son los recursos disponibles dentro de la comunidad para implementar el esquema de seguridad.

- Infraestructura tecnológica existente (computadoras, redes de internet, servidores comunitarios).
- Nivel de conocimiento de la comunidad sobre seguridad digital.
- Liderazgo comunitario y apoyo de instituciones locales.
- Disponibilidad de herramientas y software de seguridad gratuitos o accesibles.

Fases

Son las etapas del proceso de implementación del esquema de seguridad de la información.

Evaluación y Diagnóstico de Riesgos

- Identificación de vulnerabilidades en el acceso a la información.
- Encuestas y entrevistas sobre conocimientos de ciberseguridad.
- Análisis de infraestructura tecnológica comunitaria.

Diseño del Esquema de Seguridad

- Definición de políticas y normativas internas.
- Selección de herramientas tecnológicas adecuadas.
- Creación de procedimientos para control de accesos y protección de datos.

Implementación de Controles de Seguridad

- Configuración de firewalls y herramientas de cifrado.
- Aplicación de medidas de autenticación segura.
- Establecimiento de mecanismos de monitoreo y auditoría.

Capacitación y Sensibilización en Seguridad Digital

- Talleres de ciberseguridad adaptados a la comunidad.
- Materiales en idiomas indígenas y estrategias educativas.
- Simulacros de ataques digitales para reforzar la enseñanza.

Monitoreo, Evaluación y Mejora Continua

- Auditorías regulares sobre el cumplimiento de medidas de seguridad.
- Actualización de estrategias y herramientas según nuevas amenazas.
- Retroalimentación de la comunidad sobre la efectividad del esquema.

Resultados (Salidas Internas)

Son los beneficios obtenidos a nivel interno en la comunidad después de aplicar el esquema de

seguridad.

- Mayor protección de la información comunitaria y personal.
- Reducción de ataques digitales y fraudes en la comunidad.
- Mayor conciencia y adopción de buenas prácticas de ciberseguridad.
- Creación de un entorno digital seguro y sostenible para el uso comunitario.

Impactos (Salidas Externas)

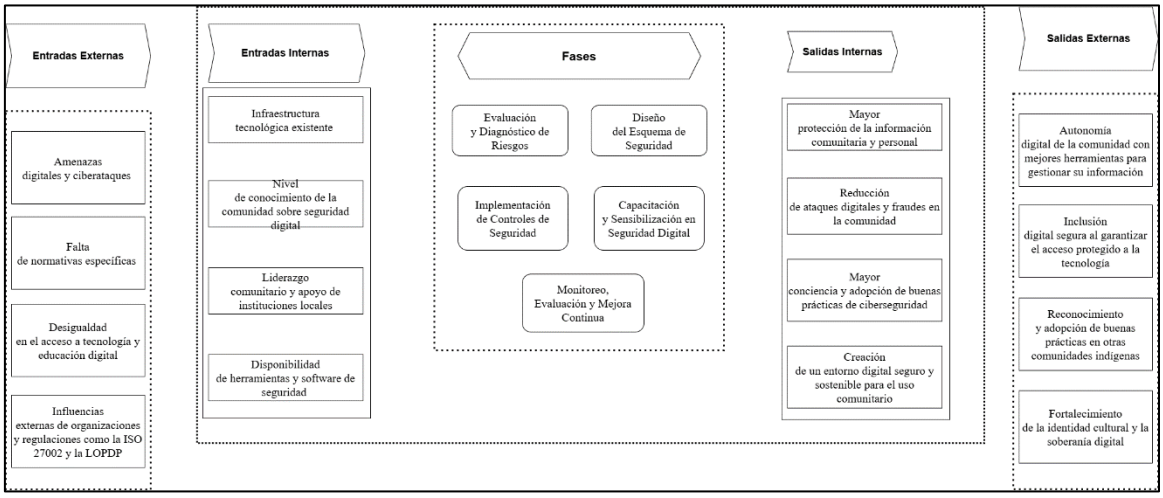
Son los efectos a largo plazo y cómo la implementación del esquema influye en la comunidad y su relación con el entorno digital.

- Autonomía digital de la comunidad con mejores herramientas para gestionar su información.
- Inclusión digital segura al garantizar el acceso protegido a la tecnología.
- Reconocimiento y adopción de buenas prácticas en otras comunidades indígenas.
- Fortalecimiento de la identidad cultural y la soberanía digital.

En la figura 1 se puede visualizar las etapas del proyecto.

Figura 12

Etapas del proyecto.



Control y Retroalimentación

El monitoreo y la mejora continua son fundamentales para asegurar que el esquema de seguridad se mantenga efectivo y actualizado.

- Evaluaciones periódicas sobre la efectividad de las medidas aplicadas.
- Ajustes en estrategias según el nivel de riesgo y amenazas emergentes.
- Capacitaciones continuas para actualizar conocimientos de ciberseguridad.
- Documentación de incidentes y mejora de protocolos de respuesta ante amenazas.

4. Herramientas Tecnológicas Aplicadas

En esta sección se presentan diversas herramientas, plantillas, checklists y materiales adicionales

que pueden ser utilizados para facilitar la implementación del Esquema de Seguridad de la Información en comunidades indígenas rurales. Además, se incluyen recomendaciones prácticas para garantizar la correcta aplicación de estas herramientas en el contexto comunitario.

4.1. Materiales Adicionales

A continuación, se presentan algunos recursos útiles que pueden ser utilizados por líderes comunitarios, instituciones y miembros de la comunidad para fortalecer la seguridad de la información.

4.1.1. Formularios de Evaluación de Seguridad

Los formularios ayudan a identificar los riesgos y vulnerabilidades dentro de una comunidad en relación con el uso de tecnología y la protección de datos.

Formulario de Evaluación de Seguridad en la Comunidad

Evaluar el nivel de conocimiento sobre seguridad digital dentro de la comunidad.

- Preguntas sobre el uso de contraseñas seguras en dispositivos personales.
- Identificación de correos electrónicos sospechosos y ataques de phishing.
- Métodos utilizados para almacenar información digital de la comunidad.
- Uso de autenticación de doble factor en servicios digitales.

4.1.2. Plantillas de Políticas de Seguridad

Las plantillas permiten definir normas y regulaciones en la comunidad para la protección de información digital.

Plantilla de Política de Uso de Internet en la Comunidad

Establecer reglas sobre el acceso y uso de internet en centros comunitarios y espacios públicos.

- Regulación del uso de redes sociales en espacios comunitarios.
- Restricción de descargas de archivos desconocidos desde internet.
- Uso obligatorio de software de seguridad en computadoras comunitarias.

Plantilla de Política de Contraseñas Seguras

Definir requisitos de seguridad para la creación y almacenamiento de contraseñas.

- Uso de contraseñas de al menos 12 caracteres con letras, números y símbolos.
- Prohibición de utilizar nombres propios o fechas de nacimiento como contraseña.
- Cambio obligatorio de contraseñas cada 90 días en cuentas críticas.

4.1.3. Checklists de Seguridad

Los checklists ayudan a verificar si se han implementado correctamente las medidas de seguridad establecidas.

Checklist de Seguridad Digital para la Comunidad

Comprobar si se están aplicando las mejores prácticas en la protección de datos.

- Uso de contraseñas seguras en dispositivos personales.
- Implementación de autenticación multifactor en cuentas importantes.
- Cifrado de documentos con información sensible.
- Instalación de software antivirus en dispositivos comunitarios.

Checklist de Protección contra Phishing

Evaluar si los miembros de la comunidad pueden identificar intentos de fraude en línea.

- Capacitación de los miembros de la comunidad sobre correos fraudulentos.
- Implementación de filtros de seguridad en correos electrónicos.
- Revisión de intentos recientes de fraude dentro de la comunidad.

4.1.4. Infografías Educativas

Las infografías son una excelente herramienta visual para explicar conceptos de seguridad digital de manera sencilla.

Cómo Crear una Contraseña Segura

Enseñar a los miembros de la comunidad a proteger sus cuentas con contraseñas seguras.

- Explicación sobre la importancia de las contraseñas largas y complejas.
- Comparación entre contraseñas débiles y seguras.
- Métodos para recordar contraseñas sin anotarlas en lugares inseguros.

Cómo Protegerse del Phishing

Explicar cómo detectar y evitar correos electrónicos fraudulentos.

- Características de un correo sospechoso.
- Diferencias entre enlaces legítimos y enlaces fraudulentos.
- Pasos a seguir en caso de recibir un intento de phishing.

4.2. Recomendaciones Prácticas

Además de los recursos anteriores, es fundamental aplicar una serie de buenas prácticas para asegurar una correcta implementación del esquema de seguridad de la información.

4.2.1. Uso de Herramientas de Cifrado

Se recomienda el uso de software de cifrado para proteger documentos con información personal o financiera.

Cifrado de discos duros y memorias USB utilizadas en oficinas comunitarias.

4.2.2. Control de Accesos a la Información

Implementación de autenticación en dos pasos en cuentas de correo electrónico comunitarias.

Establecimiento de permisos de acceso en documentos compartidos en plataformas digitales.

4.2.3. Protección contra Amenazas Digitales

Instalación de firewalls en redes comunitarias para bloquear accesos no autorizados.

Implementación de software antivirus en dispositivos utilizados por varias personas.

4.2.4. Educación y Concienciación en Ciberseguridad

Simulacros de ataques de phishing para capacitar a la comunidad.

Organización de talleres educativos sobre seguridad digital.

5. Buenas Prácticas y Consideraciones Finales

Este capítulo presenta una serie de buenas prácticas esenciales para la implementación de un Esquema de Seguridad de la Información en comunidades indígenas rurales de Otavalo. Se detallan los errores más comunes que deben evitarse, se brindan recomendaciones estratégicas para mejorar la implementación y se identifican los factores clave de éxito que asegurarán la sostenibilidad del esquema a largo plazo.

5.1. Errores Comunes a Evitar

Uno de los principales desafíos en la implementación de estrategias de seguridad de la información en comunidades rurales es la falta de planificación y adaptación a las condiciones específicas de cada entorno. Para maximizar la efectividad del esquema de seguridad, es crucial evitar los siguientes errores:

Falta de Capacitación y Concienciación en Ciberseguridad

Un problema recurrente en muchas comunidades es la falta de educación en materia de ciberseguridad. La ausencia de conocimiento sobre amenazas digitales, protección de datos personales y buenas prácticas de seguridad puede hacer que los miembros de la comunidad sean vulnerables a fraudes, robos de información y accesos no autorizados.

Para abordar esta situación, es esencial implementar programas de capacitación en seguridad digital, diseñados de manera sencilla y accesible. La información debe ser clara y adaptada al contexto local, incorporando metodologías de enseñanza visuales y participativas que permitan a los miembros de la comunidad comprender la importancia de la seguridad digital y aplicar medidas efectivas para protegerse.

Uso de Contraseñas Débiles y Compartidas

Las contraseñas son la primera línea de defensa en la protección de la información, pero en muchas comunidades se siguen utilizando credenciales débiles o compartidas entre múltiples usuarios. Esta práctica expone los sistemas a riesgos de acceso no autorizado y posibles violaciones de datos.

Para mitigar este problema, se deben implementar políticas de contraseñas seguras, promoviendo el uso de credenciales robustas que incluyan combinaciones de letras, números y

caracteres especiales. Además, es recomendable el uso de autenticación en dos pasos para aumentar la protección de las cuentas personales y comunitarias.

Falta de Control en el Acceso a la Información

Muchas comunidades indígenas rurales carecen de políticas claras sobre quién puede acceder a determinada información. En muchos casos, documentos importantes y bases de datos están disponibles sin restricciones, lo que aumenta el riesgo de manipulación, pérdida o robo de datos.

Para evitar este problema, se deben establecer niveles de acceso según el rol de cada usuario dentro de la comunidad. Los permisos deben ser configurados de tal manera que solo las personas autorizadas puedan acceder a información crítica, reduciendo así el riesgo de exposición indebida.

No Realizar Copias de Seguridad de la Información

La falta de un sistema de respaldo de datos puede llevar a la pérdida de información valiosa en caso de incidentes como fallos técnicos, ataques cibernéticos o desastres naturales. Muchas comunidades rurales no cuentan con un protocolo establecido para la realización de copias de seguridad, lo que las deja en una situación de vulnerabilidad ante estos escenarios.

Es fundamental implementar políticas de respaldo periódico de la información, almacenando copias de seguridad en dispositivos externos y en plataformas de almacenamiento en la nube. Estas copias deben realizarse de forma regular y verificarse periódicamente para asegurar su integridad y disponibilidad en caso de necesidad.

5.2. Sugerencias para una Mejor Implementación

Para garantizar el éxito en la aplicación del esquema de seguridad de la información en comunidades indígenas rurales, se recomienda seguir una serie de estrategias y buenas prácticas diseñadas para maximizar su efectividad y sostenibilidad.

Implementar Políticas de Seguridad Escritas y de Fácil Acceso

Un error común en la gestión de la seguridad de la información es la falta de documentación y procedimientos formalizados. Es importante que cada comunidad cuente con un manual de políticas de seguridad, en el que se definan reglas claras sobre el acceso, almacenamiento y uso de la información.

Este documento debe ser elaborado de manera sencilla y accesible para todos los miembros de la comunidad. Además, debe estar disponible en formato digital e impreso en lugares estratégicos dentro de la comunidad, facilitando su consulta y aplicación.

Promover la Cultura de Seguridad Digital en la Comunidad

Más allá de la implementación de herramientas tecnológicas, es fundamental que la seguridad de la información sea adoptada como parte de la cultura comunitaria. Para ello, se deben fomentar iniciativas de sensibilización y concienciación sobre la importancia de la

protección de datos.

Estas iniciativas pueden incluir charlas, talleres y material educativo enfocado en cómo evitar fraudes digitales, cómo reconocer correos electrónicos sospechosos y cómo proteger información personal en dispositivos móviles y computadoras compartidas.

Usar Herramientas de Código Abierto para Reducir Costos

Uno de los mayores desafíos en comunidades rurales es el acceso a tecnología avanzada debido a las limitaciones económicas. En este sentido, el uso de herramientas de código abierto es una alternativa viable y efectiva para mejorar la seguridad de la información sin incurrir en grandes costos.

Se recomienda el uso de software libre para la gestión de seguridad, como firewalls, antivirus y sistemas de cifrado, que permitan a las comunidades proteger su información sin necesidad de invertir en soluciones comerciales costosas.

Realizar Simulacros de Ataques Cibernéticos

Para fortalecer la capacidad de respuesta ante incidentes de seguridad, es recomendable realizar simulaciones de ataques digitales dentro de la comunidad. Estas pruebas pueden ayudar a los miembros a identificar posibles vulnerabilidades en sus sistemas y mejorar su capacidad de reacción frente a amenazas reales.

Algunos ejercicios útiles incluyen la simulación de intentos de phishing, la detección de accesos no autorizados y la práctica de recuperación de datos ante la pérdida accidental de información.

5.3. Factores de Éxito

Para asegurar que la implementación del esquema de seguridad de la información sea efectiva y sostenible a largo plazo, se deben considerar los siguientes factores clave:

Liderazgo Comunitario Activo en Seguridad de la Información

El éxito de un esquema de seguridad digital depende en gran medida del compromiso de los líderes comunitarios en la promoción y aplicación de medidas de protección de datos. Es esencial contar con figuras de referencia dentro de la comunidad que puedan guiar y supervisar la correcta aplicación de las estrategias de seguridad.

Los líderes comunitarios deben actuar como facilitadores, asegurándose de que la información sobre ciberseguridad llegue a todos los miembros de la comunidad y que se respeten las políticas de seguridad establecidas.

Capacitación Continua en Ciberseguridad

El conocimiento en seguridad digital debe actualizarse constantemente para hacer frente a nuevas amenazas y vulnerabilidades. La implementación de un programa de formación continua permitirá que los miembros de la comunidad estén mejor preparados para gestionar riesgos y reaccionar ante posibles ataques.

Este programa puede incluir sesiones periódicas de capacitación, acceso a cursos en línea y la distribución de material educativo que refuerce la importancia de la protección de la información.

Monitoreo y Evaluación Constante del Esquema de Seguridad

Un esquema de seguridad debe ser dinámico y adaptarse a las necesidades cambiantes de la comunidad. Para ello, es necesario establecer mecanismos de monitoreo y evaluación que permitan medir la efectividad de las estrategias implementadas y realizar ajustes cuando sea necesario.

Es recomendable realizar auditorías periódicas para identificar posibles vulnerabilidades y garantizar que se cumplan las políticas de seguridad establecidas.

6. Conclusiones y Recomendaciones

La seguridad de la información es un elemento clave para garantizar la protección de datos personales y comunitarios en las comunidades indígenas rurales de Otavalo. Con el crecimiento del acceso a herramientas digitales, estas comunidades han visto mejorar sus oportunidades en educación, comunicación y servicios administrativos. Sin embargo, también han surgido nuevas vulnerabilidades, como el robo de identidad, fraudes digitales y la apropiación indebida de conocimientos culturales. La implementación de un esquema de seguridad de la información es fundamental para fortalecer la autonomía digital y reducir los riesgos asociados a la tecnología.

Esta guía ha proporcionado un enfoque práctico para desarrollar estrategias de ciberseguridad adaptadas a la realidad de estas comunidades. La aplicación de buenas prácticas como el uso de contraseñas seguras, la implementación de controles de acceso y la concienciación sobre riesgos digitales ha demostrado ser efectiva en diversos entornos. Sin embargo, la seguridad digital no debe verse como una acción puntual, sino como un proceso continuo que requiere monitoreo, adaptación y educación constante. Para lograrlo, es indispensable el compromiso de los líderes comunitarios, docentes, instituciones y todos los miembros de la comunidad.

Una de las principales áreas de mejora en la implementación del esquema de seguridad es la accesibilidad del conocimiento. Muchas de las herramientas y metodologías disponibles en ciberseguridad están diseñadas en idiomas técnicos y formatos poco comprensibles para las comunidades indígenas. Por ello, es fundamental traducir estos contenidos a lenguas originarias y desarrollar materiales educativos adaptados a su contexto sociocultural. Además, la capacitación debe ser un proceso continuo, promoviendo programas de formación en seguridad digital con enfoque comunitario.

El acceso a la tecnología sigue siendo desigual en muchas comunidades rurales, lo que limita la posibilidad de implementar herramientas de seguridad avanzadas. Para superar este obstáculo, es

recomendable el uso de software de código abierto y soluciones de bajo costo que permitan garantizar la protección de datos sin generar gastos elevados. Asimismo, los centros comunitarios de acceso a internet deben contar con políticas de seguridad bien definidas, evitando que la información sensible quede expuesta a riesgos innecesarios.

Otro aspecto fundamental es la creación de programas de certificación en seguridad digital para líderes indígenas. La figura de un "guardián digital" dentro de cada comunidad permitiría supervisar la implementación de buenas prácticas y actuar como enlace con expertos en ciberseguridad. Además, fortalecer el marco legal en torno a la protección de datos en comunidades indígenas contribuiría a garantizar que estas estrategias sean reconocidas y respaldadas a nivel institucional, permitiendo que los derechos digitales sean considerados dentro del marco de autonomía de los pueblos originarios.

Las mejoras futuras en la seguridad de la información en comunidades indígenas deben enfocarse en la sostenibilidad y la actualización constante de estrategias. La evolución de las amenazas digitales hace necesario que los esquemas de seguridad sean dinámicos y flexibles, adaptándose a los nuevos riesgos que puedan surgir. Establecer mecanismos de monitoreo, auditorías periódicas y alianzas con organizaciones especializadas en ciberseguridad permitirá mejorar continuamente la protección de la información en estos entornos.

Bibliografía

Aguasanta, P., & Lozada, E. (2023). *PLAN DE SEGURIDAD INFORMÁTICO BASADO EN LAS NORMAS ISO 27001 Y 27002 PARA EL COMERCIAL "EL FERRETERO" DE LA CIUDAD DE TENA.*

Capobianco, L. (2009). *Seguridad comunitaria y pueblos indígenas: Compartiendo Conocimiento, Aprendizajes y Acción.* https://cipc-icpc.org/wp-content/uploads/2019/09/Seguridad_comunitaria_y_pueblos_indigenas._Compartiendo_Conocimiento__Aprendizajes_y_Accion_ESP.pdf

Howard, & Mazaheri. (2009). *Telecommunications Reform, Internet Use and Mobile Phone Adoption in the Developing World.* https://doi.org/10.1016/j.worlddev.2008.12.005

Mas, M., Íñiguez, G., & Botero, H. (2018). *Red local inalámbrica en la comunidad indígena de Otavalo.* https://www.researchgate.net/publication/335032004_Red_local_inalambrica_en_la_comunidad_indigena_de_Otavalo_Ecuador_2018

Puma, J. (2023). *Comunidades indígenas y su combate diario ante la discriminación.* https://dialnet.unirioja.es/descarga/articulo/9124236.pdf