PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

TECNOLOGÍA SUPERIOR

ADMINISTRACIÓN DE LAS ORGANIZACIONES DE LA ECONOMÍA POPULAR Y SOLIDARIA

TEMA:

"Plan de negocios para la creación de una cooperativa de servicios digitales en ciberseguridad en la ciudad de Quito, 2026"

Trabajo de investigación previo a la obtención del título de Tecnólogo Superior en Administración de Organizaciones de la Economía Popular y Solidaria.

Autor: *Andrés Jonathan Inga Gallo*

Tutor: MSc. Williams Vallejo Roja

Quito - Ecuador

2026

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

DECLARACIÓN y AUTORIZACIÓN

Yo, Jonathan Andrés Inga Gallo con C.I. 1722404942 autor(a) del trabajo de titulación intitulado:

Trabajo de investigación previo a la obtención del título profesional de Tecnólogo Superior en Administración de Organizaciones de la Economía Popular y Solidaria.

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación 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.- Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE el referido trabajo de titulación, respetando las políticas de propiedad intelectual de Universidad.

Quito, agosto 2025

Jonathan Andrés Inga Gallo

C.L.1722404942

Tabla de contenido

Índice de Tablas

Índice de Ilustraciones

Capítulo 1

Introducción

El crecimiento digital se ha destacado en los últimos años, especialmente durante la pandemia de COVID-19. En América Latina, el acceso a internet ha permitido el crecimiento de emprendimientos digitales, el comercio electrónico, teletrabajo, etc. En este contexto, la creación de una cooperativa de servicios tecnológicos orientada a la protección y seguridad de la información busca atender las necesidades de organizaciones de la EPS y empresas expuestas a riesgos cibernéticos. En el Ecuador uno de los principales riesgos es la falta de gestión y dedicación exclusiva de ciberseguridad en las organizaciones, empresas o instituciones. Junto con estos porcentajes bajos de protección los tipos de ataques más frecuentes a instituciones son el phishing, ingeniería social y software espía.

La iniciativa se fundamentada en principios cooperativos, prioriza la colaboración, la innovación tecnológica y el impacto social, posicionándose como un modelo sostenible y eficiente para contribuir a la protección de los activos digitales en las organizaciones y empresas. La presente propuesta tiene como fin satisfacer las necesidades tecnológicas de las organizaciones e introducirlas en una propuesta innovadora brindando los servicios de nueva generación como ciberseguridad.

Importancia y Diagnóstico

En la actualidad vivimos en una época en la que la tecnología no es solo una herramienta, sino una verdadera fuente de oportunidades, sin embargo, con este crecimiento tambien aumentan las amenazas cibernéticas.

La cooperativa de ciberseguridad va más allá de ser solo un modelo técnico; se convertirá en un refugio de resiliencia digital para emprendedores, organizaciones de la EPS, pequeñas y medianas empresas que se enfrentan a amenazas en un entorno donde" el 68% de los ciberataques en Ecuador impactan a los pequeños negocios" (Centro de Respuesta a Incidentes Cibernéticos del Ecuador, 2022)

La cooperativa busca beneficiar a las organizaciones transmitiendo una información eficaz que eviten perdidas en sus datos y activos digitales, su propósito se alinea con el ODS 8, que promueve el trabajo decente, al fomentar la creación de empleo técnico inclusivo. También se relaciona con el ODS 9, que impulsa la innovación, al facilitar el acceso a la ciberseguridad. Además, contribuye a reducir las desigualdades (ODS 10) al apoyar a las cooperativas rurales y fortalece la resiliencia urbana (ODS 11) en Quito, estableciendo alianzas (ODS 17) con actores clave. Su misión no solo se alinea con el ODS 8 (trabajo decente), sino que también respalda el ODS 9 (industria e innovación), al facilitar el acceso a tecnologías seguras en un país que ocupa el puesto 119 de 182 en el Índice Global de Ciberseguridad.

Estructura del Proyecto

La investigación realizada no solo busca demostrar la viabilidad de la cooperativa, sino que también propone un camino claro y estructurado hacia su creación.

Aplicando la estructura del documento a continuación tendremos una secuencia de tres capítulos que demuestran aspectos esenciales para el desarrollo del plan de negocio:

Fundamentación Teórica

El enfoque teórico se complementa con un análisis crítico de la brecha digital en la EPS, mostrando cómo la autogestión tecnológica puede ser una herramienta de resiliencia frente a las ciber amenazas.

Al final, se comparan estos principios con las políticas públicas locales para descubrir oportunidades de colaboración. (Plan Quito digital, 2023-2027)

Diagnóstico Situacional Estratégico

Aquí se presenta un análisis detallado de las condiciones actuales, donde se evalúan tanto los factores internos como externos que podrían afectar la viabilidad y factibilidad del proyecto. Este diagnóstico incluye estadísticas, estudios de mercado y entrevistas con expertos en seguridad y ciberseguridad, brindando una perspectiva realista y bien fundamentada sobre los desafíos y oportunidades en este mercado que ha sido descuidado.

Propuesta del Modelo de Negocio

Este último capítulo ofrece una visión detallada de la propuesta para la Cooperativa, abarcando su estructura organizativa, los mecanismos de operación y cómo se garantizará su sostenibilidad financiera. También se plantean estrategias para atraer a nuevos miembros, facilitar el acceso a recursos tecnológicos y fomentar la concientización en ciberseguridad. Esta estructura no solo organiza el contenido del proyecto, sino que también demuestra el compromiso de abordar el desafío de manera integral, humana y estratégica. A medida que el lector avanza por estos capítulos, se espera que comprenda no solo la relevancia de esta iniciativa, sino también los pasos necesarios para hacerla realidad.

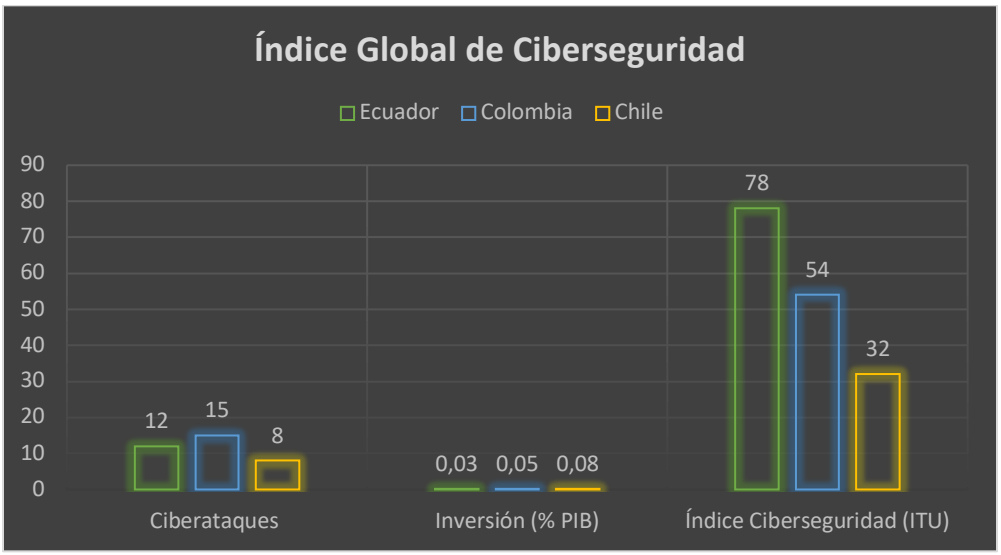
Contexto Externo

Contexto Internacional

Según (GCI, 2024) "El Ecuador es vulnerable ante las amenazas cibernéticas, esto de acuerdo con el Índice Global de Ciberseguridad (GCI), emitido por la ITU, publicado en el año 2024, que ubica al país en el puesto 78 de 194, siendo 194 el país con mayores vulnerabilidades a nivel mundial."

Ilustración 1

Índice global de ciberseguridad



Nota. Situación crítica Ecuador es el segundo país más vulnerable en ciberseguridad en la región andina, solo superado por Bolivia.

Contexto Nacional y local

Factores Políticos

En Ecuador, las políticas públicas han promovido la creación de asociaciones y cooperativas a través de la Ley Orgánica de Economía Popular y Solidaria (2011) y el Plan Nacional de Desarrollo 2021-2025.

Según el informe Estado de Ciberseguridad en Ecuador, elaborado por la firma Deloitte, que encuestó a cerca de 100 empresas a escala nacional: El 51% de las organizaciones tiene un responsable que cubre la seguridad física y digital. El 13% no cuenta con un experto entre su personal. Pero, además solo el 3% de las empresas aplican herramientas que amortiguan los riesgos cibernéticos de almacenamiento en la nube. (Sayago-Heredia, 2022)

Tabla 1

Diagnóstico de Ciberseguridad en Empresas Ecuatorianas

Indicador	Porcentaje	Interpretación
Organizaciones con responsable de seguridad física y digital	51%	La mayoría de estas empresas comparten roles improvisados en seguridad digital
Empresas sin experto en ciberseguridad	13%	Falta concientización y desconocimiento de riesgos ante ataques cibernéticos
Empresas con protección en almacenamiento cloud(nube)	3%	Brecha alarmante en seguridad física y digital
Organizaciones sin responsable de seguridad física y digital	33%	Mercado desatendido

Nota. Cálculos basados en datos de Deloitte. El 3% de empresas protegidas corresponde principalmente a grandes corporaciones del sector bancario.

Se puede interpretar que el entorno político del Ecuador representa una oportunidad para la creación de una cooperativa de servicios digitales en ciberseguridad, debido al respaldo normativo existente hacia las organizaciones de la Economía Popular y Solidaria y al impulso gubernamental a la transformación digital. Aunque existen riesgos asociados a la burocracia y

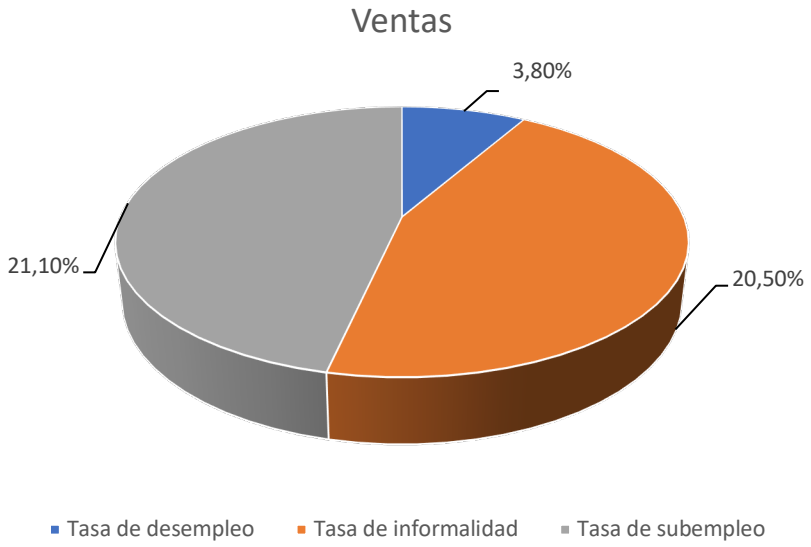
posibles cambios de administración, la afectación es baja, lo que permite avanzar con seguridad en el desarrollo del proyecto.

Factores Económicos

En el Ecuador según el INEC (INEC, 2025) la tasa de desempleo y subempleo se mantienen relativamente estables, pero con algunas variaciones. La tasa de desempleo en el primer trimestre de 2025 fue del 3,8%, mientras que la tasa de subempleo fue del 20,5%. La tasa de informalidad laboral también es alta, alcanzando el 55,7%

Ilustración 2

Tasa de empleo, desempleo y subempleo



Nota. La taza de desempleo es crítica en el país.

En conclusión, los factores como el desempleo, la inflación y las limitaciones en el acceso a financiamiento pueden representar ciertos retos. En este sentido, se considera que la

afectación económica es media y puede ser gestionada adecuadamente mediante una planificación financiera eficiente.

Factores Sociales

El acceso a internet y a herramientas tecnológicas sigue siendo desigual en Ecuador.

Según la Encuesta Nacional de Empleo, Desempleo y Subempleo (ENEMDU, 2022), menos del 45% de los hogares ecuatorianos tienen acceso a internet fijo, y en zonas rurales, la cifra cae a 15%.

Tabla 2

Acceso a internet y herramientas tecnológicas

Indicador	**Valor**	**Fuente**
Hogares con acceso a internet fijo en Ecuador	**45%**	ENEMDU (2022)
Acceso a internet en zonas Rurales	**15%**	ENEMDU (2022)
Penetración de smartphones en Ecuador	**82%**	ARCOTEL (2023)
Acceso a educación digital	**60%**	SENESCYT (2023)

en áreas urbanas		
Población con habilidades digitales básicas	**37%**	Ministerio de Telecomunicaciones (2023)

Nota. Brecha Digital y Acceso a Tecnología en Ecuador.

La Cooperativa buscará minimizar la brecha digital mediante capacitaciones, acceso a herramientas tecnológicas y conectividad, fortaleciendo la conciencia en ciberseguridad.

De igual forma la Asociación Ecuatoriana de Ciberseguridad (AECI), realizó un estudio en el primer semestre del año 2020, en donde se identificó la alta afectación en el Ecuador donde uno de los principales riesgos es la falta de gestión y dedicación exclusiva de ciberseguridad en las empresas o instituciones. Junto con estos porcentajes bajos de protección los tipos de ataques más frecuentes a instituciones son el phishing, ingeniería social y software espía. (Sayago-Heredia, 2022)

En conclusión, la población ecuatoriana muestra una creciente familiarización con las tecnologías digitales, lo que favorece la aceptación de servicios de ciberseguridad. Sin embargo, aún persiste una brecha digital en ciertos sectores sociales, lo que puede limitar el alcance del mercado objetivo. La afectación social es baja, y representa más una oportunidad que una amenaza.

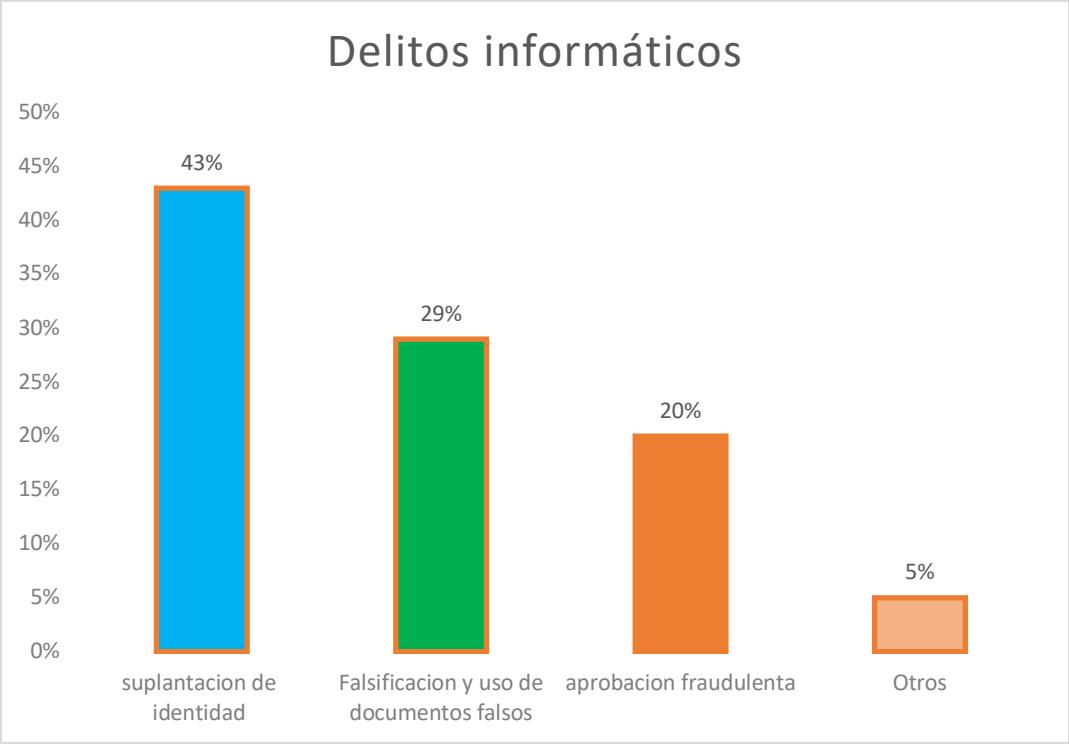
Factores Tecnológicos

Según datos de la Fiscalía General del Estado, hasta agosto de 2020, se registraron 5.048 denuncias por delitos informáticos, en el Ecuador. El 92% se concentra en los delitos como: suplantación de identidad (43%), falsiicación y uso de documento falso (29%) y apropiación

fraudulenta por medios electrónicos (20%). Esta alarmante situación incluso se acentuó en el marco de la pandemia ocasionada por el COVID-19. (SFPS, 2021)

Ilustración 3

Delitos informáticos



Nota. Es fundamental contar con información sobre el estado y avances tanto en cuanto a la digitalización de servicios, como en relación a la prevención, vigilancia e iniciativas adoptadas en el ámbito de Seguridad de la Información y Ciberseguridad.

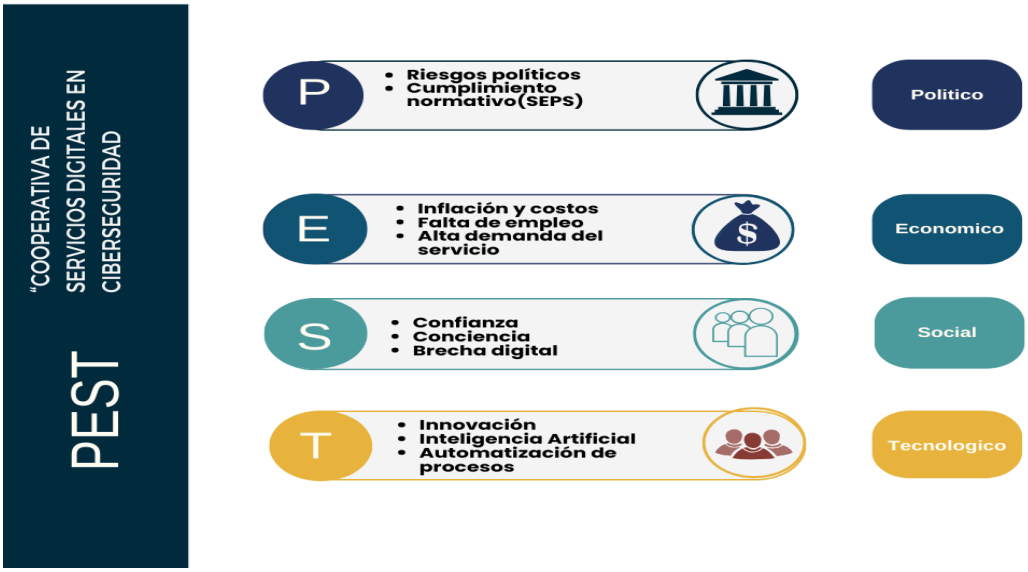
Se puede interpretar que los avances tecnológicos, especialmente en inteligencia artificial y automatización, ofrecen herramientas innovadoras para la detección de amenazas, reducción de costos operativos y mejora en la protección de sistemas. En Ecuador, existe una creciente adopción de tecnologías digitales y una conciencia sobre la importancia de la ciberseguridad. La

falta de proveedores cooperativos en este sector evidencia una brecha que este modelo de negocio podría aprovechar. La afectación tecnológica es altamente positiva.

Incidencia de los Factores PEST

Ilustración 4

Factores PEST



Nota. La ilustración muestra los factores políticos, económicos, sociales y tecnológicos.

Ilustración 5

Análisis de los factores PEST

Factores	Descripción	Muy negativo	Indiferente	Positivo	Deseable
Político	Riesgos políticos				
Económico	Inflación y costos				
Sociocultural	Cultura de prevención				
Tecnológico	Innovación				

Nota. La ilustración muestra que los factores políticos y económicos del pais no son favorables, sin embargo, los factores sociales y tecnológicos son alentadores.

Ante los datos analizados se puede interpretar que los riesgos políticos y económicos son factores que afectan directamente al ser inestables, sin embargo, la innovación tiende a ser aceptada rápidamente, con esa ventaja podemos crear una cultura de prevención sobre los riesgos cibernéticos en organizaciones, empresas y usuarios finales impulsando la demanda de servicios digitales en ciberseguridad.

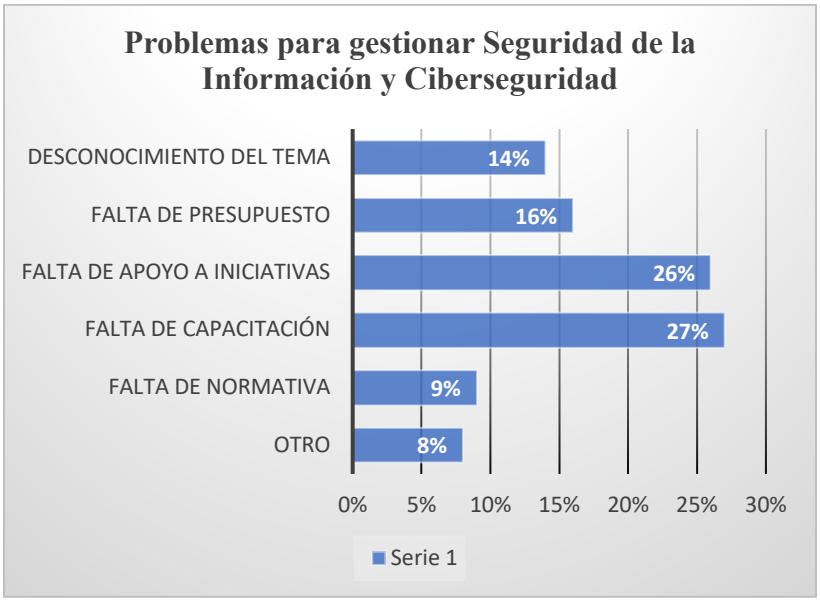
Contexto Interno y Específico

La propuesta de creación de una cooperativa de servicios digitales en ciberseguridad nace en un entorno donde las amenazas informáticas han incrementado significativamente, especialmente en sectores financieros y cooperativos, los cuales manejan datos sensibles y recursos digitales de alto valor. En este escenario, la ausencia de cooperativas que ofrezcan servicios especializados en ciberseguridad representa una oportunidad estratégica dentro del mercado local de Quito.

Los principales problemas que enfrenta el sector de la EPS en el manejo de la Seguridad de la Información y la Ciberseguridad. Los resultados arrojan que el 27% de las entidades indican que los problemas provienen de la falta de capacitación, mientras que el 26% de las entidades señala que los problemas derivan de la falta de apoyo e iniciativas por parte de la alta gerencia. El 16% de las entidades encuestadas menciona la falta de presupuesto como principal problema, mientras que un 14% mencionan como problema al desconocimiento del tema (seguridad y Ciberseguridad) y un 9% a la falta de normativa.

Ilustración 6

Porcentajes de los problemas para gestionar riesgos cibernéticos



Nota. la ilustración muestra el desconocimiento en temas de seguridad de la información y ciberseguridad.

Análisis de las 5 Fuerzas Competitivas de Porter

Para entender el entorno competitivo y cómo afecta a las organizaciones de la EPS de Quito, se debe analizar el contexto utilizando las 5 Fuerzas de Porter:

Clientes

Según el Ministerio de Telecomunicaciones y de la Sociedad de la Información de Ecuador, los ciberataques en Quito han experimentado un aumento del 35% en el último año. Esto destaca la creciente amenaza que enfrenta la ciudad en el ámbito digital y la necesidad de fortalecer sus defensas cibernéticas. (Latam, s.f.)

En el mercado de servicios digitales en ciberseguridad, los clientes especialmente las cooperativas y pequeñas empresas tienden a comparar precios, calidad y soporte técnico antes de contratar un proveedor. Dado que existen varias empresas privadas consolidadas en el sector y la ciberseguridad no es aún una necesidad percibida como urgente por todos los actores, el poder de negociación de los clientes es alto. Esto obliga a la nueva cooperativa a ofrecer propuestas de valor diferenciadas, precios competitivos y confianza en el servicio.

En conclusión, es preocupante el aumento del 35% en ciberataques en Quito, muestra que cada vez más empresas, especialmente pequeñas y medianas, necesitan protección digital. Sin embargo, como estas organizaciones comparan cuidadosamente opciones antes de contratar servicios, la cooperativa deberá destacarse no solo por precios justos, sino por ofrecer un trato cercano, soluciones a medida y una atención que genere verdadera confianza en sus clientes.

Proveedores

Los proveedores en este sector incluyen desarrolladores de software de ciberseguridad, plataformas de análisis, infraestructura tecnológica y talento humano especializado. Si bien existen múltiples opciones de proveedores en el mercado nacional e internacional, la alta especialización en ciberseguridad puede limitar las alternativas viables y aumentar los costos. No obstante, el modelo cooperativo permite negociar colectivamente y establecer alianzas estratégicas, lo que reduce la dependencia individual de proveedores y deja una brecha de negociación moderada.

En conclusión, al adaptarse al modelo cooperativo y aplicando alianzas estratégicas, se podría negociar en equipo y formar redes de apoyo mutuo, no solo se logran mejores condiciones, sino que se fortalece la capacidad de ofrecer soluciones accesibles sin sacrificar calidad.

Competencia

La creciente demanda de servicios de ciberseguridad y la baja barrera de entrada para consultores independientes o pequeñas firmas tecnológicas hacen que nuevos competidores puedan ingresar al mercado con relativa facilidad. Sin embargo, el enfoque cooperativo y solidario ofrece una propuesta de valor distinta que puede generar fidelización en segmentos específicos del mercado, como las organizaciones de la Economía Popular y Solidaria. La amenaza es moderada alta, por lo que se requiere innovación continua y diferenciación.

En conclusión, la competencia en ciberseguridad es intensa por la facilidad de entrada al mercado o la falta de control a empresas que figuran como organizaciones de la EPS para beneficio de su normativa y leyes. Para mantenerse relevante, la cooperativa deberá innovar constantemente y reforzar su identidad colaborativa como principal diferenciador.

Productos Sustitutos

Existen algunos sustitutos indirectos como software de seguridad gratuito o soluciones automáticas con inteligencia artificial que prometen proteger sin intervención técnica constante. Sin embargo, estos sustitutos no ofrecen el mismo nivel de personalización, acompañamiento ni análisis especializado que una empresa o cooperativa puede brindar. Por ello, la amenaza de sustitutos es baja a moderada, aunque puede aumentar si no se mantiene un valor agregado en los servicios ofrecidos.

Se puede concluir diciendo que, en el mercado existen alternativas automatizadas y gratuitas. La cooperativa se destaca por ofrecer soluciones a medida con acompañamiento personalizado que se adapte a cada organización. Para mantener esta ventaja, se debe seguir enfatizando el enfoque cercano y especializado.

Amenaza de Nuevos Competidores

En Quito ya operan varias empresas especializadas en ciberseguridad, algunas con experiencia internacional y servicios avanzados. Esta competencia es intensa, especialmente en el segmento empresarial. No obstante, ninguna de estas entidades opera bajo el modelo cooperativo ni se enfocan en atender específicamente a las organizaciones de la Economía Popular y Solidaria, lo que abre un nicho potencial. La rivalidad es alta, pero con un enfoque claro y estratégico, se puede posicionar la cooperativa de forma sólida.

En conclusión, tomando en cuenta los competidores la amenaza de nuevos competidores es intermedia por la competencia existente, pero el enfoque cooperativo y especializado en la Economía Popular y Solidaria permite ocupar un nicho único en el mercado de la ciudad de Quito.

Formulación del Problema

En la ciudad de Quito, las organizaciones que conforman la Economía Popular y Solidaria, especialmente las cooperativas de ahorro y crédito enfrentan crecientes riesgos asociados a la seguridad digital debido al incremento de las amenazas informáticas y a la digitalización de sus procesos. Sin embargo, la oferta de servicios especializados en ciberseguridad está dominada por empresas privadas, cuyas soluciones resultan en muchos casos inaccesibles o poco adaptadas a las necesidades y capacidades del sector solidario.

Ante esta situación, no existe hasta el momento una cooperativa de servicios digitales que brinde soluciones de ciberseguridad con un enfoque solidario, participativo y adaptado a las características de estas organizaciones. Esta ausencia limita el fortalecimiento tecnológico del sector, expone a las entidades a vulnerabilidades informáticas y representa una barrera para su sostenibilidad en un entorno cada vez más digitalizado.

Por tanto, surge la necesidad de desarrollar un plan de negocios que permita crear una cooperativa especializada en servicios digitales de ciberseguridad, orientada a cubrir esta demanda insatisfecha, garantizar la protección de datos y apoyar el crecimiento seguro de las organizaciones de la Economía Popular y Solidaria en el entorno digital.

Objetivo general

Elaborar el plan de negocios para la creación de una cooperativa de servicios digitales en ciberseguridad en la ciudad de Quito, 2026.

Objetivos específicos

Analiza la teoría más significativa para la creación de un plan de negocios de una cooperativa de servicios digitales en ciberseguridad.

Identificar las necesidades y preferencias de los clientes a la hora de buscar un servicio de ciberseguridad.

Determinar la viabilidad de la creación de un plan de negocios de una cooperativa de servicios digitales en ciberseguridad.

Metodología

En esta sección se explica el enfoque metodológico que se empleará para desarrollar el trabajo. Se describe el tipo de investigación que se llevará a cabo, se identifica la población de estudio y se define la muestra. Finalmente, se detalla el procedimiento para recolectar la información, incluyendo los métodos, técnicas e instrumentos que se utilizarán.

Para la recolección de datos cuantitativos, se diseñará una encuesta estructurada con preguntas cerradas, orientadas a conocer el nivel de digitalización de las cooperativas, su vulnerabilidad ante ciberataques, la disponibilidad para invertir en ciberseguridad y la disposición a contratar servicios desde una cooperativa tecnológica local.

Adicionalmente, se llevará a cabo una entrevista semiestructurada a expertos en ciberseguridad y representantes de cooperativas, con el fin de profundizar cualitativamente en temas como los riesgos informáticos más frecuentes, las barreras para la contratación de servicios digitales y la viabilidad de crear una cooperativa especializada en este ámbito. La aplicación de ambos métodos permitirá enriquecer el análisis del contexto económico social del proyecto.

Tipo de investigación

En este proyecto se desarrollará una investigación utilizando un enfoque de métodos mixtos, tanto cuantitativos como cualitativos, con el fin de obtener una visión integral sobre la necesidad, demanda y percepción de los servicios de ciberseguridad dentro de las organizaciones de la Economía Popular y Solidaria (EPS), específicamente en las cooperativas de ahorro y crédito de la ciudad de Quito.

Población

Según la Superintendencia de Economía Popular y Solidaria (SEPS, 2024), en la ciudad de Quito se registran 85 cooperativas de ahorro y crédito activas, que representan el universo de estudio, en tanto constituyen el segmento de mercado principal para los servicios digitales de ciberseguridad.

En cuanto al análisis del entorno competitivo, se identificaron al menos tres empresas especializadas en servicios de ciberseguridad en Quito, como Killka-Tech, Greenetics, y KCPACITEC, lo que demuestra un mercado aún en expansión con oportunidad para nuevas propuestas cooperativas (Nexdu, 2024).

Muestra

Dado que el universo de cooperativas en la ciudad de Quito es finita y demasiado pequeña, no se calculará una muestra estadística ya que según la SEPS Quito cuenta con 85 cooperativas de ahorro y crédito activas las cuales serán encuestadas para la obtención de los resultados que se pretenden obtener.

Variables

Las variables cuantitativas del estudio estarán relacionadas con:

Nivel de conocimiento sobre ciberseguridad

Uso actual de herramientas digitales

Frecuencia de incidentes de seguridad

Presupuesto destinado a tecnología

Interés en contratar servicios desde una cooperativa

Las variables cualitativas permitirán explorar:

La percepción sobre riesgos cibernéticos

Opiniones sobre la creación de una cooperativa tecnológica

Recomendaciones sobre servicios prioritarios

Instrumentos

Se utilizarán dos instrumentos principales:

Encuesta cuantitativa con 12 preguntas, distribuidas en 3 secciones: nivel de digitalización, percepción de riesgos, y disposición a adquirir servicios.

Guía de entrevista cualitativa con 5 preguntas abiertas, dirigida a expertos en tecnología, representantes de cooperativas, y funcionarios de la SEPS, para captar su visión sobre la implementación de una cooperativa de servicios digitales en el sector EPS.

Ambos instrumentos serán validados a través de juicio de expertos y aplicados de forma digital.

Procedimiento

La recolección de datos se realizará en dos fases:

Primera fase cuantitativa: se enviarán encuestas electrónicas a los representantes legales y tecnológicos de las 85 cooperativas seleccionadas. Se utilizará la herramienta Google Forms para su distribución.

Segunda fase cualitativa se organizarán entrevistas en modalidad presencial o virtual a lideres de opinión, expertos en ciberseguridad y seguridad cibernética por Zoom o Google Meet, dependiendo la disponibilidad y por el medio que se llegue a concretar la entrevista o sesiones grabadas como evidencia, con el consentimiento de los participantes, para su posterior transcripción y análisis.

Análisis de datos

Cuantitativos

Los datos se analizarán mediante estadística descriptiva, presentando frecuencias, promedios y porcentajes. Se utilizarán gráficos de barras y circulares para visualizar los resultados por cada categoría. Además, se identificará la tendencia general respecto a la necesidad y aceptación de los servicios digitales cooperativos.

Cualitativos

Las respuestas de las entrevistas serán analizadas mediante análisis de contenido, agrupando las ideas principales por categorías temáticas. Se destacarán los comentarios más relevantes sobre la factibilidad, limitaciones y proyecciones del modelo cooperativo en ciberseguridad.

Integración de resultados

Los resultados cuantitativos y cualitativos serán integrados en un análisis conjunto, que permitirá contrastar la percepción de los actores con los datos duros recolectados. Esta integración brindará una comprensión más profunda sobre la viabilidad de crear una cooperativa de servicios digitales en ciberseguridad, orientada al sector EPS en Quito.

Capítulo 2

Diagnóstico Situacional Estratégico

En este capítulo serán presentado los hallazgos obtenidos a través de entrevistas y encuestas dirigidas a organizaciones de la EPS y profesionales del sector tecnológico especializado en ciberseguridad en la ciudad de Quito. El objetivo es comprender sus desafíos, necesidades y aspiraciones en el ámbito de la ciberseguridad, con el fin de diseñar un plan de negocios para una cooperativa de servicios digitales que sea funcional, sostenible y alineado con los principios de la economía popular y solidaria.

Metodologia y propósito

Las entrevistas cualitativas buscan captar tanto las experiencias y motivaciones de las organizaciones de EPS y profesionales expertos frente a los retos de la ciberseguridad donde abordan preguntas como:

¿Qué obstáculos enfrentan para proteger sus datos?

¿Qué los motiva a buscar soluciones accesibles?

permiten identificar no solo necesidades técnicas, sino también las aspiraciones de estos actores. Por su parte, las encuestas proporcionan datos cuantitativos sobre tendencias, como la frecuencia de incidentes de ciberseguridad y la demanda de servicios especializados, ofreciendo una base sólida para el diseño del modelo de negocio.

Tras la recolección de datos provenientes de encuestas y entrevistas, se llevó a cabo un análisis exhaustivo de las respuestas obtenidas, procesando la información y representándola

mediante tablas y gráficos claros y precisos. Las encuestas, dirigidas a cooperativas de ahorro y crédito, se diseñaron y distribuyeron utilizando la herramienta digital Google Forms, seleccionada por su versatilidad y capacidad para gestionar respuestas a gran escala. Este instrumento permitió captar las percepciones, necesidades y vulnerabilidades en ciberseguridad de estas organizaciones, que constituyen un pilar fundamental de la economía popular y solidaria. Paralelamente, se realizaron entrevistas estructuradas a profesionales y expertos en ciberseguridad, cuya experiencia enriqueció la comprensión de los riesgos digitales y las soluciones aplicables al contexto de las cooperativas.

El análisis consideró factores clave, como el nivel de exposición a amenazas cibernéticas, el grado de adopción de medidas de protección digital, el conocimiento técnico de los colaboradores y las necesidades específicas de seguridad en las operaciones financieras en línea. Los datos recopilados reflejan tanto las perspectivas de las cooperativas como los aportes especializados de los expertos, ofreciendo una visión integral de las demandas en ciberseguridad. Los resultados se presentan en tablas y gráficos que sintetizan la información obtenida de la muestra, facilitando su interpretación y uso estratégico.

Entrevistas a los Expertos y Líderes De Opinión

Con base en la metodología establecida, se diseñó un conjunto de preguntas (ver Anexo A: Entrevista a expertos) orientadas a profundizar en los aspectos clave de la creación y operación de una cooperativa de servicios digitales en ciberseguridad. Para ello, se aplicó la técnica de entrevistas estructuradas, realizadas a través de la plataforma Zoom, garantizando flexibilidad y accesibilidad para los participantes. La selección de los expertos se llevó a cabo considerando a dos profesionales con amplia trayectoria y reconocimiento en el campo de la

ciberseguridad, quienes son referentes en el ámbito de la protección digital y la gestión de riesgos tecnológicos, especialmente en el contexto de la economía popular y solidaria.

Entrevista al Msc. Luis Fernando Arias

Tabla 3

Datos del experto en ciberseguridad

Experiencia	5 años en ciberseguridad 10 años en Tecnología
Roles actuales	Docente de informática Coord. Seguridad Digital (Fundación Conexión Educativa)
Especialización	Auditorías de seguridad digital Creación de capacidades (capacitación)
Formación académica	Magíster en ciberseguridad

Nota. Datos del Autor

Pregunta 1

¿En su opinión qué tan necesario considera la adopción de servicios de ciberseguridad para pymes y organizaciones?

Desde mi experiencia, considero que la adopción de servicios de ciberseguridad es fundamental para las empresas y organizaciones, especialmente aquí en Quito, donde muchas empresas están digitalizándose sin contar con la protección adecuada. He visto cómo negocios pequeños se enfrentan a ataques que podrían haberse evitado con medidas básicas. La

ciberseguridad no solo protege datos, también brinda tranquilidad y fortalece la confianza con los clientes. Creo firmemente que no se trata de un gasto, sino de una inversión para asegurar la continuidad y el crecimiento del negocio. Hoy más que nunca, proteger la información es proteger el futuro de la empresa.

Pregunta 2

¿En su opinión cree usted que actualmente el mercado oferta suficientes servicios de ciberseguridad, y que sean asequibles para la protección de la información en pymes y organizaciones?

En mi opinión, actualmente el mercado no ofrece suficientes servicios de ciberseguridad que sean verdaderamente accesibles y adaptados a las necesidades de las empresas y organizaciones, especialmente en ciudades como grandes como Quito, Guayaquil. Muchos servicios están pensados para grandes empresas, con precios y soluciones fuera del alcance de negocios más pequeños. He notado que muchas microempresas no acceden a protección adecuada, no porque no la necesiten, sino porque no la pueden pagar o no saben por dónde empezar. Esto crea una brecha muy peligrosa en un mundo cada vez más digital. Creo que ahí existe una gran oportunidad para ofrecer servicios estos servicios de protección de datos personalizados y asequibles. La seguridad no debería ser un privilegio, sino un derecho para cualquier organización

Pregunta 3

¿Qué tipo de ataques cibernéticos considera que son los más frecuentes en Ecuador?

Según mi experiencia y después de 8 años de trabajar en las principales ciudades del Ecuador los ataques más frecuentes que he observado son el phishing (cuando se hacen pasar por empresas o personas), el robo de credenciales y el ransomware (virus que infecta sistemas y los secuestra). También son comunes los ataques a través de correos electrónicos falsos y malware (se usa para robar información personal) distribuido por descargas no seguras. Los negocios pequeños y microempresas suelen ser blanco fácil por falta de capacitación y controles básicos en seguridad digital generando pérdidas económicas y daño a la reputación de los negocios.

Pregunta 4

Según su experiencia, ¿cuáles son los riesgos de ciberseguridad más frecuentes que enfrentan las organizaciones y empresas que no salvaguardan su información digital?

Según mi experiencia, las organizaciones que no protegen adecuadamente su información digital enfrentan riesgos como el robo de datos sensibles, pérdidas económicas por fraudes o secuestro de información y la interrupción total de sus operaciones. También he visto casos en los que se pierde la confianza de los clientes, lo que afecta directamente la reputación de la empresa. Además, la falta de protección puede llevar a sanciones legales si se vulneran datos personales pero muchas empresas no son conscientes hasta que les sucede y ya es demasiado tarde.

Pregunta 5

Según su experiencia, ¿cuáles son las mayores barreras que impiden a las organizaciones y empresas implementar servicios de ciberseguridad?

Desde mi experiencia, las principales barreras son la falta de presupuesto y el desconocimiento sobre la importancia de la ciberseguridad. Muchas empresas ven la seguridad digital como un gasto, no como una inversión. También influye la escasa oferta de servicios accesibles y adaptados a pequeñas organizaciones. La falta de personal capacitado en el tema dentro de las empresas es otro obstáculo. Todo esto genera un obstáculo frente a los riesgos digitales que se encuentra en el día a día.

Pregunta 6

¿Cree usted que una red colaborativa de profesionales en ciberseguridad podría mejorar la capacidad de las organizaciones y empresas para mitigar riesgos digitales?

Sí, estoy convencido de que una red colaborativa de profesionales en ciberseguridad puede marcar una gran diferencia en la protección de las empresas y organizaciones frente a riesgos digitales. Este tipo de redes permitiría compartir conocimientos, experiencias y soluciones adaptadas a diferentes realidades, He palpado cómo el trabajo en conjunto fortalece las capacidades de respuesta y prevención más eficaz. Además, facilita el acceso a servicios más asequibles y personalizados. Creo que, al unir esfuerzos, se puede crear un ecosistema más seguro y solidario para todas las pequeñas empresas y organizaciones.

Pregunta *7*

¿Qué herramientas o programas recomendaría para proteger datos sensibles en una empresa u organización?

De acuerdo con los programas que yo utilizo personalmente y tomando en cuenta los datos sensibles a proteger recomendaría usar un buen antivirus empresarial como firewalls y herramientas de cifrado como BitLocker o VeraCrypt para proteger los datos. También es clave implementar autenticación de datos con el programa multifactor y respaldos automáticos con soluciones como Veeam o Acronis. Todos estos programas acompañados de políticas claras y capacitaciones al personal crearían un ambiente más profesional y seguro.

Entrevista al Ing. Ricardo Manuel Prieto Galarza

Tabla 4

Datos del experto en ciberseguridad

Experiencia	5 años en ciberseguridad 15 años en Tecnología 3 años en inteligencia artificial
Roles actuales	Eón corp. Desarrollador de software enfocado en inteligencia artificial
Especialización	Pruebas de ciberseguridad en cooperativas y entidades financieras. Pentesting avanzado en sistemas transaccionales
Formación académica	Ingeniero electrónico con especialización en ciberseguridad y telecomunicaciones.

Nota. Datos del Autor

Pregunta 1

¿En su opinión qué tan necesario considera la adopción de servicios de ciberseguridad para pymes y organizaciones?

Desde mi experiencia, considero fundamental la adopción de servicios de ciberseguridad. He trabajado intensamente resolviendo incidentes en este ámbito, especialmente en Pymes y organizaciones, que suelen ser las más vulnerables a ataques cibernéticos. Este riesgo es crítico si tomamos en cuenta que, a nivel económico, este sector representa la mayor parte de las entidades del país.

La falta de protección adecuada no solo expone a pérdidas financieras, sino también a daños reputacionales y operativos. Por ello, insisto en que invertir en ciberseguridad no es un gasto, sino una necesidad estratégica para garantizar la continuidad y confianza en los negocios.

Pregunta 2

¿En su opinión cree usted que actualmente el mercado oferta suficientes servicios de ciberseguridad, y que sean asequibles para la protección de la información en pymes y organizaciones?

Desde mi trayectoria en el mercado laboral, he observado que la oferta de servicios de ciberseguridad es insuficiente, principalmente por dos razones:

Es un servicio especializado y de alto costo, lo que limita su acceso.

Falta de planes de gestión de riesgos proactivos en las organizaciones.

Además, muchas empresas solo buscan estas soluciones *después* de sufrir un incidente, lo que evidencia un enfoque reactivo en lugar de preventivo. Para lograr una adopción masiva, es crucial:

Formar más profesionales especializados en ciberseguridad.

Fomentar una cultura de colaboración entre expertos y organizaciones.

Pregunta 3

¿Qué tipo de ataques cibernéticos considera que son los más frecuentes en Ecuador?

En mi experiencia laboral e identificado tres ciber amenazas críticas que afectan a las organizaciones:

Suplantación de identidad digital, técnica que permite la malversación de información confidencial que tiene como consecuencia directa estafas financieras con pérdidas económicas para víctimas u organizaciones.

El Phishing, es el engaño sistemático para obtener acceso ilegítimo a sistemas corporativos que da puerta de entrada a ataques más severos.

Ransomware, el más frecuente actualmente

Conlleva al secuestro de datos con exigencia de rescate, esto afecta operaciones y genera pérdidas de información y recursos.

Pregunta 4

Según su experiencia, ¿cuáles son los riesgos de ciberseguridad más frecuentes que enfrentan las organizaciones y empresas que no salvaguardan su información digital?

Desde mi experiencia directa en el campo, observo con preocupación que es alarmante comprobar cómo la mayoría de las personas y organizaciones operan sin planes de ciberseguridad ni protocolos para gestionar su información, ampliando su vulnerabilidad ante ataques. Lo más preocupante es que, incluso con advertencias y casos cercanos, persiste una actitud necia donde solo actúan tras sufrir un ataque y se resisten a invertir en protección o capacitación a sus colaboradores. Esta combinación de falta de prevención y escasa priorización genera un riesgo crítico a las organizaciones, en mi opinión debeos crear una cultura de cambio donde la ciberseguridad no debe verse como un gasto, sino como una inversión estratégica para la continuidad en el mercado laboral.

Pregunta 5

Según su experiencia, ¿cuáles son las mayores barreras que impiden a las organizaciones y empresas implementar servicios de ciberseguridad?

Desde mi perspectiva, identifico dos obstáculos clave en la adopción de servicios de ciberseguridad el primero, el factor económico junto con la subestimación del riesgo, donde muchos argumentan que sus negocios han operado sin incidentes graves por años y no prevén riesgos a futuro; y segundo, la naturaleza intangible del servicio, que dificulta su valoración y lleva a las organizaciones a minimizar su importancia hasta que sufren un ataque cibernético. Esta combinación de percepción de bajo riesgo y falta de visibilidad concreta resulta en una peligrosa postergación de medidas esenciales de protección ante cercanos ataques cibernéticos.

Pregunta 6

¿Cree usted que una red colaborativa de profesionales en ciberseguridad podría mejorar la capacidad de las organizaciones y empresas para mitigar riesgos digitales?

Efectivamente, la creación de una red colaborativa no solo es valiosa, sino imprescindible. Como profesional, he evidenciado que gran parte de mis contrataciones consisten en resolver inconsistencias dejadas por otros expertos, donde diferencias metodológicas o niveles de actualización técnica generan vulnerabilidades. Una cooperativa especializada permitiría estandarizar soluciones, combinando eficiencia con efectividad, y posicionarnos colectivamente para aspirar a contratos mayores, incluso con entidades gubernamentales que requieren metodologías unificadas. Más allá de la ventaja operativa, esta sinergia nos daría mayor visibilidad social y solidez institucional, demostrando que en ciberseguridad la unión multiplica nuestra capacidad de protección frente a trabajar de forma aislada. La formalización de esta organización representaría un salto cualitativo para el sector.

Pregunta 7

¿Qué herramientas o programas recomendaría para proteger datos sensibles en una empresa u organización?

Como primer paso fundamental, recomiendo realizar una evaluación detallada de la información crítica que maneja cada organización y sus necesidades específicas antes de implementar cualquier solución de ciberseguridad.

Mis recomendaciones técnicas indispensables serian:

- la implementación de un gestor de contraseñas seguro (baúl de claves)
- un antivirus premium con soporte local en Ecuador para garantizar respuesta ágil ante incidentes
- copias de seguridad cifradas con VeraCrypt (que ofrece cifrado militar para documentos sensibles)
- la migración a sistemas operativos Linux por su mayor seguridad inherente al ser software libre.

Estas medidas conforman una base sólida para proteger los activos digitales, aunque siempre deben adaptarse al contexto particular de cada entidad.

Procesamiento y Análisis de los Datos Cuantitativos

Aquí se presentan los resultados obtenidos a partir de la aplicación de la encuesta (ver anexo 2: encuestas), junto con la correspondiente tabulación de datos y los gráficos ilustrativos que facilitan su interpretación:

Pregunta 1

¿Qué tan prioritario es para su organización proteger sus datos financieros y los de sus clientes?

Tabla 5

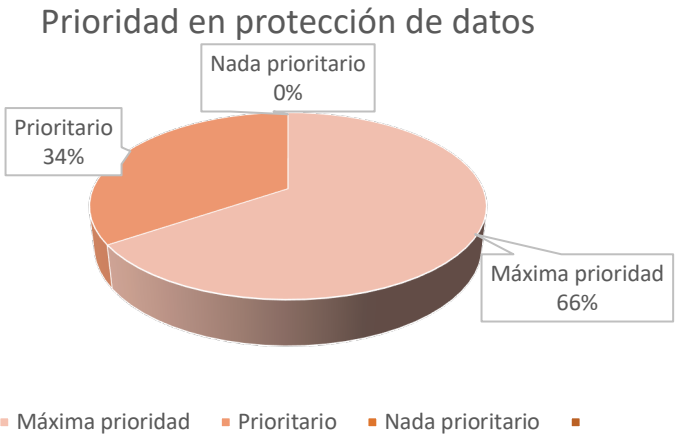
Prioridad en protección de datos

Respuestas	Valor	Porcentaje
Nada prioritario	0	0%
Prioritario	31	36,4%
Máxima prioridad	54	63,6%
Total	85	100%

Nota. Datos que se obtuvieron de las encuestas realizadas.

Ilustración 7

Porcentaje de prioridad en protección de datos



Nota. La alta prioridad asignada a la protección de datos financieros resalta la urgente necesidad de implementar medidas robustas de ciberseguridad en las cooperativas de ahorro y crédito.

Se puede concluir diciendo que los resultados obtenidos por las encuestas demuestran que el 63.6% de las organizaciones considera a la ciberseguridad como máxima prioridad y un 36.4% adicional la califica como prioritaria. Las cooperativas de ahorro y crédito consideran la ciberseguridad como un aspecto importante para garantizar la seguridad y sostenibilidad de sus operaciones.

Pregunta 2

¿Su organización ha sufrido algún tipo de ciberataque a la información interna, tales como robo de datos, phishing, etc. en los últimos 2 años?

Tabla 6

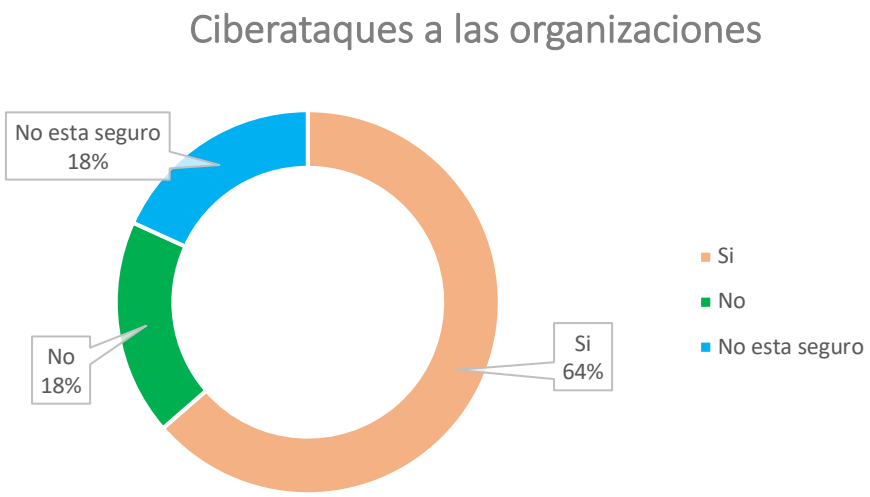
Ciberataques a las organizaciones

Respuestas	Valor	Porcentaje
Si	54	63,6%
No	15	18,2%
No está seguro	15	18,2%
Total	85	100%

Nota. Datos que se obtuvieron de las encuestas realizadas

Ilustración 8

Porcentajes de ciberataques



Nota. La tasa de ciberataques reportada de las cooperativas marca la vulnerabilidad crítica del sector y la necesidad urgente de implementar soluciones fuertes de ciberseguridad

Se puede concluir diciendo que los resultados obtenidos por medio de las encuestas muestran que la mayoría de las cooperativas han sufrido ciberataques, el 63.6% de las organizaciones indican que han sufrido ciberataques en los últimos 2 años, además un 18.2% desconoce si ha sido víctima de algún ciberataque y solo el 18.2% afirma no haber sido afectado, lo que resalta la urgencia de desarrollar soluciones especializadas y asequibles para proteger los datos financieros y garantizar la sostenibilidad operativa del sector cooperativo.

Pregunta 3

¿Su organización al momento cuenta con alguna herramienta digital de ciberseguridad para protegeré su información?

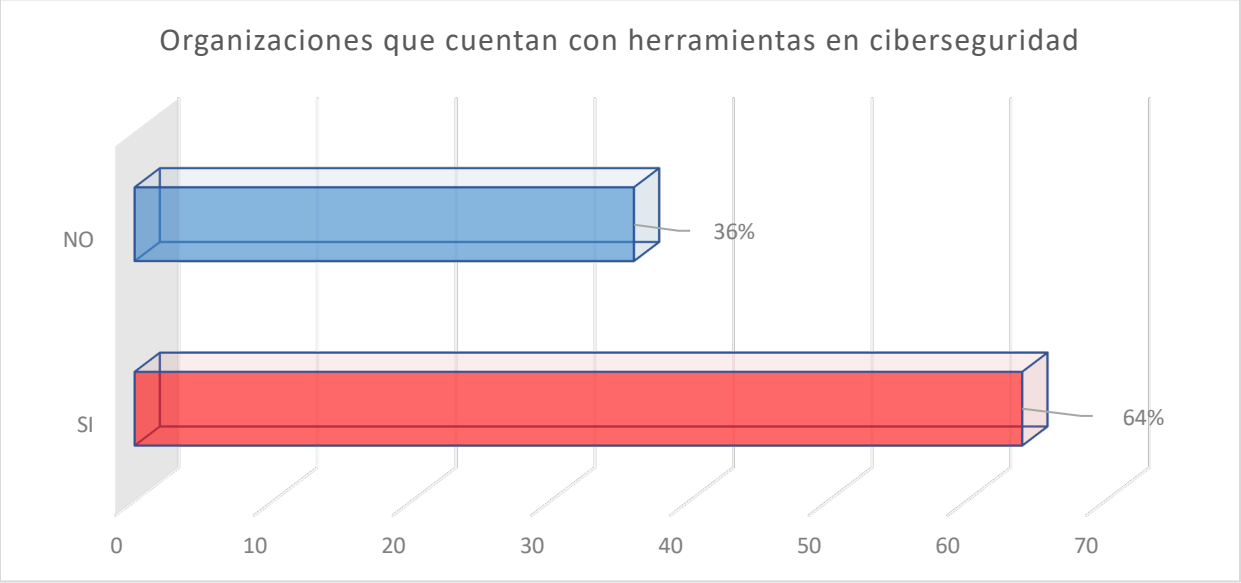
Tabla 7

Adopción de herramientas en ciberseguridad

Respuestas	Valor	Porcentaje
Si	54	64%
No	31	36%
Total	85	100%

Nota. Datos que se obtuvieron de las encuestas realizadas

Ilustración 9



Nota. Alarmante proporción de cooperativas sin herramientas digitales de ciberseguridad.

Conclusión. De acuerdo con los resultados obtenidos por las encuestas reflejan que, aunque el 64% de las organizaciones reporta contar con herramientas digitales de ciberseguridad, un preocupante 36% carece de ellas, tomando en cuenta que existe conciencia sobre la necesidad de seguridad digital, aún persisten obstáculos para su implementación total.

Pregunta 4

En el caso de ser negativa su respuesta anterior, ¿Considera usted que su organización estaría interesada en contar con los servicios de ciberseguridad?

Tabla 8

Adopción de servicio de ciberseguridad

Respuestas	Porcentaje
Si	100%
No	0%
Total	100%

Nota. Datos que se obtuvieron de las encuestas realizadas.

Ilustración 10

Interés en adoptar los servicios de ciberseguridad

Nota. Todas las organizaciones que no cuentan con este servicio estan dispuestas a adoptar servicios de ciberseguridad.

Conclusión. De acuerdo con los resultados obtenidos el 100% de las organizaciones encuestadas que no contaban con este servicio, manifestó el interés en contar con servicios de ciberseguridad para su organización.

Pregunta 5

¿Qué factor considera usted que sería decisivo para contratar un servicio de ciberseguridad?

Tabla 9

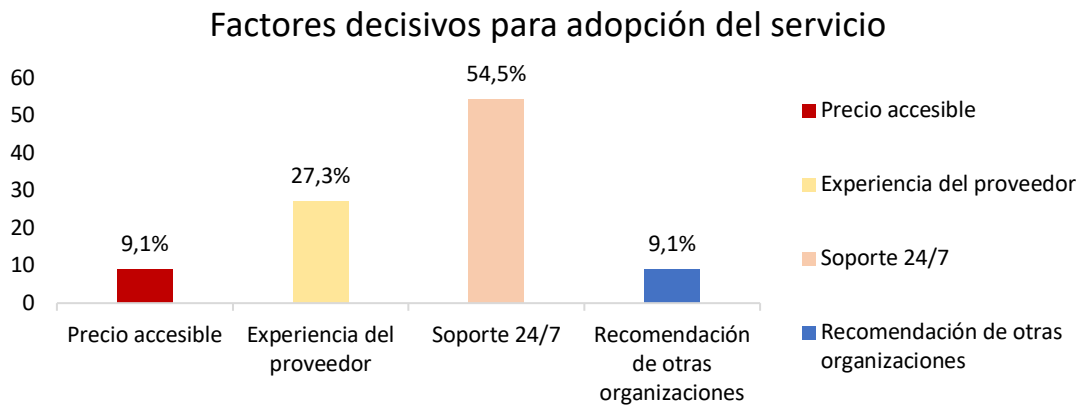
Factores decisivos para adopción del servicio

Respuestas	Valor	Porcentaje
Precio accesible	8	9,1%
Experiencia del proveedor	23	27.3%
Soporte 24/7	46	54,5%
Recomendación de otras organizaciones	8	9,1%
Otros (especifique)	0	0%
Total	85	100%

Nota. Datos que se obtuvieron de las encuestas realizadas.

Ilustración 11

Factores por los cuales contratarían los servicios de ciberseguridad



Nota. Mayor interés en adoptar un servicio con soporte permanente.

Conclusión. El análisis que revelan las encuestas realizadas indica que el soporte técnico 24/7 tiene un 54.5% y es el factor más determinante para contratar servicios de ciberseguridad, seguido de la experiencia del proveedor en un 27.3%, mientras que el precio accesible y las recomendaciones arrojan un 9.1% cada uno teniendo menor influencia a la hora de contratar el servicio de ciberseguridad.

Pregunta 6

¿Qué resultado considera más valioso en un servicio de ciberseguridad?

Tabla 10

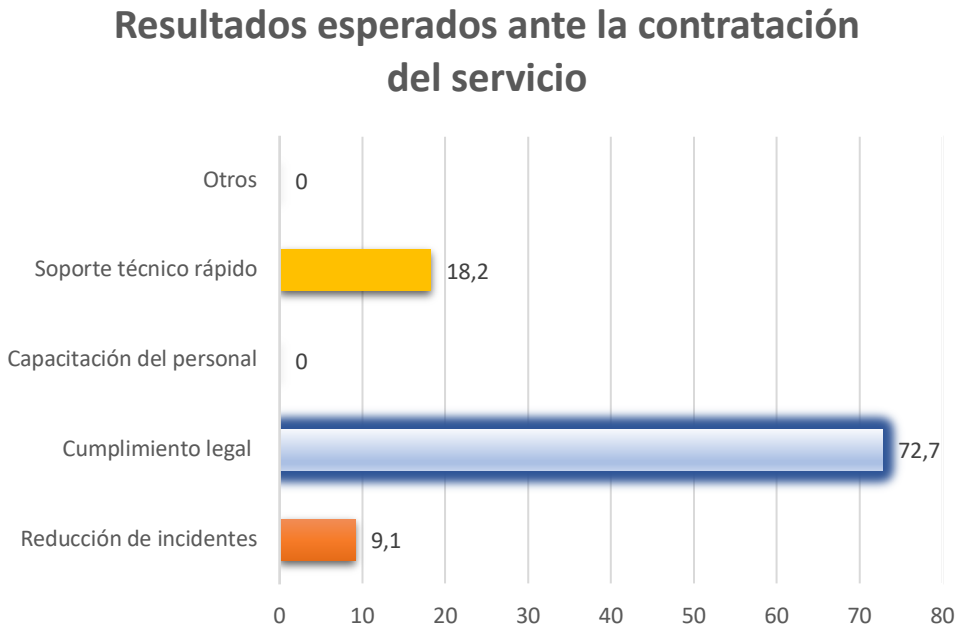
Resultados esperados ante la contratación del servicio

Respuestas	Valor	Porcentaje
Reducción de incidentes	8	9,1%
Cumplimiento legal (protección de datos)	62	72,7%
Capacitación del personal	0	0%
Soporte técnico rápido	15	18,2%
Otros (especifique)	0	0%
Total	85	100%

Nota. Datos que se obtuvieron de las encuestas realizadas.

Ilustración 12

Razones por las cuales contratarían los servicios de ciberseguridad



Nota. El embudo refleja que el cumplimiento legal es la mayor razón para contratar el servicio.

Conclusión. Los resultados obtenidos mediante las encuestas aplicadas priorizan claramente el cumplimiento legal y protección de datos en un 72.7% como el resultado más valioso, seguido del soporte técnico rápido con un 18.2%, mientras que la reducción de incidentes en un 9.1% tiene menor relevancia.

Pregunta 7

¿Qué tipo de servicios le interesaría contratar?

Tabla 11

Tipos de servicios que desean adquirir las cooperativas

Respuestas	Valor	Porcentaje
Auditorías de ciberseguridad	15	18,2%
Capacitación en ciberseguridad y protección de datos	8	9,1%
Protección de Infraestructuras Digitales	39	45,5%
Monitoreo y alertas en tiempo real	23	27,3%
Otros	0	0%
Total	85	100%

Nota. Datos que se obtuvieron de las encuestas realizadas.

Ilustración 13

Servicios que Oferta la Cooperativa

Nota. La marcada preferencia por la protección de bases de datos se destaca en la ilustración.

Conclusión. Los datos revelan que el servicio más demandado es la Protección de Infraestructuras Digitales.con un 45,5%, seguido del Monitoreo y alertas en tiempo real con un 27,3%, mientras que las auditorías de ciberseguridad un 18,2% y capacitación en ciberseguridad y protección de datos un 9,1% tienen menor preferencia.

Pregunta 8

¿Su personal ha recibido capacitación básica en ciberseguridad?

Tabla 12

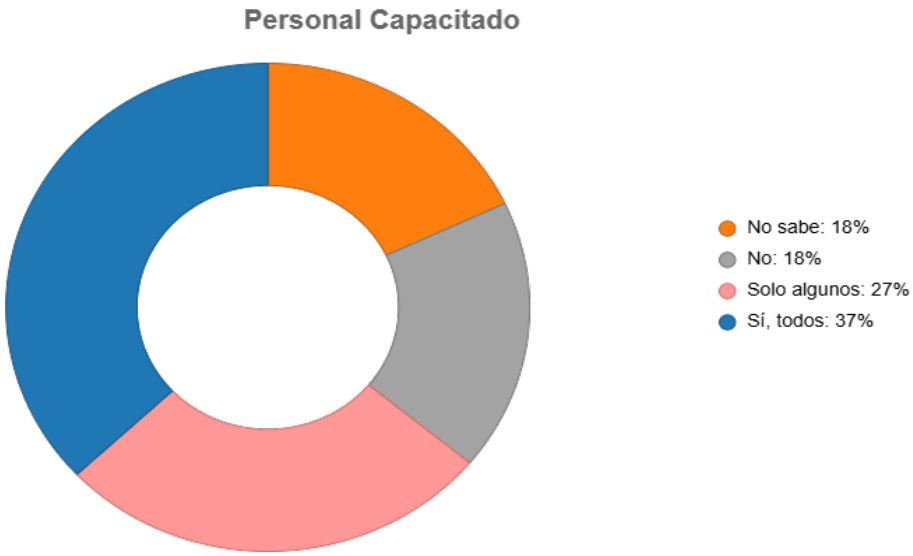
Personal capacitado en ciberseguridad

Respuestas	Valor	Porcentaje
Sí, todos	31	36,4%
Solo algunos	23	27,3%
No	15	18%
No sabe	16	18,3%
Total	85	100%

***Nota**:* Datos que se obtuvieron de las encuestas realizadas.

Ilustración 14

Porcentaje de personal capacitado en ciberseguridad de las organizaciones



Nota. La mayor parte de cooperativas no cuentan con personal capacitado en temas de ciberseguridad.

Conclusión. Los datos revelan que solo el 36,4% del personal ha recibido capacitación completa en ciberseguridad, mientras que el 27,3% indica capacitación parcial y un 18% admite no haberla impartido temas de ciberseguridad en su organización. Además, el 18,3% desconoce si existe dicha formación, evidenciando falencias críticas en la preparación contra amenazas digitales.

Pregunta 9

¿Qué tiempo de respuesta esperaría ante un incidente de seguridad?

Tabla 13

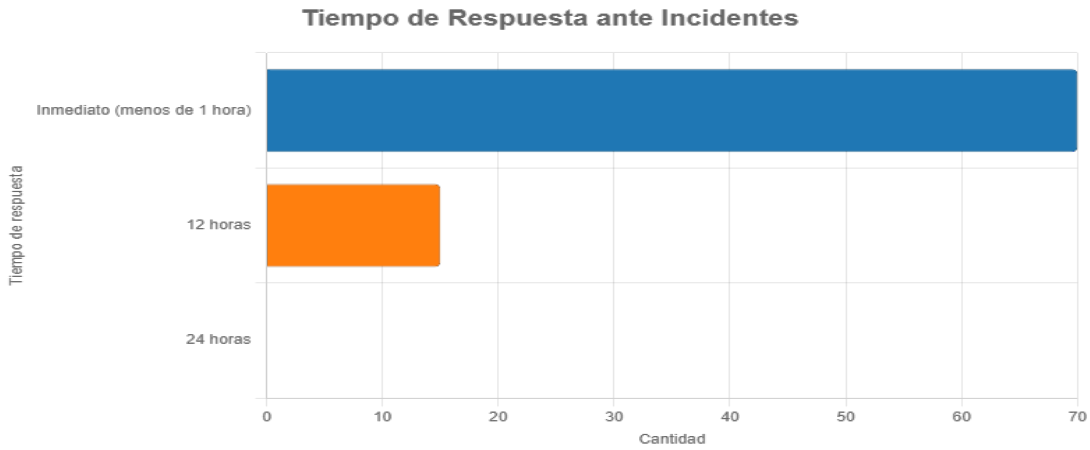
Tiempo de respuesta ante incidentes

Respuestas	Valor	Porcentaje
Inmediato (menos de 1 hora)	70	81,8%
12 horas	15	18,2%
24 horas	0	0%
Total	85	100%

Nota: Datos que se obtuvieron de las encuestas realizadas.

Ilustración 15

Tiempo de respuesta a incidentes



Nota. La acción inmediata ante incidentes cibernéticos resalta como la mayor opción esperada al contratar el servicio de ciberseguridad.

Conclusión. Los resultados obtenidos en las encuestas subrayan que el 81,8% de las organizaciones esperan un tiempo de respuesta inmediato ante un incidente de ciberseguridad, mientras que un 18,2% indican que esperarían un rango de tiempo de 12 horas máximo.

Pregunta 10

Considerando los servicios de ciberseguridad mencionados, ¿qué rango de inversión consideraría adecuado para su organización?

Tabla 14

Presupuesto destinado a la contratación del servicio

Respuestas	Valor	Porcentaje
Menos de $100	8	9,1%
$101 - $300	8	9,1%
$301 - $600	15	18,2%
$601 - $1,000	15	18,2%
Más de $1,000	23	27,3%
Prefiero un modelo de pago por servicio específico	16	18,2%

Total	85	100%

Nota: Datos que se obtuvieron de las encuestas realizadas.

Ilustración 16

Presupuesto a invertir en servicios de ciberseguridad

Nota. El rango de inversión es considerable para resguardar sus datos sensibles.

Conclusión. Los resultados de las encuestas a las cooperativas de ahorro y crédito indican que un 27,3% estan dispuestas a invertir en un servicio con un costo de más de 1000 dolares, mientras que un 18,2% prefieren un servicio especifico dependiendo la necesidad de la organización y menos de 9,1% buscan estos servicios con costos de menos de 110 dolares.

Pregunta 11

¿Prefiere un servicio de ciberseguridad con pagos:

Tabla 15

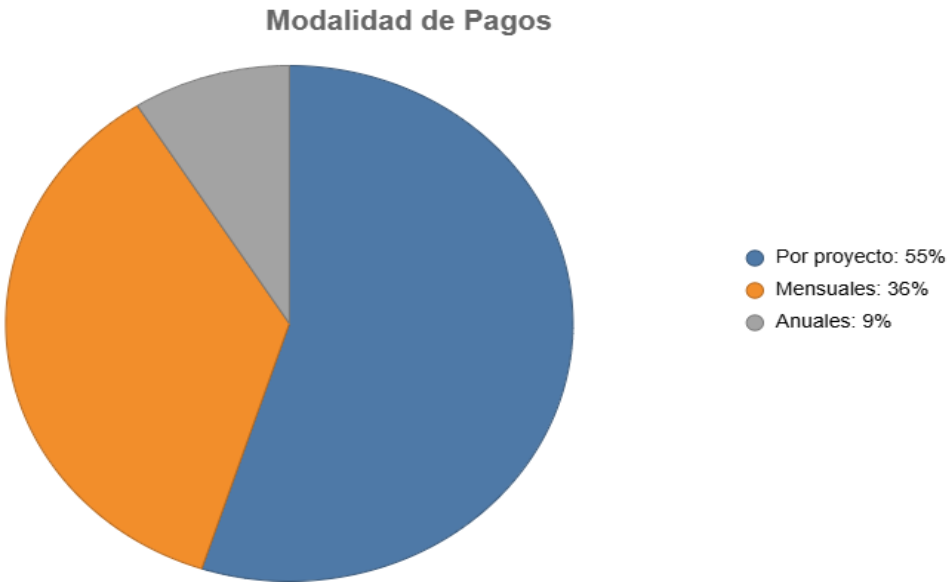
Modalidad de pago

Respuestas	Valor	Porcentaje
Mensuales	31	36,4%
Anuales	8	9,1%
Por proyecto	46	54,5%
Total	85	100%

Nota: Datos que se obtuvieron de las encuestas realizada

Ilustración 17

Preferencia de modalidad de pagos por el servicio



Nota. La ilustración muestra que la mayor parte de las organizaciones estan dispuestas a adoptar un servicio con cobros por proyecto o realizando un pago mensual.

Conclusión. De acuerdo con los resultados obtenidos un 55% de los encuestados señalan que contratarían el servicio de ciberseguridad por proyecto, mientras que un 36% indican que contratarían un servicio con pagos mensuales y un 9 % contratarían el servicio con pagos anuales.

Pregunta 12

¿Invertiría en un paquete de servicios que incluya monitoreo + capacitación por un costo mensual de $100-$200?

Tabla 16

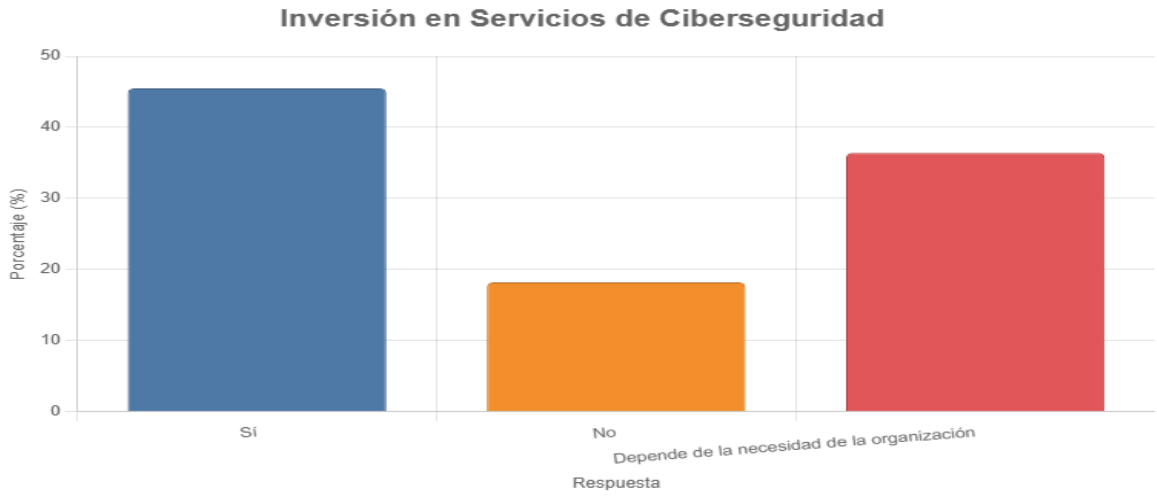
Inversión en servicios de ciberseguridad

Respuestas	Valor	Porcentaje
Si	39	45,5%
No	15	18,2%
Depende de la necesidad de la organización	31	36,4%
Total	85	100%

Nota. Datos que se obtuvieron de las encuestas realizadas.

Ilustración 18

Porcentaje de inversión actual en servicios de ciberseguridad



Nota. La mayoría de las organizaciones estan dispuestas a invertir en los servicios de ciberseguridad.

Conclusión. De acuerdo con los resultados obtenidos un 45,5% de los encuestados señalan que estarían dispuestos a invertir en un paquete de servicios que incluya monitoreo + capacitación por un costo mensual de $100-$200, mientras que un 36,4% señalan que evaluarían la necesidad de la organización y un 18,2% manifestaron que no estarían dispuestos a contratar el servicio por ese costo.

Conclusiones Generales En Diagnóstico Situacional

Los hallazgos derivados de las entrevistas a expertos y encuestas aplicadas a cooperativas de ahorro y crédito en Quito revelan un escenario crítico, pero con oportunidades estratégicas para la implementación del proyecto. Los datos cuantitativos muestran que el 63.6% de las organizaciones ha sido víctima de ciberataques en los últimos dos años, mientras que un 36% carece completamente de herramientas de protección digital, situación que los expertos califican como alarmante y urgente de atender.

En la investigación también se destaca una limitada comprensión por parte de las organizaciones sobre la importancia de la ciberseguridad, así como una deficiente valoración del trabajo realizado por los profesionales en este ámbito. Según los expertos entrevistados, esta falta de reconocimiento se debe, en parte, a la naturaleza intangible del servicio, lo que dificulta su apreciación y priorización en las organizaciones.

En el presente estudio se identificó tres necesidades prioritarias, el cumplimiento normativo, la protección de bases de datos y el monitoreo continuo. Sin embargo, se detecta una incertidumbre significativa donde se indica que mientras el 81.8% exige respuesta inmediata ante incidentes cibernéticos, solo el 9.1% valora las capacitaciones en temas de ciberseguridad, contradicción que según los expertos refleja una subestimación del servicio en seguridad digital.

Los obstáculos clave incluyen:

- Limitaciones presupuestarias (16%)
- Desconocimiento técnico (14%)
- Percepción de bajo riesgo (mencionado en ambas entrevistas)

No obstante, los resultados son alentadores para implementar el modelo cooperativo de ciberseguridad en sus organizaciones:

54.5% de las organizaciones encuestadas prefiere esquemas de pago por proyecto.

45.5% de las organizaciones encuestadas dicen que contrataría paquetes integrados de monitoreo o capacitación en ciberseguridad.

27.3% de las organizaciones encuestadas están dispuestas a invertiría más de $1000 en este servicio.

Cabe recalcar que en las entrevistas los expertos coinciden en que una red colaborativa podría facilitar el acceso total a todas estas organizaciones que estan dispuestas a proteger sus datos y los de sus clientes, entendiendo que este servicio puede prevenir perdidas futuras de recursos y garantizar la reputación de las organizaciones.

Los expertos enfatizan que este modelo permitiría transformar la percepción actual de la ciberseguridad vista como gasto por el 16% de las organizaciones encuestadas hacia una visión de inversión estratégica. Esta perspectiva se alinea perfectamente con los hallazgos cuantitativos donde el 100% de las organizaciones sin protección actual manifestó interés en contratar servicios, particularmente si se ofrecen bajo modalidades flexibles.

Este diagnóstico sustenta la viabilidad de una cooperativa de servicios tecnológicos en ciberseguridad donde mediante principios de economía solidaria y valores organizacionales, Al unir esfuerzos, se puede crear un ecosistema más seguro y solidario donde se puedan cerrar las brechas identificadas en la investigación, mientras se fomenta una cultura y se concientiza la necesidad de poseer los servicios de seguridad digital en todo el sector de EPS.

Capítulo 3

Propuesta

A continuación, la propuesta que se plantea no es solo un modelo de negocios, si no una correcta iniciativa de desarrollo tanto cooperativo como tecnológico. Con esta propuesta, se pretende transformar las aspiraciones de seguridad digital en realidades tangibles, superando las barreras de acceso a servicios especializados y abriendo caminos hacia un futuro digital seguro, inclusivo y sostenible para las organizaciones de Quito.

Filosofía Empresarial

A continuación, se presenta la filosofía empresarial de la Cooperativa de servicios digitales en ciberseguridad AI Cybersecurity.

Misión

Somos una cooperativa que se dedica a proporcionar servicios digitales de ciberseguridad enfocados en salva guardar la información y activos digitales de las organizaciones. Promovemos un ecosistema digital confiable con una propuesta cooperativa, innovador y sostenible en el tiempo para nuestros socios y clientes.

Visión

Ser la cooperativa líder en servicios digitales de ciberseguridad en 2030, comprometidos con la innovación y la transformación digital segura, reconocidos por la contribución a un ecosistema tecnológico equitativo, resiliente y confiable.

Valores Corporativos:

Colaboración

Fomentar el trabajo en equipo para proteger y fortalecer a la comunidad.

Innovación

Integrar tecnología avanzada para soluciones de ciberseguridad efectivas.

Confianza

Garantizar transparencia y seguridad en cada servicio que ofrecemos.

Accesibilidad

Brindar soluciones inclusivas para organizaciones de todos los segmentos.

Compromiso

Priorizar la protección de datos y el bienestar de nuestros clientes.

Capacitación

Promover el aprendizaje continuo para una cultura de resiliencia digital.

Políticas

Administrativas

Gestión Transparente de Recursos Humanos

Garantizar una administración ética y eficiente del personal, promoviendo equidad y desarrollo profesional.

Acciones clave:

- Implementar procesos de contratación inclusivos y transparentes.
- Establecer evaluaciones de desempeño semestrales con retroalimentación.
- Ofrecer planes de capacitación anuales en ciberseguridad y liderazgo.

Cumplimiento Normativo y Gobernanza

Revisar que todas las operaciones cumplan con las regulaciones locales y los principios cooperativos.

Acciones clave:

- Crear un comité de gobernanza para supervisar el cumplimiento de la Ley de Cooperativas del Ecuador.
- Realizar auditorías internas trimestrales de procesos administrativos.
- Documentar todas las decisiones en actas accesibles para los socios.

Políticas de Mercadotecnia

Estrategia de Posicionamiento

Promover la visibilidad de la cooperativa como líder en ciberseguridad accesible en Quito.

Acciones clave:

- Diseñar campañas digitales enfocadas en la importancia de la ciberseguridad.
- Participar en eventos locales de tecnología y cooperativismo para networking.
- Crear contenido educativo gratuito para atraer clientes.

Segmentación y Personalización de Servicios

Adaptar las estrategias de marketing a las necesidades específicas de cooperativas, pymes y organizaciones.

Acciones clave:

- Realizar estudios de mercado anuales para identificar necesidades específicas.
- Ofrecer paquetes promocionales personalizados según el segmento y sector de la organización.
- Utilizar herramientas con inteligencia artificial para seguimiento personalizado de clientes.

Políticas de Producción y Servicios

Calidad y Estandarización de Servicios

Garantiza que los servicios de ciberseguridad sean consistentes, confiables y de alta calidad.

Acciones clave:

- Implementar protocolos estandarizados para auditorías, monitoreo y respuesta a incidentes.
- Integrar herramientas de IA para optimizar la detección de amenazas.
- Realizar revisiones de calidad trimestrales para evaluar la satisfacción del cliente.

Innovación Continua en Servicios

Promover el desarrollo y mejora constante de soluciones de ciberseguridad mediante tecnología innovadora.

Acciones clave:

- Recopilar retroalimentación de clientes para mejorar servicios trimestrales.
- Colaborar con organizaciones para investigar nuevas tecnologías de ciberseguridad.

Políticas Financieras

Gestión de Recursos

Asegurar la sostenibilidad financiera mediante una administración eficiente y transparente.

Acciones clave:

- Elaborar presupuestos anuales aprobados por los socios.
- Crear un fondo de emergencia con activos digitales que se revaloricen con el tiempo.
- Publicar informes financieros trimestrales para los socios con el fin de fomentar la tranquilidad de su inversión.

Acceso a Financiamiento

Facilita el acceso a recursos financieros para apoyar a clientes y la propia cooperativa.

- Buscar subsidios gubernamentales o capitales semilla para proyectos de ciberseguridad comunitaria.
- Establecer alianzas con instituciones financieras para ofrecer planes de pago flexibles a clientes.

Protección de Datos y Privacidad

Garantizar la confidencialidad, integridad y disponibilidad de los datos de clientes y socios, cumpliendo con la Ley Orgánica de Protección de Datos Personales del Ecuador.

Acciones clave:

- Implementar cifrado de datos en tránsito y en reposo.

- Realizar auditorías periódicas de cumplimiento normativo.
- Designar un oficial de protección de datos.

Política de Respuesta Rápida a Incidentes de Ciberseguridad

Establecer procedimientos para identificar, responder y mitigar incidentes cibernéticos en tiempo real.

Acciones clave:

- Crear un equipo de respuesta a incidentes disponible 24/7.
- Notificar a clientes dentro de las 24 horas posteriores a un incidente.
- Usar herramientas de IA para detección y respuesta automatizada.

Política de Capacitación Continua en Ciberseguridad

Promover la formación regular de empleados y clientes para prevenir riesgos cibernéticos.

Acciones clave:

- Ofrecer talleres trimestrales sobre phishing, contraseñas seguras y normativas.
- Desarrollar certificaciones internas para el personal.
- Proveer recursos educativos gratuitos para organizaciones sobre baúles de contraseñas.

Política de Innovación

Regular el uso ético y transparente de herramientas de IA en los servicios de ciberseguridad.

Acciones clave:

- Documentar y auditar procesos de IA para garantizar transparencia.
- Capacitar al personal en el uso responsable de IA.

Política de Inclusión

Verificar que los servicios sean accesibles para organizaciones de todos los segmentos, promoviendo la equidad.

Acciones clave:

- Diseñar paquetes de servicios asequibles para pymes y organizaciones.
- Incluir personal diverso en la toma de decisiones de la cooperativa.

Política de Colaboración y Alianzas Estratégicas

Fomentar alianzas con actores clave para fortalecer la infraestructura y credibilidad de la cooperativa.

Acciones clave:

- Establecer acuerdos con universidades y organizaciones tecnológicas para promover conciencia en los servicios de ciberseguridad.
- Crear redes de intercambio de conocimientos en temas de seguridad digital.

Objetivos

Objetivos a Corto Plazo

1. Cubrir los costos totales de operaciones.

S	Cubrir costos de operaciones
M	Incrementar la venta de servicios en un 20%
A	El incremento de ventas aumenta la liquidez de la organización, al obtener mejores recursos podemos gestionar mejor los procesos.
R	Avanzar en el desarrollo de la organización.
T	1 Año

2. Identificar los requerimientos del sector Cooperativo realizando visitas de campo a potenciales clientes.

S	Identificar los requerimientos del sector Cooperativo

M	Realizar visitas de campo a 10 potenciales clientes
A	El crecimiento en el sector cooperativos y la creciente tecnología induce a tener mejores servicios asociados con la ciberseguridad para protección de datos
R	Permite desarrollar productos y servicios según las necesidades de los clientes
T	6 Meses Del 10 de enero al 10 de julio del 2026

3.Reducir los tiempos de respuesta ante ataques cibernéticos y amenazas.

S	Reducir los tiempos de respuesta ante ataques cibernéticos
M	Optimizar el tiempo de respuesta ante amenazas en un 15%
A	Mejorar la infra estructura y equipos tecnológicos para una mejor protección de datos de nuestros clientes.
R	Es clave para mejorar la satisfacción del cliente y fortalecer la reputación de la organización en un mercado bastante amplio.
T	1 año Inicio 15 de Marzo 2025 Fin 15 de marzo 2026

Objetivos a Mediano Plazo

1. Ensayar un servicio piloto de detección de amenazas con inteligencia artificial para clientes potenciales que requieran asistencia 24/7.

S	Detección de amenazas con inteligencia artificial
M	Lograr 95% de detección en pruebas y 4 clientes satisfechos.
A	Usar recursos de IA y equipo de soporte
R	Fortalecer oferta de ciberseguridad y responder a demanda de asistencia continua.
T	Finalizar en 6 meses

2. Automatizar procesos operativos y administrativos con herramientas digitales para un servicio más eficiente y profesional.

S	Automatizar procesos operativos y administrativos
M	Automatizar el 80% de los procesos administrativos y operativos
A	La mejora de servicios y la satisfacción del cliente crecerían notablemente con un sistema más rapido y eficiente.
R	La automatización permitirá mejorar la eficiencia operativa y reducir costos.
T	1 años

3. Capacitación masiva a todos socios en actualizaciones de software y sistemas operativos con certificaciones internacionales.

S	Capacitar a todos los socios en actualizaciones de software y sistemas operativos con certificaciones internacionales.
M	Capacitar a los socios en actualización de software y sistemas operativos 3 veces al año.
A	Debido a los avances tecnológicos es necesario actualizar los conocimientos regularmente.
R	las capacitaciones en actualizaciones tecnológicas ayudan a actualizar conocimientos, optimizar los recursos y mejorar los servicios prestados.
T	15 meses

Objetivos a Largo Plazo

1. Posicionar a la cooperativa como líder en servicios de ciberseguridad para organizaciones en Ecuador, expandiendo operaciones a Guayaquil y Cuenca.

S	Posicionar la cooperativa como líder en ciberseguridad

M	Captar 10 nuevos clientes en cada ciudad y lograr un 20% de reconocimiento de marca en el sector.
A	Captar 10 nuevos clientes en cada ciudad y lograr un 20% de reconocimiento de marca en el sector.
R	Fortalecer la presencia en el mercado de ciberseguridad, respondiendo a la creciente demanda de protección digital.
T	3 años

2. Evaluar la satisfacción del cliente con respecto a la eficacia del servicio.

S	Evaluar la satisfacción del cliente con respecto a la eficacia del Servicio
M	Realizar simulacros de ataques cibernéticos 2 veces al año.
A	Recibir feeck back del cliente para encontrar mejoras del Servicio.
R	La satisfacción del cliente permite identificar las áreas de mejora y brindar un mejor servicio, con el fin de aumentar la retención y fidelización de clientes
T	15 meses

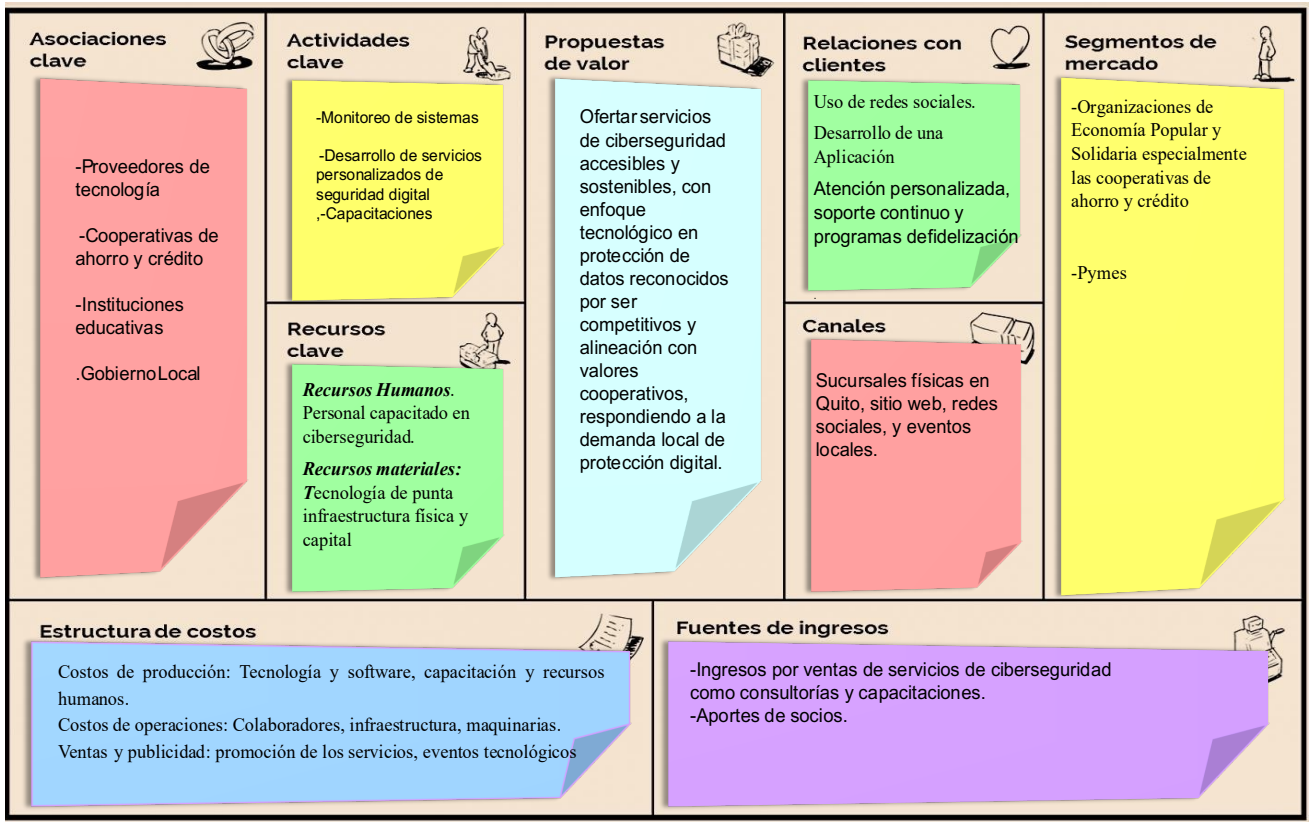
3. Participar en proyectos de ciberseguridad con ministerios o instituciones del Estado.

S	Participar en al menos 3 proyectos de ciberseguridad con ministerios o instituciones estatales en Ecuador.
M	Firmar 3 contratos con instituciones públicas y lograr un 90% de cumplimiento en los entregables.
A	Utilizar experiencia existente en ciberseguridad y contactos institucionales para licitar proyectos viables.
R	Fortalecer la reputación de la cooperativa y contribuir a la seguridad digital del sector público.
T	2 años

Modelo Canvas

Ilustración 19

Modelo canvas de la cooperativa AI Cibersecurity



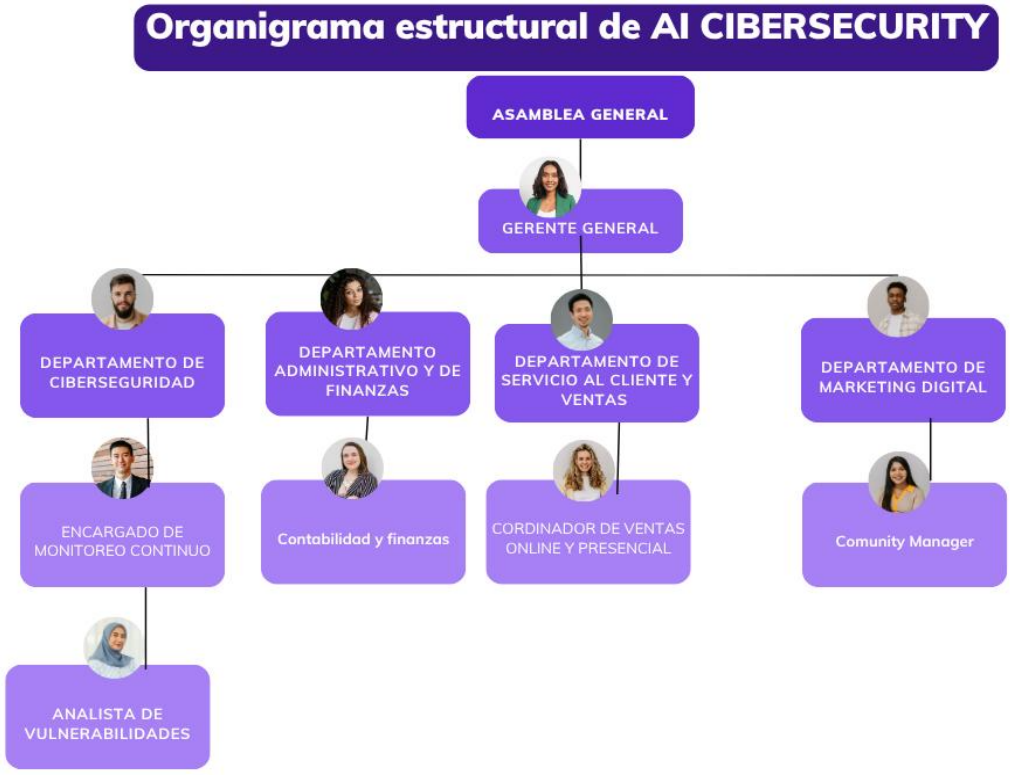
Nota. Estructura clave del modelo de negocios de la cooperativa AI Cibersecurity.

Organigramas

Organigrama Estructural

Ilustración 20

Estructura organizacional

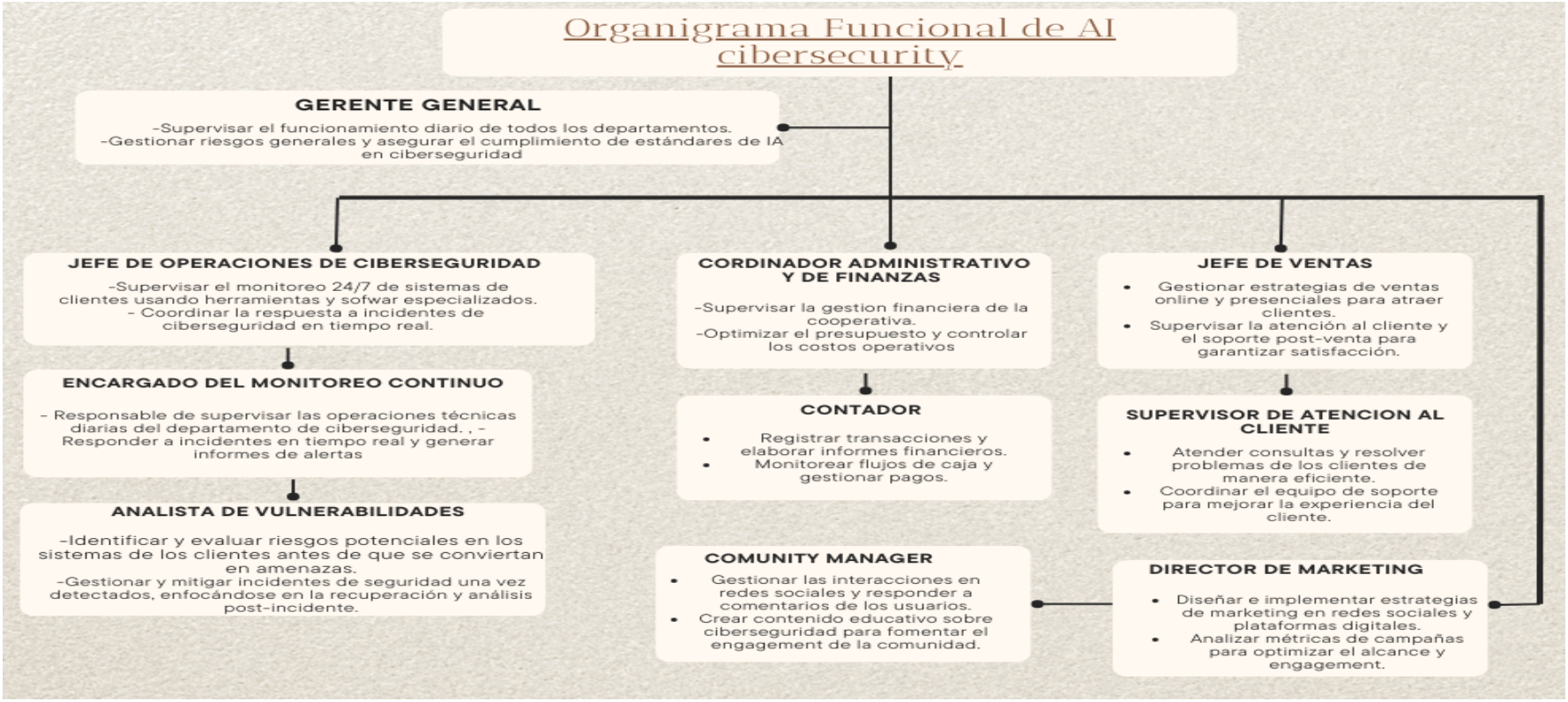


Nota. Organigrama esencial para el buen funcionamiento de la cooperativa AI Cibersecurity.

Organigrama Funcional

Ilustración 21

Funciones establecida de acuerdo con el rol que desempeñan



Nota. Funciones que desempeñara cada colaborador de la cooperativa.

Matriz FODA

Tabla 17

Análisis Estratégico FODA de AI Cibersecurity

Matriz FODA			
Organización		Cooperativa de servicios tecnológicos en ciberseguridad AI Cibersecurity	
Fortalezas		Debilidades	
F1	Innovación	D1	Recursos limitados
F2	fácil accesibilidad	D2	Servicios intangibles
F3	Modelo cooperativo	D3	Falta de experiencia
F4	Marco jurídico	D4	Grandes competencias
F5	Nuevas tecnologías	D5	Reto para atraer nuevos socios con conocimientos
Oportunidades		Amenazas	
O1	Ataques cibernéticos a organizaciones	A1	Leyes regulatorias cambiantes
O2	Acceso a Capital semilla	A2	Rápidos avances tecnológicos
O3	Alianzas estratégicas	A3	Inseguridad
O4	Mercado desatendido	A4	Situación del pais inestable
O5	Crecimiento del sector de la EPS	A5	Guerras

Nota: Identificación de factores clave para la viabilidad de la organización AI cibersecurity.

Conclusión. La presente matriz FODA permite visualizar los factores como fortalezas y oportunidades a ser aprovechados y también se visualizan las amenazas y debilidades a las que se enfrenta la organización para poder trascender en el tiempo.

Matriz EFE

Tabla 18

Factores externos, oportunidades y amenazas

Matriz (EFE)				
Factores externos claves del éxito		**Peso actividad**	**Valor/ Calificación**	**Peso Ponderado**
	Oportunidades			
1	Ataques cibernéticos a organizaciones	0,25	4	1,00
2	Acceso a Capital semilla	0,15	3	0,45
3	Alianzas estratégicas	0,15	3	0,45
4	Mercado desatendido	0,15	3	0,45
5	Crecimiento del sector de la EPS	0,10	3	0,30
Amenazas				
1	Leyes regulatorias cambiantes	0,10	2	0,20
2	Rápidos avances tecnológicos	0,10	2	0,20
3	Inseguridad	0,05	2	0,10
4	Situación del pais inestable	0,05	2	0,10
5	Guerras	0,05	1	0,05
	Total	**1,00**		**2,95**

NOTA. La matriz EFE, nos muestra la ponderación obtenida, indicando la viabilidad del plan de negocios.

Interpretación del factor resultante, Con el valor obtenido de 2,95, el entorno externo muestra oportunidades importantes, especialmente en el crecimiento de frecuentes ataques cibernéticos y acceso a capital semilla, aunque existen rápidos avances tecnológicos y la situación de país inestable.

Matriz EFI

Tabla 19

Factores internos, fortalezas y debilidades

Matriz (EFI)				
Factores externos claves del éxito		**Peso actividad**	**Valor/ Calificación**	**Peso Ponderado**
	Fortalezas			
1	Innovación	0,25	4	1,00
2	Fácil Accesibilidad	0,20	3	0,60
3	Modelo cooperativo	0,15	3	0,45
4	Marco jurídico	0,15	3	0,45
5	Nuevas tecnologías	0,1	3	0,30
Debilidades				
1	Recursos limitados	0,15	2	0,30
2	Servicios intangibles	0,05	2	0,10
3	Falta de experiencia	0,05	2	0,10
4	Grandes competencias	0,05	2	0,10
5	Reto para atraer nuevos socios con conocimientos	0,05	2	0,10
	Total	**1,00**		**3,00**

Nota. La presente matriz nos muestra la ponderación obtenida, indicando la viabilidad del plan de negocios.

Interpretación del factor resultante Con el resultado obtenido de 3, AI cibersecurity muestra una base interna sólida, con fortalezas clave la fácil accesibilidad y la innovación, son los factores más destacados y notorios ante las fuertes amenazas como recursos limitados que con la reputación adquirida se podría mitigar y con un buen marketing se aumentara la visibilidad de los servicios que ofrece la cooperativa.

MATRIZ DAFO

Tabla 20

Matriz de estrategias DAFO

Matriz DAFO		Fortalezas		Debilidades	
Organización		F1	Innovación	D1	Recursos limitados
Cooperativa de servicios tecnológicos AI SEGURITY		F2	Fácil accesibilidad	D2	Servicios intangibles
		F3	Modelo cooperativo	D3	Falta de experiencia
		F4	Marco Jurídico	D4	Grandes competencias
Oportunidades		F5	Nuevas tecnologías	D5	Reto para atraer nuevos socios con conocimientos
O1	Ataques cibernéticos a organizaciones	Estrategias FO		Estrategias DO	
O2	Acceso a Capital semilla	F1 O1	Adoptar Inteligencia artificial para crear soluciones automatizadas y eficientes ante la creciente necesidad de protección datos.	D1O2	Buscar activamente financiamiento a través de programas de capital semilla para superar las limitaciones de recursos iniciales.
O3	Alianzas estratégicas				
O4	Mercado desatendido				
O5	Crecimiento del sector de la EPS	F1 O4	Ofrecer servicios de ciberseguridad asequibles y fáciles de implementar para organizaciones de todos los segmentos.	D2O4	Desarrollar campañas educativas para demostrar la importancia de los servicios de ciberseguridad a las organizaciones, aumentando su aceptación.
Amenazas					
A1	Leyes regulatorias cambiantes				

A2	Rápidos avances tecnológicos	F3 O3	Establecer alianzas con cooperativas e instituciones tecnológicas para fortalecer la red colaborativa y expandir el alcance.		
A3	Inseguridad			D505	Realizar investigaciones de mercado y talleres con actores de la EPS para entender y atender sus necesidades específicas.
A4	Situación del pais inestable				
A5	Guerras	Estrategias FA		Estrategias DA	
		F3A1	Crear servicios especializados para el cumplimiento normativo en protección de datos.	D2A1	Desarrollar materiales educativos y casos de éxito para destacar la importancia de la ciberseguridad,
				D3A2	Trabajar con proveedores expertos en tecnologías cambiantes.
		F2A4	Ofrecer servicios accesibles ajustándonos al entorno económico y social.	D3A3	Enfocarse en nichos de mercado específicos para evitar competencia directa con grandes empresas
		F1A2	Mantenerse en constante capacitación para actualizar continuamente conocimientos, contrarrestando as los rápidos cambios tecnológicos.		

Nota. La presente matriz convierte el análisis FODA en estrategias concretas para fortalecer la viabilidad del plan de negocios.

Nota importante: La matriz DAFO transforma el diagnóstico estratégico en acciones concretas, combinando fortalezas y oportunidades para potenciar el crecimiento de la organización. Además, propone estrategias para minimizar riesgos y superar debilidades, asegurando un desarrollo sostenible y mayor impacto en el ecosistema cibernético de Quito.

Plan de Servicios

La cooperativa ofrecerá servicios tecnológicos especializados en ciberseguridad uno de estos servicios son la consultoría para las organizaciones sobre ciberseguridad.

Servicios de Consultoría en Ciberseguridad

1. Asesoramiento en la Implementación de Estrategias de Ciberseguridad para las organizaciones.

Objetivo:

Proporcionar información correcta para diseñar, implementar y optimizar estrategias de ciberseguridad adaptadas a las necesidades específicas de las organizaciones, con el fin de proteger sus datos y activos digitales.

Descripción del servicio

Evaluación del Estado Actual de servicios (si lo tiene): Revisión de la infraestructura tecnológica, políticas de seguridad existentes y nivel de seguridad que requiere la organización.

Identificación de Objetivos: Definición de los objetivos de seguridad de la Organización (protección de datos, cumplimiento normativo, prevención de ataques).

Priorización de Iniciativas: Identificación de las áreas críticas que requieren atención inmediata (protección de datos, seguridad en la nube, gestión de accesos).

Plan de Implementación: Creación de un cronograma detallado con fases, responsables y recursos necesarios.

Especificaciones del servicio

Selección de Herramientas y Tecnologías: Recomendación de software y hardware adecuados (firewalls, sistemas de detección de intrusiones, antivirus).

Configuración de Sistemas: Asistencia en la configuración segura de redes, servidores, bases de datos y aplicaciones.

Integración de Soluciones: Asegurar que las nuevas herramientas se integren correctamente con los sistemas existentes o nuevos sistemas adquiridos.

Capacitación y Concientización:

Formación del Personal: Capacitación a empleados y equipos técnicos en el uso de nuevas herramientas y prácticas de seguridad.

Cultura de Seguridad: Promoción de una mentalidad proactiva hacia la ciberseguridad en todos los niveles de la organización.

Monitoreo y Mejora Continua:

Evaluación Periódica: Revisión regular de la estrategia para identificar áreas de mejora, realizando simulacros y recibiendo feed back del cliente.

Actualización de Políticas: Ajuste de políticas y procedimientos en función de cambios en el entorno tecnológico o normativo.

Costo por el servicio: 800$

Informes de Progreso: Generación de informes detallados para la alta dirección, mostrando el avance y el ROI de las iniciativas de seguridad.

Ilustración 22

Precio del servicio de consultoría

Nota. Datos del autor

Tabla 21

Ficha de procesos

Nombre del proceso:	**Servicios de Consultoría en Ciberseguridad**	
Entradas:	**Interesados en el servicio de consultoría**	
Salidas:	**Ingreso de documentación aprobada de nuevos socios**	
	Computador	
Recursos:	**Sistemas de software**	
	Dispositivos de almacenamiento	
	Jefe de ciberseguridad	
	Oficial de ciberseguridad	
Responsables:	**Jefe de ventas**	
	Analista de riesgos	
	Jefe de ciberseguridad	
Actividad	**Descripción**	**Responsable**
Solicitar Información sobre el servicio	**El cliente se contacta para solicitar el servicio**	**Cliente, jefe de Ventas**

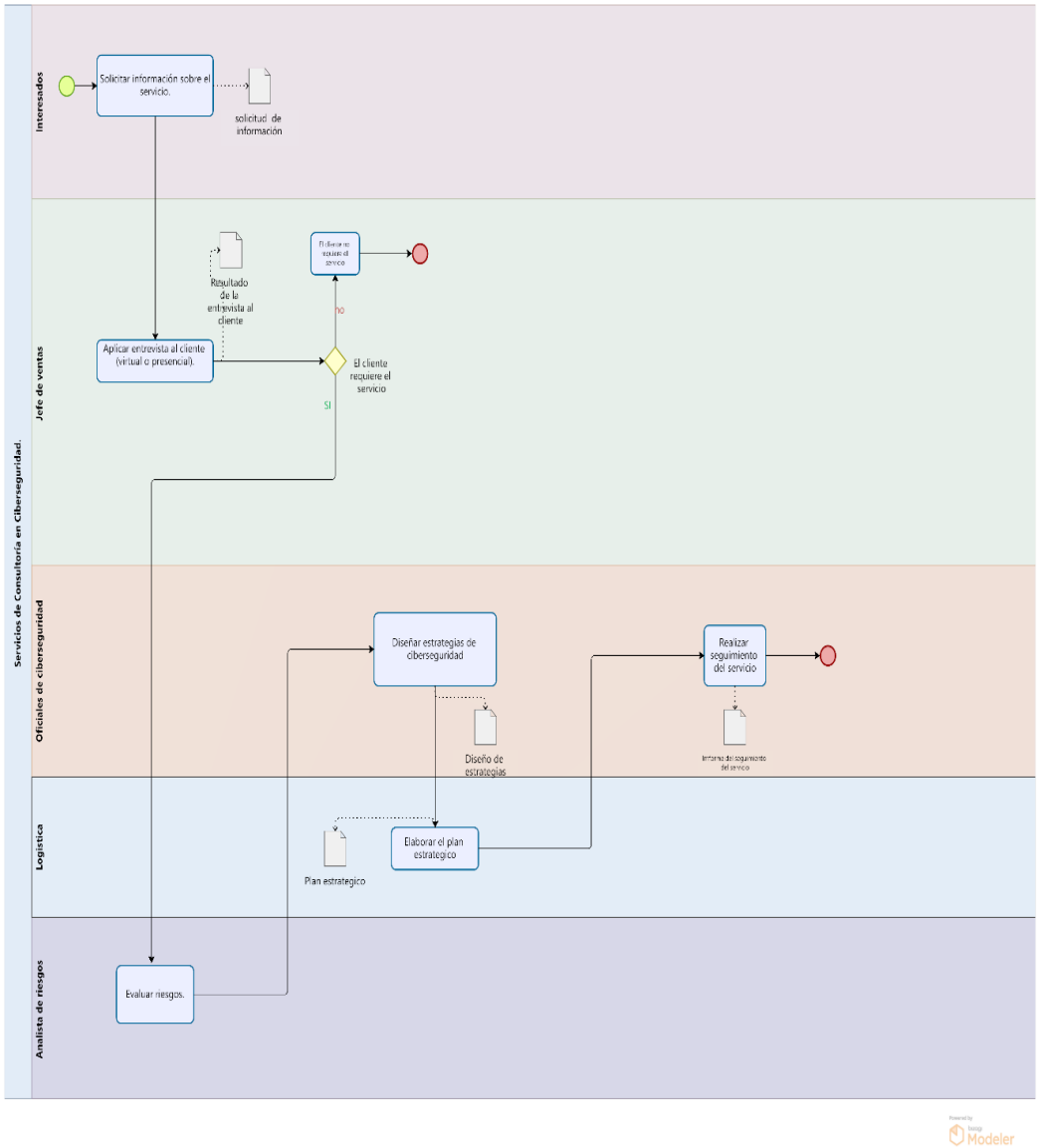
Reunión con el cliente	**Reunión inicial para entender necesidades, revisar infraestructura de lo que solicita el cliente.**	**Jefe de ciberseguridad, Oficial de ciberseguridad, jefe de ventas de la cooperativa Al cibersecurity**
Evaluación del riesgo	**Identificación de activos digitales, análisis de amenazas y vulnerabilidades, y priorización de riesgos.**	**Jefe de ciberseguridad, Analista de riesgos**
Diseño de la estrategia de ciberseguridad de acuerdo con el requerimiento de la organización	**Realizar la propuesta de controles de seguridad y creación de un plan de implementación.**	**Oficiales de ciberseguridad de la cooperativa Al ciberseguridad**
Elaboración del plan estratégico para ejecutar el servicio	**Desarrollo de un plan de respuesta a incidentes, creación de un DRP y recomendaciones al cliente en planes futuros de ciberseguridad.**	**Departamento de logística y Oficial de ciberseguridad**
Seguimiento del servicio	**Reunión Dpto. Asociatividad con Junta Directiva para análisis de inclusión de nuevos postulantes a la Asociación como socios activos. En caso de decidir que el postulante no ingresa, notificar rechazo de solicitud.**	**Oficiales de ciberseguridad de la cooperativa Al cibersecurity**
Seguimiento y mejora continua	**Revisiones periódicas, actualización de la estrategia y soporte continuo para la implementación de recomendaciones.**	**Oficiales de ciberseguridad de la cooperativa Al cibersecurity**

Flujograma

En la presente ilustración se muestra la descripción del Flujo de Procesos del Servicio de Consultoría en Ciberseguridad:

Ilustración 23

Flujograma del servicio de consultoría



Nota. Proceso que se utilizara en el servicio de consultoría en ciberseguridad de la cooperativa AI Cibersecurity.

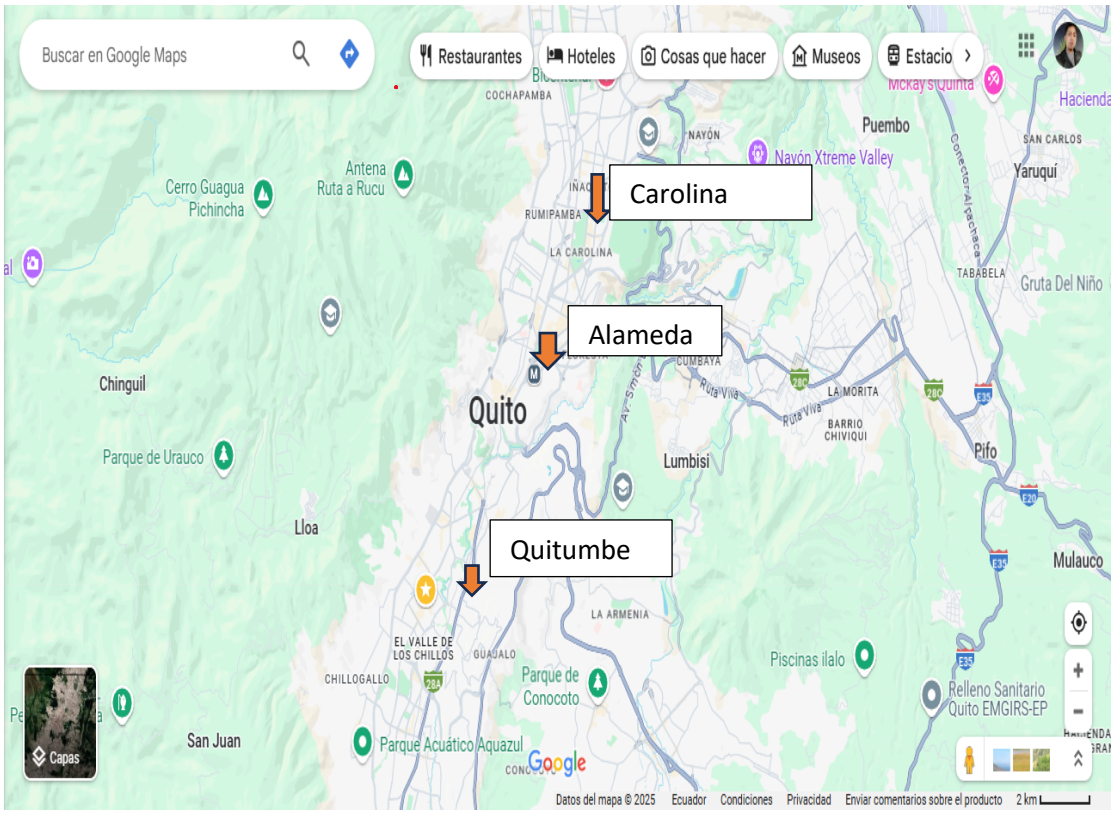
Macro localización y Micro localización

La Cooperativa de servicios digitales en ciberseguridad AI Cibersecurity estará ubicada al norte de Quito como macro localización.

En cuanto a la micro localización se definirá en 3 lugares estratégicos en el sector de Quitumbe, sector la Carolina o el sector de Alameda.

Ilustración 24

Posibles puntos estratégicos de ubicación de AI Cibersecurity



Nota. Ubicaciones estratégicas para el funcionamiento de la cooperativa AI cibersecuriti

Tabla 22

Macro localización de AI Cibersecurity

MACRO LOCALIZACIÓN							
DIRECCIÓN /UBICACIÓN		SUR		CENTRO		NORTE	
FACTORES	PONDERACIÓN	CALIFICACIÓN 1-10	CALIFICACIÓN PONDERADA	CALIFICACIÓN 1-10	CALIFICACIÓN PONDERADA	CALIFICACIÓN 1-10	CALIFICACIÓN PONDERADA
Infraestructura	22	6	132	6	105	9	120
Economía local	28	6	168	5	140	9	252
Acceso a transporte público	25	7	175	8	200	10	250
Ubicación de competencia	11	6	66	7	77	7	66
Disponibilidad de conexiones y datos	30	5	150	7	210	10	150
Costo de alquiler de instalaciones.	25	7	175	8	200	10	175
TOTAL			866		932		1013

Nota. Datos de auto

Tabla 23

Micro localización de AI Cibersecurity

MICRO LOCALIZACIÓN							
DIRECCIÓN /UBICACIÓN		Quitumbe		La Colón		La Carolina	
FACTORES	PONDERACIÓN	CALIFICACIÓN 1-10	CALIFICACIÓN PONDERADA	CALIFICACIÓN 1-10	CALIFICACIÓN PONDERADA	CALIFICACIÓN 1-10	CALIFICACIÓN PONDERADA
Infraestructura	22	7	154	8	105	9	120
Economía local	28	8	224	10	280	9	252
Acceso a transporte público	25	10	250	8	200	9	225
Ubicación de competencia	11	7	77	7	77	5	77
Disponibilidad de conexiones y datos	30	9	270	7	210	10	270
Costo de alquiler de instalaciones.	25	7	175	8	200	9	175
TOTAL			1150		1072		1119

Nota. Datos del autor

Marketing

La cooperativa AI Cibersecurity reconoce que el éxito organizacional va más allá de la calidad de sus productos y servicios; se basa en su diseño, posicionamiento y comunicación efectiva hacia el público objetivo.

Diseño del Servicio

La cooperativa ofrece servicios digitales especializados en ciberseguridad, enfocados en cuatro productos clave:

Tabla 24

Servicios que oferta AI Cibersecurity

Nombre	Tipo	Descripción	Beneficio
Auditorias de ciberseguridad	Servicio	Evaluación de sistemas vulnerables, con informes detallados.	Identificación y mitigación de posibles riesgos cibernéticos.
Capacitación en ciberseguridad y protección de datos.	Servicio	Programas personalizados con simulaciones y respuestas rápidas ante riesgos de ataques cibernéticos y seguridad digital.	Crear conciencia y habilidades al personal, reduciendo las brechas de seguridad.
Protección de Infraestructuras Digitales.	Servicio	Gestión inmediata ante incidentes y restauración de sistemas afectados.	Minimizar el impacto ante incidentes.

Monitoreo y alertas en tiempo real	Servicio	Estrategias personalizadas con monitoreo activo 24/7 y prevención de riesgos cibernéticos	Reducir la probabilidad de ataques y asegurar la continuidad del negocio.

Nota. servicios que oferta la cooperativa.

Características del diseño de productos y servicios

- Escalabilidad: Servicios adaptados a organizaciones de distintos segmentos y sectores.
- Tecnología: Algoritmos de IA actualizados para enfrentar amenazas emergentes.
- Enfoque en experiencia del cliente: reportes claros, fácil manejo de los programas, capacitación continua y soporte 24/7.

Estrategia de Precios

La cooperativa AI Cibersecurity está comprometida con extender el conocimiento sobre la ciberseguridad para las organizaciones de economía popular y solidaria en Quito, asegurando que la protección digital sea accesible y sostenible. La estrategia de precios busca equilibrar la calidad de los servicios con la demanda del servicio y adaptándose a las necesidades económicas de las organizaciones, reforzando los principios cooperativos.

Estructura de precios

- **Precios Accesibles**: La cooperativa negociará con proveedores de tecnología, software y socios locales para reducir costos en herramientas de análisis y monitoreo, ofreciendo auditorías de seguridad y planes de mitigación a tarifas asequibles que respeten los recursos limitados de las organizaciones

- **Planes de Pago:** Se implementarán opciones de pago en cuotas mensuales accesibles para servicios como planes de mitigación de riesgos y capacitaciones, facilitando la inversión en seguridad sin afectar la estabilidad financiera de las organizaciones.

- **Beneficios para Socios**: Las organizaciones afiliadas a la cooperativa o a redes de economía popular y solidaria en Quito recibirán descuentos del 8-12% en todos los servicios, promoviendo la solidaridad y el fortalecimiento de la comunidad.

Tabla 25

Tabla de precios de los servicios

Tipo de servicio	Precio del servicio (USD)
Consultoría y auditorías de seguridad	600-2000$ dependiendo el tamaño de la organización
Capacitación en ciberseguridad y protección de datos.	400$- 1000$ dependiendo el personal a capacitar.
Protección de Infraestructuras Digitales	500 - 3000$ dependiendo el incidente
Monitoreo y alertas en tiempo real	500-1200$ según la necesidad de las organizaciones

Nota. Se detalla los precios de los servicios que oferta la organización.

Plaza (Distribución y Canales de Venta)

Canales de distribución:

- **Oficinas en Quito**: Espacio donde los clientes podrán recibir asesoría personalizada, acceder a productos y participar en capacitaciones.
- **Plataforma y tiendas online**: Implementar una página web para contratación servicios online, acceder a informes de auditorías, inscribirse en capacitaciones y gestionar planes de mitigación. Incluyendo un panel de cliente para monitoreo en tiempo real.
- **Redes sociales y canales digitales:** Mantener presencia en rede sociales y plataformas como Mercado libre, Google Cloud y Marketplace para llegar a organizaciones que buscan soluciones integradas de ciberseguridad.
- **Asociaciones estratégicas**: Colaborar con organizaciones, cooperativas tecnológicas y cámaras de comercio para distribuir servicios.
- **Eventos especializados**: Participar en eventos tecnológicos que impulsen la conciencia de contratar servicios tecnológicos como ciberseguridad, Inteligencia artificial, Block chain, sistemas operativos libres y asi captar clientes empresariales.

Estrategia de Promoción y Publicidad

- **Marketing de contenidos**: Crear blogs y videos sobre temas como “Prevención de ataques cibernéticos" o "Errores comunes al momento de guardar claves en tu dispositivo digital", con el fin de dar a conocer los posibles riesgos de ciberseguridad y atraer posibles clientes.

- **Redes sociales**: Crear contenido para plataformas como LinkedIn para conectar con tomadores de decisiones (CIOs o Gerentes de organizaciones) para compartir alertas de amenazas y consejos rápidos para prevención de ciberataques.

- **Talleres gratuitos**: Organizar sesiones virtuales por zoom o colaboraciones con organizaciones sobre auditorías o capacitaciones, que demuestren el valor de los servicios de ciberseguridad y prevención de ataques cibernéticos.

- **Programas de referidos**: Ofrecer descuentos a clientes potenciales con el fin que recomienden los servicios que oferta la organización.

Plan Financiero

Tabla 26

Costos de alquiler de oficinas y equipos

Articulo	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
Alquiler de oficinas	12 meses	$ 600,00	$ 7.200,00
Mobiliario de Oficinas	12	$ 100,00	$ 1.200,00
Equipos de comunicación	5	$ 120,00	$ 600,00
Servidores y software de seguridad	1	$ 1.500,00	$ 1.500,00
TOTAL			**$ 10.500,00**

Nota. La tabla enumera los costos de la cooperativa de ciberseguridad en Quito, abarcando el alquiler de oficinas, mobiliario, equipos de comunicación, servidores y software de seguridad, fundamentales para establecer la infraestructura operativa adecuada para su funcionamiento.

Tabla 27

Costos de equipo de tecnológicos y software

Articulo	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
Laptops	8	$ 800,00	$ 6.400,00
Servicios en la nube	1	$ 1.000,00	$ 1.000,00
Licencias de software	1	$ 1.200,00	$ 1.200,00
Proyectores	3	$ 700,00	$ 2.100,00
TOTAL			**$ 10.700,00**

Nota. La tabla describe la inversión en equipos tecnológicos y software necesarios para garantizar una infraestructura tecnológica robusta y facilitar las operaciones de AI Cibersecurity.

Tabla 28

Costos de enseres y mobiliarios

Articulo	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
Sillas ergonómicas	6	$ 100,00	$ 600,00
Cafeteras	2	$ 60,00	$ 120,00
Microondas	2	$ 70,00	$ 140,00
Estanterías	3	$ 150,00	$ 450,00
TOTAL			**$ 1.310,00**

Nota. La tabla muestra la inversión estratégica de la cooperativa de ciberseguridad para crear un espacio de trabajo dinámico y funcional cada elemento cuidadosamente seleccionado para impulsar un entorno eficiente en la entrega de servicios de seguridad digital de primer nivel.

Tabla 29

Inversión Inicial

Resumen de la inversión inicial	Costos ($)
Costos de alquiler oficinas y equipos	$ 10.500,00
Costos de mobiliario y enseres	$ 1.130,00
Costos de equipos de cómputo y software	$ 10.700,00
TOTAL	**$ 22.330,00**

Nota. La Tabla expone la inversión inicial de la cooperativa, destinada a construir una base operativa sólida, todo cuidadosamente planificado para impulsar la eficiencia y la innovación en la seguridad tecnológica.

Tabla 30

Remuneraciones del personal humano

Personal	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
Gerente General	1	$ 1.200,00	$ 1.200,00
Administrador	1	$ 850,00	$ 850,00
Contador	1	$ 800,00	$ 800,00
Asistente	1	$ 700,00	$ 700,00
TOTAL			**$ 3.550,00**

Nota. Los sueldos de los colaboradores detallan la inversión estratégica de la cooperativa de ciberseguridad en su talento humano, todo diseñado para fortalecer la estructura organizativa y potenciar la entrega de servicios digitales innovadores.

Tabla 31

Costos de los Sueldos del personal Operativo

Personal	CANTIDAD	COSTO UNITARIO	COSTO TOTAL
Analista de ciberseguridad	1	$ 1.000,00	$ 1.000,00
Especialista en Pentesting	1	$ 1.200,00	$ 1.200,00
Ejecutivo de ventas	1	$ 1.000,00	$ 1.000,00
Community manager	1	$ 900,00	$ 700,00
TOTAL			**$ 3.900,00**

Nota. La inversión en talento humano operativo permitirá que la cooperativa rinde un servicio eficiente.

Tabla 32

Costos anuales de los colaboradores de AI Cibersecurity

Dependencia	Costo total ($)	Costo Anual ($)
Personal Operativo	$ 3.900,00	$ 46.800,00
Personal Administrativo	$ 3.550,00	$ 42.600,00
TOTAL	**$ 7.450,00**	**$ 89.400,00**

Nota. Los costos anuales del talento humano muestran la solides y garantizan la sostenibilidad de la cooperativa.

Tabla 33

Tabla de la amortización crediticia

Valor del préstamo	30.475,00
Tasa Nominal	16,25%
Años	3
Frecuencia de Pago	Mensual
Interés equivalente	*1,354%*
N° de pagos por año	*12*
N° Total de Cuotas	*36*
CUOTA PARA PAGAR	*$ 1.075,18*

Resumen:	
Valor préstamo	*$ 30.475,00*
Suma de Cuotas	*$ 38.706,33*
Suma de Interés	*$ 8.231,33*

Número de Cuota	CUOTA PARA PAGAR	INTERÉS	CAPITAL AMORTIZADO	SALDO CAPITAL
0				$ 30.475,00
1	$ 1.075,18	$ 412,68	$ 662,49	$ 29.812,51
2	$ 1.075,18	$ 403,71	$ 671,46	$ 29.141,04
3	$ 1.075,18	$ 394,62	$ 680,56	$ 28.460,48
4	$ 1.075,18	$ 385,40	$ 689,77	$ 27.770,71
5	$ 1.075,18	$ 376,06	$ 699,11	$ 27.071,60
6	$ 1.075,18	$ 366,59	$ 708,58	$ 26.363,02
7	$ 1.075,18	$ 357,00	$ 718,18	$ 25.644,84
8	$ 1.075,18	$ 347,27	$ 727,90	$ 24.916,94
9	$ 1.075,18	$ 337,42	$ 737,76	$ 24.179,18
10	$ 1.075,18	$ 327,43	$ 747,75	$ 23.431,43
11	$ 1.075,18	$ 317,30	$ 757,88	$ 22.673,55
12	$ 1.075,18	$ 307,04	$ 768,14	$ 21.905,42
13	$ 1.075,18	$ 296,64	$ 778,54	$ 21.126,88
14	$ 1.075,18	$ 286,09	$ 789,08	$ 20.337,79
15	$ 1.075,18	$ 275,41	$ 799,77	$ 19.538,02
16	$ 1.075,18	$ 264,58	$ 810,60	$ 18.727,43
17	$ 1.075,18	$ 253,60	$ 821,58	$ 17.905,85
18	$ 1.075,18	$ 242,48	$ 832,70	$ 17.073,15
19	$ 1.075,18	$ 231,20	$ 843,98	$ 16.229,17
20	$ 1.075,18	$ 219,77	$ 855,41	$ 15.373,77
21	$ 1.075,18	$ 208,19	$ 866,99	$ 14.506,78
22	$ 1.075,18	$ 196,45	$ 878,73	$ 13.628,05
23	$ 1.075,18	$ 184,55	$ 890,63	$ 12.737,42
24	$ 1.075,18	$ 172,49	$ 902,69	$ 11.834,73
25	$ 1.075,18	$ 160,26	$ 914,91	$ 10.919,82

26	$ 1.075,18	$ 147,87	$ 927,30	$ 9.992,51
27	$ 1.075,18	$ 135,32	$ 939,86	$ 9.052,65
28	$ 1.075,18	$ 122,59	$ 952,59	$ 8.100,06
29	$ 1.075,18	$ 109,69	$ 965,49	$ 7.134,58
30	$ 1.075,18	$ 96,61	$ 978,56	$ 6.156,02
31	$ 1.075,18	$ 83,36	$ 991,81	$ 5.164,20
32	$ 1.075,18	$ 69,93	$ 1.005,24	$ 4.158,96
33	$ 1.075,18	$ 56,32	$ 1.018,86	$ 3.140,10
34	$ 1.075,18	$ 42,52	$ 1.032,65	$ 2.107,45
35	$ 1.075,18	$ 28,54	$ 1.046,64	$ 1.060,81
36	$ 1.075,18	$ 14,37	$ 1.060,81	$ 0,00

Nota. Datos del autor

Tabla 34

Precio e ingresos de la venta de servicios

Tiempo	Producción por unidades	Costo Unitario ($)	Costo Variable	Costo total	Utilidad	Precio	Ingreso Total
Mensual	18	$ 330,12	$ 68,30	$ 5942,16	$ 1828,44	$ 500	$ 9000

Nota. Ingresos de AI Cibersecurity por la venta de servicios

Interpretacion

La tabla refleja la proyección de ingresos de la cooperativa AI Cibersecurity, basada en la prestación de sus servicios digitales, para determinar el costo unitario de los servicios de

ciberseguridad ofrecidos por la cooperativa en Quito, se tomaron en cuenta todos los rubros incluidos en la inversión inicial (infraestructura tecnológica, licencias de software, equipos) y los costos por el talento humano necesario (especialistas en ciberseguridad, analistas, capacitadores). Se proyecta una producción mensual de 18 servicios. El costo variable fue calculado como el valor indicado en la tabla ($68.30 por unidad). El costo total fue la suma de los costos fijos y variables. La utilidad se obtuvo restando el costo total de los ingresos totales. El precio se determinó dividiendo el ingreso total entre la producción. El ingreso total mensual se obtuvo multiplicando la producción (18 servicios) por el precio de cada servicio.

Proyección de Ventas

Tabla 35

Ventas proyectadas AI Cibersecurity

AÑO	Unidades Vendidas	Ingresos Totales	Costos Totales	Utilidad Total
2026	216	$ 121.125,00	$ 139.577,57	-$18.452,57
2027	238	$ 133.227,50	$ 137.502,69	-$ 4.275,19
2028	261	$ 146.561,25	$ 134.501,24	$ 12.060,01
2029	287	$ 161.217,38	$ 136.286,36	$ 24.931,02

2030	316	$ 177.339,11	$ 138.250,00	$ 39.089,11

Nota. Datos del Autor

La tabla presenta la proyección financiera de la cooperativa de ciberseguridad en Quito para los años 2026 a 2030, basada en la venta de servicios. En 2026, con 216 servicios vendidos, los ingresos totales alcanzan $121,125, pero los costos totales ($139,577.57) generan una pérdida de $18,452.57. En 2027, las unidades vendidas aumentan a 238, con ingresos de $133,227.50, pero persiste una pérdida menor de $4,275.19. Para 2028, con 261 servicios, los ingresos ($146,561.25) superan los costos ($134,501.24), logrando una utilidad de $12,060.01. La tendencia positiva continúa en 2029 (287 servicios, utilidad de $24,931.02) y 2030 (316 servicios, utilidad de $39,089.11), reflejando un crecimiento sostenido en ventas e ingresos, junto con una mejor gestión de costos, lo que indica una mejora en la rentabilidad de la cooperativa con el tiempo.

Tabla 36

Flujo de Ingresos y Gastos

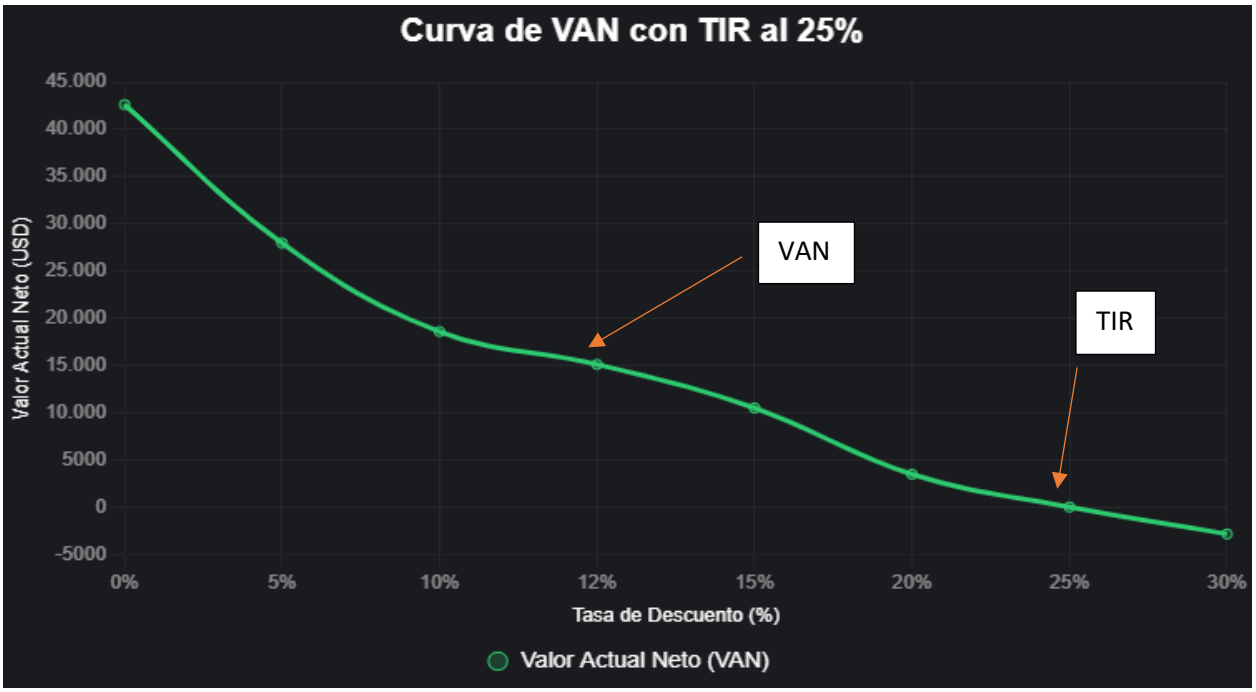
INGRESOS:	**AÑO 0**	**AÑO 1**	**AÑO 2**	**AÑO 3**	**AÑO 4**	**AÑO 5**
Ventas (deducido IVA)		**$ 121.125,00**	**$ 133.237,50**	**$ 146.561,25**	**$ 161.217,38**	**$ 177.339,11**
Total ingresos		$ 121.125,00	$ 133.237,50	$ 146.561,25	$ 161.217,38	$ 177.339,11
GASTOS:	**AÑO 0**	**AÑO 1**	**AÑO 2**	**AÑO 3**	**AÑO 4**	**AÑO 5**
Gastos de operación						
Gastos variables		$ 14.753,09	$ 16.228,40	$ 17.851,24	$ 19.636,36	$ 21.600,00
Gastos fijos		$ 104.400,00	$ 104.400,00	$ 104.400,00	$ 104.400,00	$ 104.400,00
Gastos de mantenimiento		$ 6.250,00	$ 6.250,00	$ 6.250,00	$ 6.250,00	$ 6.250,00
Subtotal Gastos de operación		**$ 125.403,09**	**$ 126.878,40**	**$ 128.501,24**	**$ 130.286,36**	**$ 132.250,00**
Gastos de Promoción y publicidad		$ 6.000,00	$ 6.000,00	$ 6.000,00	$ 6.000,00	$ 6.000,00
Gastos financieros		$ 8.174,47	$ 4.624,29		$ -	$ -
Total gastos		**$ 139.577,57**	**$ 137.502,69**	**$ 134.501,24**	**$ 136.286,36**	**$ 138.250,00**
Déficit o Superávit operativo		**$ -18.452,57**	**$ -4.265,19**	**$ 12.060,01**	**$ 24.931,01**	**$ 39.089,11**

Nota. Datos del Autor

Interpretación. La tabla proyecta el flujo financiero de la cooperativa de ciberseguridad en Quito desde el Año 0 al Año 5, mostrando un crecimiento sostenible en ingresos por ventas de servicios digitales. Inicialmente, los gastos operativos, de promoción y financieros superan los ingresos, generando déficits en los Años 1 y 2. Desde el Año 3, la cooperativa logra superávits crecientes, impulsados por mayores ventas y control de costos variables. Los gastos fijos y de mantenimiento permanecen constantes, mientras que los costos financieros disminuyen tras el Año 2. Este panorama refleja una transición hacia la rentabilidad, consolidando la viabilidad del proyecto.

Ilustración 25

Curva del VAN y el TIR



Nota. Datos del autor

Tabla 37

Tabla de indicadores financieros

Tasa de descuento anual	12,0%

CÁLCULO DE INDICADORES FINANCIEROS			
INDICADOR	VALOR US$	RANGO	ESTADO
AÑO 0	-11.625		
AÑO 1	-18.453		
AÑO 2	-4.265		
AÑO 3	12.060		
AÑO 4	24.931		
AÑO 5	39.089		
VA (año 1 a 5)	26.733		
VAN	15.108	positivo	Factible
TIR	25%	> tasa desc.	Factible
B/C	2,3	> 1	Factible

Nota. Datos del Autor

Interpretación

La tabla presenta los indicadores financieros proyectados para la cooperativa AI Cibersecurity, evaluando la viabilidad de su inversión en servicios con una tasa de descuento anual del 12%. En el Año 0, se registra una inversión inicial de -$11,625, reflejando los costos de arranque. En el Año 1 (2026), la cooperativa incurre en una pérdida de -$18,453, seguida de una pérdida menor en el Año 2 (2027) de -$4,265, debido a ingresos insuficientes frente a los costos.

A partir del Año 3 (2028), con $12,060, se logra una utilidad positiva, que crece significativamente en el Año 4 (2029) a $24,931 y en el Año 5 (2030) a $39,089, indicando una mejora en la rentabilidad. El Valor Actual de los flujos de caja de los años 1 a 5 suma $26,733. El Valor Actual Neto de $15,108, positivo, sugiere que el proyecto es financieramente factible, al generar valor por encima de la inversión inicial. La Tasa Interna de Retorno (TIR) del 25%, superior a la tasa de descuento del 12%, confirma la rentabilidad del proyecto. El Beneficio/Costo de 2.3, mayor a 1, indica que los beneficios superan ampliamente los costos. En conjunto, los indicadores demuestran que la cooperativa es una inversión factible y atractiva, con un retorno creciente a medida que aumenta la producción y se optimizan los costos.

Conclusiones generales

El capítulo tres demuestra que la propuesta de creación de una cooperativa de servicios digitales en ciberseguridad resulta relevante y pertinente para fortalecer al sector de la Economía Popular y Solidaria, pues responde a una necesidad creciente de protección digital dentro de las organizaciones de Quito. La filosofía empresarial, políticas institucionales y modelo de negocio planteados muestran sólidos fundamentos cooperativos, enfocados en la innovación, accesibilidad y sostenibilidad. Desde el punto de vista financiero, pese a registrar pérdidas en los dos primeros años de operación, las proyecciones evidencian que a partir del tercer año se genera rentabilidad, lo que confirma la viabilidad económica del plan. En este sentido, los indicadores financieros (VAN, TIR y B/C) reflejan que la inversión es atractiva y genera valor social y económico a mediano plazo. Asimismo, la estrategia de marketing, los servicios propuestos y las alianzas estratégicas previstas permiten posicionar a la cooperativa como una alternativa competitiva en un mercado desatendido, generando impactos positivos tanto en la seguridad digital como en el desarrollo del tejido cooperativo.

Recomendaciones generales

Se sugiere fortalecer las campañas de sensibilización y capacitación en ciberseguridad dirigidas a potenciales clientes del sector EPS, con el fin de incrementar el nivel de conciencia sobre los riesgos digitales y fomentar la contratación de servicios especializados. Además, es recomendable priorizar la búsqueda de financiamiento externo (capital semilla, subvenciones y alianzas con instituciones públicas o privadas) para mitigar las limitaciones presupuestarias iniciales y acelerar el crecimiento operativo. Igualmente, se aconseja implementar una estrategia de diferenciación basada en el modelo cooperativo y el uso de tecnologías innovadoras como la inteligencia artificial, para generar ventajas competitivas sostenibles frente a grandes empresas privadas del sector. Finalmente, se recomienda mantener un sistema de monitoreo continuo de los indicadores financieros y operativos, ajustando los procesos según los cambios del entorno tecnológico y socioeconómico, con el propósito de asegurar el cumplimiento de los objetivos estratégicos planteados hasta 2030.

Anexos

Anexo 1

Modelo de entrevistas

Las presente preguntas tienen fines estrictamente académicos, y sus respuestas tendrán la confidencialidad del caso. Por favor sírvase contestar las siguientes preguntas con la mayor sinceridad posible.

Entrevista a lideres de opinión en ciberseguridad

1.- ¿En su opinión qué tan necesario considera la adopción de servicios de ciberseguridad para pymes y organizaciones?

2.- ¿En su opinión cree usted que actualmente el mercado oferta suficientes servicios de ciberseguridad, y que sean asequibles para la protección de la información en pymes y organizaciones?

3.- ¿Qué tipo de ataques cibernéticos considera que son los más frecuentes en Ecuador?

4.-Según su experiencia, ¿cuáles son los riesgos de ciberseguridad más frecuentes que enfrentan las organizaciones y empresas que no salvaguardan su imformacion digital?

5.-Según su experiencia, ¿cuáles son las mayores barreras que impiden a las organizaciones y empresas implementar servicios de ciberseguridad?

6.- ¿Cree usted que una red colaborativa de profesionales en ciberseguridad podría mejorar la capacidad de las organizaciones y empresas para mitigar riesgos digitales?

7.- ¿Qué herramientas o programas recomendaría para proteger datos sensibles en una empresa u organización?

Anexo 2

Encuesta a Las Cooperativas de Ahorro y Crédito de la Ciudad de Quito

La presente encuesta tiene fines estrictamente académicos, y sus respuestas tendrán la confidencialidad del caso. Por favor sírvase contestar las siguientes preguntas con la mayor sinceridad posible.

1.- ¿Su organización ha sufrido algún tipo de ciberataque a la información interna, tales como robo de datos, phishing, etc. en los últimos 2 años?

☐ Sí

☐ No

☐ No está seguro

2.- ¿Qué tan prioritario es para su organización proteger sus datos financieros y los de sus clientes?

☐ Nada prioritario

☐Prioritario

☐Máxima prioridad

3.- ¿Su organización al momento cuenta con alguna herramienta digital de ciberseguridad para protegeré su información?

☐ SI

☐ NO

4.- En el caso de ser negativa su respuesta anterior, ¿Considera usted que su organización estaría interesada en contar con los servicios de ciberseguridad?

☐ Sí

☐ No

5.- ¿Qué factor considera usted que sería decisivo para contratar un servicio de ciberseguridad?

☐ Precio accesible

☐ Experiencia del proveedor

☐ Soporte 24/7

☐ Recomendación de otras organizaciones

Otros (especifique)

6.- ¿Qué resultado considera más valioso en un servicio de ciberseguridad?

☐ Reducción de incidentes

☐ Cumplimiento legal (protección de datos)

☐ Capacitación del personal

☐ Soporte técnico rápido

Otros (especifique)

7.- ¿Qué tipo de servicios le interesaría contratar?

☐ Auditorías de seguridad

☐ Capacitaciones para empleados/socios

☐ Protección de bases de datos

☐ Monitoreo continuo de redes

☐ Otro: _____.

8.- ¿Su personal ha recibido capacitación básica en ciberseguridad?

☐ Sí, todos

☐ Solo algunos

☐ No

☐ No sabe

9.- ¿Qué tiempo de respuesta esperaría ante un incidente de seguridad?

☐ Inmediato (menos de 1 hora)

☐ 12 horas

☐ 24 horas

☐ 1 semana

10.-Considerando los servicios de ciberseguridad mencionados, ¿qué rango de inversión consideraría adecuado para su organización?"

☐ Menos de $100

☐ $100 - $300

☐ $301 - $600

☐ $601 - $1,000

☐ Más de $1,000

☐ Prefiero un modelo de pago por servicio específico

11.- ¿Prefiere un servicio de ciberseguridad con pagos:

☐ Mensuales

☐ Anuales

☐ Por proyecto

12.- ¿Invertiría en un paquete de servicios que incluya monitoreo + capacitación por un costo mensual de $100-$200?

☐ Sí

☐ No

☐ Depende de la necesidad de la organización

Bibliografía

GCI. (0ctubre de 2020). *Estrategias nacionales de ciberseguridad.* Obtenido de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2022/10/Difusion-ENC.pdf

Gomez, L. (agosto de 2024). *Transformación digital en Ecuador: Un viaje de innovación y adaptación*. Obtenido de https://itahora.com/2024/08/15/transformacion-digital-en-ecuador-un-viaje-de-innovacion-y-adaptacion/

Heredia, J. S. (2021). *Ciberseguridad en Ecuador y Latinoamérica.* Esmeraldas. Obtenido de https://killkana.ucacue.edu.ec/index.php/killkana_tecnico/article/view/957/1074

ISO, s. c. (s.f.). *ww.iso.org*. Obtenido de file:///C:/Users/EQUIPO/Videos/ISO%2026.000.pdf

LOEPS. (10 de mayo de 2011). *constitucion de la republica del Ecuador*. Obtenido de file:///C:/Users/EQUIPO/Downloads/Ley%20org%C3%A1nica%20EPS.pdf

Mundial, B. (2020). Obtenido de https://www.bancomundial.org/ext/es/home

Pursell, S. (13 de 12 de 2021). *HUBSPOT*. Obtenido de https://blog.hubspot.es/marketing/que-es-plan-de-negocios

SEPS. (Julio de 2021). Obtenido de https://www.seps.gob.ec/wp-content/uploads/Evaluacio%CC%81n-de-la-Inclusio%CC%81n-Financiera-y-los-Servicios-Financieros-Digitales-en-el-Ecuador.pdf

Centro de Respuesta a Incidentes Cibernéticos del Ecuador. (Marzo de 2022). Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/05/DIAGNO%CC%81STICO-DE-LAS-CAPACIDADES-DE-CIBERSEGURIDAD-Ecuador-Diciembre-2022_compressed.pdf

GCI. (2024). Obtenido de https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

Gomez, L. (Agosto de 2024). *Transformación digital en Ecuador: Un viaje de innovación y adaptación*. Obtenido de https://itahora.com/2024/08/15/transformacion-digital-en-ecuador-un-viaje-de-innovacion-y-adaptacion/

Heredia, J. S. (2021). *Ciberseguridad en Ecuador y Latinoamérica.* Esmeraldas. Obtenido de https://killkana.ucacue.edu.ec/index.php/killkana_tecnico/article/view/957/1074

INEC. (2024). *Tecnologías de la Información y Comunicación-TIC*. Obtenido de https://www.ecuadorencifras.gob.ec/tecnologias-de-la-informacion-y-comunicacion-tic/

ISO, s. c. (s.f.). *ww.iso.org*. Obtenido de file:///C:/Users/EQUIPO/Videos/ISO%2026.000.pdf

Latam, P. (s.f.). Obtenido de https://www.pentestinglatam.com/ciberseguridad-en-quito/

LOEPS. (10 de mayo de 2011). *constitucion de la republica del Ecuador*. Obtenido de file:///C:/Users/EQUIPO/Downloads/Ley%20org%C3%A1nica%20EPS.pdf

Mundial, B. (2020). Obtenido de https://www.bancomundial.org/ext/es/home

Plan Quito digital. (27 de Febrero de 2023-2027). Obtenido de https://www.quitoinforma.gob.ec/2024/02/27/plan-de-seguridad-y-convivencia-2023-2027-disponible-en-webs-municipales/#:~:text=%E2%80%93%20El%20Plan%20Metropolitano%20de%20Seguridad,para%20la%20ciudadan%C3%ADa%20en%20general.

Pursell, S. (13 de 12 de 2021). *HUBSPOT*. Obtenido de https://blog.hubspot.es/marketing/que-es-plan-de-negocios

Sayago-Heredia, J. (21 de febrero de 2022). *Ciberseguridad en Ecuador y Latinoamérica.* Obtenido de https://killkana.ucacue.edu.ec/index.php/killkana_tecnico/article/view/957

SEPS. (Julio de 2021). Obtenido de https://www.seps.gob.ec/wp-content/uploads/Evaluacio%CC%81n-de-la-Inclusio%CC%81n-Financiera-y-los-Servicios-Financieros-Digitales-en-el-Ecuador.pdf

SEPS. (2023). Obtenido de https://www.seps.gob.ec/wp-content/uploads/CUC-2023.pdf

SFPS. (Agosto de 2021). Obtenido de https://www.seps.gob.ec/wp-content/uploads/Estudio_SEPS_ITAhora.pdf

Centro de Respuesta a Incidentes Cibernéticos del Ecuador. (Marzo de 2022). Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/05/DIAGNO%CC%81STICO-DE-LAS-CAPACIDADES-DE-CIBERSEGURIDAD-Ecuador-Diciembre-2022_compressed.pdf

GCI. (2024). Obtenido de https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

Gomez, L. (Agosto de 2024). *Transformación digital en Ecuador: Un viaje de innovación y adaptación*. Obtenido de https://itahora.com/2024/08/15/transformacion-digital-en-ecuador-un-viaje-de-innovacion-y-adaptacion/

Heredia, J. S. (2021). *Ciberseguridad en Ecuador y Latinoamérica.* Esmeraldas. Obtenido de https://killkana.ucacue.edu.ec/index.php/killkana_tecnico/article/view/957/1074

INEC. (2024). *Tecnologías de la Información y Comunicación-TIC*. Obtenido de https://www.ecuadorencifras.gob.ec/tecnologias-de-la-informacion-y-comunicacion-tic/

INEC. (Abril de 2025). Obtenido de https://www.ecuadorencifras.gob.ec/indice-de-precios-al-consumidor/

ISO, s. c. (s.f.). *ww.iso.org*. Obtenido de file:///C:/Users/EQUIPO/Videos/ISO%2026.000.pdf

Latam, P. (s.f.). Obtenido de https://www.pentestinglatam.com/ciberseguridad-en-quito/

LOEPS. (10 de mayo de 2011). *constitucion de la republica del Ecuador*. Obtenido de file:///C:/Users/EQUIPO/Downloads/Ley%20org%C3%A1nica%20EPS.pdf

Mundial, B. (2020). Obtenido de https://www.bancomundial.org/ext/es/home

Plan Quito digital. (27 de Febrero de 2023-2027). Obtenido de https://www.quitoinforma.gob.ec/2024/02/27/plan-de-seguridad-y-convivencia-2023-2027-disponible-en-webs-municipales/#:~:text=%E2%80%93%20El%20Plan%20Metropolitano%20de%20Seguridad,para%20la%20ciudadan%C3%ADa%20en%20general.

Pursell, S. (13 de 12 de 2021). *HUBSPOT*. Obtenido de https://blog.hubspot.es/marketing/que-es-plan-de-negocios

Sayago-Heredia, J. (21 de febrero de 2022). *Ciberseguridad en Ecuador y Latinoamérica.* Obtenido de https://killkana.ucacue.edu.ec/index.php/killkana_tecnico/article/view/957

SEPS. (Julio de 2021). Obtenido de https://www.seps.gob.ec/wp-content/uploads/Evaluacio%CC%81n-de-la-Inclusio%CC%81n-Financiera-y-los-Servicios-Financieros-Digitales-en-el-Ecuador.pdf

SEPS. (2023). Obtenido de https://www.seps.gob.ec/wp-content/uploads/CUC-2023.pdf

SFPS. (Agosto de 2021). Obtenido de https://www.seps.gob.ec/wp-content/uploads/Estudio_SEPS_ITAhora.pdf