TECNOLÓGICO DE ESTUDIOS SUPERIORES DE IXTAPALUCA

MAESTRÍA EN ADMINISTRACIÓN

LINEA DE INVESTIGACION:
DESARROLLO Y FORTALECIMIENTO DE LAS ORGANIZACIONES.

MODELO DE NEGOCIOS DE UNA CONSULTORIA EN CIBERSEGURIDAD PARA PROFESIONALES DE IXTAPALUCA Y VALLE DE CHALCO

TESIS

QUE PRESENTA:

EBNER JUAREZ ELIAS

PARA OBTENER EL GRADO DE:

MAESTRO EN ADMINISTRACIÓN

DIRECTOR DE TESIS:

MTRA. ARRIETA LÓPEZ MARIA DEL CARMEN

IXTAPALUCA, ESTADO DE MÉXICO

AGOSTO, 2024

"2024. Año del Bicentenario de la Erección del Estado Libre y Soberano de México".

COMITÉ DE REVISIÓN Y TITULACIÓN APROBADO POR EL CONSEJO DE POSGRADO

Ixtapaluca, Estado de México a 13 de septiembre de 2024.

Los abajo firmantes, Miembros del Jurado para Examen de Grado de Maestría, hacen CONSTAR que, habiendo revisado el trabajo de tesis desarrollado por el **ING. JUÁREZ ELIAS EBNER,** bajo el título **"MODELO DE NEGOCIO DE UNA CONSULTORÍA EN CIBERSEGURIDAD PARA PROFESIONALES DE IXTAPALUCA Y VALLE DE CHALCO",** hemos dictaminado que ha sido aprobado y aceptado por el Comité asesor indicado, como requisito parcial para obtener el grado de Maestría en Administración, por lo que se autoriza su impresión.

A T E N T A M E N T E

PRESIDENTE

MTRA. MARÍA DEL CARMEN ARRIETA LÓPEZ
DOCENTE PTC

SECRETARIO

M.R.I. HUMBERTO ESPINOSA VEGA
DOCENTE PTC

VOCAL

DR. EDGARDO RODRÍGUEZ MORENO
DOCENTE PTC

VOCAL

DRA. MARÍA EUGENIA ESTRADA CHAVIRA
DOCENTE PTC

"2024. Año del Bicentenario de la Erección del Estado Libre y Soberano de México".

CARTA DE CESIÓN DE DERECHOS

En el Estado de México, el que suscribe **ING. JUÁREZ ELIAS EBNER,** estudiante de la Maestría en Administración, adscrito al Tecnológico de Estudios Superiores de Ixtapaluca, manifiesta que es autor intelectual del presente trabajo de Tesis bajo la dirección de la **MTRA. MARÍA DEL CARMEN ARRIETA LÓPEZ** y cede los derechos del trabajo **"MODELO DE NEGOCIO DE UNA CONSULTORÍA EN CIBERSEGURIDAD PARA PROFESIONALES DE IXTAPALUCA Y VALLE DE CHALCO",** al Tecnológico de Estudios Superiores de Ixtapaluca para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, graficas o datos del trabajo sin el permiso del autor y/o director del trabajo. Si el permiso se otorga a algún usuario, deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

Ixtapaluca, Estado de México a 13 de septiembre de 2024.

AUTOR INTELECTUAL

ING. JUÁREZ ELIAS EBNER

"2024. Año del Bicentenario de la Erección del Estado Libre y Soberano de México".

DECLARACIÓN DE AUTENTICIDAD Y DE NO PLAGIO

En el Estado de México, la que suscribe **ING. JUÁREZ ELIAS EBNER,** estudiante de la Maestría en Administración, adscrito al Tecnológico de Estudios Superiores de Ixtapaluca, manifiesta que se responsabiliza por la autenticidad y originalidad del contenido del presente trabajo de Tesis titulado **"MODELO DE NEGOCIO DE UNA CONSULTORÍA EN CIBERSEGURIDAD PARA PROFESIONALES DE IXTAPALUCA Y VALLE DE CHALCO",** el cual ha sido elaborado y presentado para la obtención del grado en la maestría en Administración.

Ixtapaluca, Estado de México a 13 de septiembre de 2024.

AUTOR INTELECTUAL

ING. JUÁREZ ELIAS EBNER

DEDICATORIA

A mis hijos Mateo, Violeta y Fátima, cuya alegría y amor incondicional me han dado la fuerza para seguir adelante en cada momento.

A mi esposa Brenda Vianey, por su constante apoyo, paciencia y comprensión. Gracias por estar siempre presente y por creer en mí incluso en los momentos más difíciles.

A la familia Hernández Miramontes y Juárez Elías, por su apoyo y cariño incondicional. Su presencia ha sido fundamental en este viaje.

Y a las personas que confiaron, gracias por motivarme a demostrar que, con esfuerzo y dedicación, todo es posible.

AGRADECIMIENTO

Quiero expresar mi más profundo agradecimiento a todos mis profesores, quienes han sido una fuente inagotable de conocimiento, inspiración y apoyo durante el posgrado.

Gracias a su dedicación y compromiso, por cada lección impartida y cada consejo brindado. Su paciencia y sabiduría han sido fundamentales para mi crecimiento personal y profesional. A cada uno de ustedes, les debo gran parte de mis logros y éxitos. Su influencia ha dejado una huella imborrable en mi vida, y por ello, siempre estaré agradecido.

A mis amigos Pablo Vera González, Juan Carlos Cisneros Rasgado, Fausto Eduardo Ordoñez Cepeda y Humberto Santiago Cruz, gracias por su amistad incondicional y por estar siempre a mi lado. Su apoyo y compañía han sido esenciales en este viaje, y no podría haberlo logrado sin ustedes.

A mi esposa Brenda Vianey Hernández Miramontes, por su amor, paciencia y constante apoyo. Gracias por estar presente, creer y ser mi mayor fuente de inspiración. Este logro es tanto tuyo como mío.

A mis padres Elvira Elías Martínez y Anastasio Juárez Andrade, por amarme incondicionalmente, sus sacrificios y su guía a lo largo de mi vida. Gracias por enseñarme el valor del esfuerzo y la perseverancia. Este logro es un reflejo de todo lo que me han enseñado.

Índice General

ÍNDICE DE TABLAS.

INDICE DE FIGURAS.

RESUMEN

La humanidad ha estado cada vez más enfocada en mejorar las tecnologías de la información y la comunicación, sin tomarse el tiempo para reflexionar y analizar los desafíos que conlleva el proteger la información.

El desconocimiento en la protección de la información a nivel de operaciones e infraestructura en las actividades de las personas físicas residentes en los municipios de Ixtapaluca y Valle de Chalco, se encuentran totalmente vulnerables a Fraudes por correo electrónico, fraudes de identidad, robo de datos financieros, ransomware, ciber espionaje. Derivado de esta necesidad de especialistas en ciberseguridad se desarrolló la presente investigación con el propósito de responder a la siguiente pregunta de investigación ¿Cuál será la viabilidad económica de una consultoría especializada en ciberseguridad para personas físicas establecidos en los municipios de Ixtapaluca y Valle de Chalco Solidaridad del Estado de México?

Para dar respuesta a pregunta anterior, la presente investigación plantea el desarrollo de un modelo de negocio CANVAS de una consultoría en ciberseguridad para personas físicas de los municipios de Ixtapaluca y Valle de Chalco del Estado de México permitirá un emprendimiento viable de acuerdo con los indicadores financieros.

Para ello se identificaron mediante un cuestionario de 15 preguntas el conocimiento a una muestra de 97 personas sobre temas de ciberseguridad en operaciones e infraestructura en móviles y computadoras, de acuerdo al análisis de los resultados de las encuestas realizadas el consumidor que se encuentra con actividades relacionadas a la educación en un 24.7%, seguido del 23.7% relacionado a las ventas y un 12.4% a la administración, el 25.8% experimento o fue víctima de robo de identidad seguido de un 16.5 % a fue víctima del robo de datos financieros y un 9.3% relacionado fue víctima de fraude por correo electrónico, con base en los resultados se desarrolló del

modelo Canvas centrado en el valor agregado en la asesoría y capacitación de los usuarios de computadoras y móviles.

Se realizo una evaluación de la viabilidad económica del modelo de negocio de la consultoría a personas físicas, dicha evaluación reporta un 48% y una VAN positiva indicando que el negocio es rentable y que el tiempo de recuperación de la inversión de $210,000 es de 2 años 1mes, indicando que existe un mercado potencial con una demanda real para los servicios de asesoría, capacitación y venta de licenciamiento de software, en ciberseguridad para las personas físicas de los municipios de Ixtapaluca y Valle de Chalco.

Palabras clave: Canvas, TIR, VAN, Ciberseguridad, Personas físicas.

ABSTRACT

Humanity has been increasingly focused on improving information and communication technologies, without taking the time to reflect and analyze the challenges involved in protecting information.

The lack of knowledge in information protection at the level of operations and infrastructure in the activities of individuals residing in the municipalities of Ixtapaluca and Valle de Chalco makes them completely vulnerable to email fraud, identity theft, financial data theft, ransomware, and cyber espionage. Due to this need for cybersecurity specialists, this research was developed with the purpose of answering the following research question: What will be the economic viability of a specialized cybersecurity consultancy for individuals established in the municipalities of Ixtapaluca and Valle de Chalco Solidaridad in the State of Mexico?

To answer the previous question, this research proposes the development of a CANVAS business model for a cybersecurity consultancy for individuals in the municipalities of Ixtapaluca and Valle de Chalco in the State of Mexico, which will enable a viable venture according to financial indicators.

For this purpose, a questionnaire with 15 questions was used to identify the knowledge of a sample of 97 people on cybersecurity issues in operations and infrastructure on mobile devices and computers. According to the analysis of the survey results, 24.7% of the respondents are engaged in education-related activities, followed by 23.7% in sales and 12.4% in administration. Additionally, 25.8% experienced or were victims of identity theft, followed by 16.5% who were victims of financial data theft, and 9.3% who were victims of email fraud. Based on these results, a Canvas model was developed, focusing on added value in advising and training computer and mobile users.

An economic viability evaluation of the business model for the consultancy for individuals was conducted. This evaluation reports a 48% and a positive NPV, indicating that the business is profitable and that the investment of $210,000 will be

recovered in 2 years and 1 month. This indicates that there is a potential market with real demand for advisory, training, and software licensing services in cybersecurity for individuals in the municipalities of Ixtapaluca and Valle de Chalco.

Keywords: Canvas, IRR, NPV, Cybersecurity, Individuals.

CAPITULO I: INTRODUCCIÓN

1.1 Situación Problemática.

La humanidad ha tenido la creciente preocupación por mejorar las tecnologías de la información y la comunicación sin realizar una pausa para reflexionar y analizar en las problemáticas como son la confidencialidad de la información, así como las tecnologías que permitirán proteger la información contra las revelaciones no autorizadas.

Exceso de información producida, adquirida y consultada en la última década agregando a esto falta de un control de acceso a esta genera el problema de integridad y veracidad ocasionando problemas en los procesos administrativos o industriales que la mayor parte de las ocasiones afectan a la industria o a terceras personas involucradas en el proceso.

La seguridad de la información debería haber evolucionado con la misma velocidad que la infraestructura, pero lamentablemente siempre se deja de lado el tema de la seguridad informática debido a que, por desconocimiento y cultura informática, erróneamente se piensa que jamás se verán afectados los intereses personales y son las organizaciones quienes tienen que contar con servicios y especialistas en asegurar la información.

En un nivel avanzado la ciberseguridad se enfoca en proteger la infraestructura informática, que incluye servidores, redes y dispositivos. Por otro lado, en el nivel intermedio, la ciberseguridad se centra en salvaguardar los archivos de información en sus diversas formas y estados. En el nivel inicial, se encuentra la seguridad del usuario final el que accidentalmente carga malware u otra forma de ciber amenaza en su equipo de escritorio, laptop o dispositivo móvil. por ello es necesario mantener protegido y actualizado contra los terribles ataques de ingeniería social y phishing, ya que cualquier paso en falso podría ser devastador para sus propios intereses o de una organización.

El entorno del profesional incluye algunos factores como son comunicación con sus pares de forma personal o mediante las redes sociales, la utilización de las redes y dispositivos de comunicación que pueden ser públicas o privadas, los diversos sistemas de software utilizados para realizar sus operaciones, el almacenamiento, procesamiento y transmisión de la información, a lo cual lo vuelve un blanco fácil por el desconocimiento existente por este en cuanto a los temas de seguridad en la información.

Ahora bien, la mayoría de los profesionales por la falta de tiempo y lo complejo que es el tema de seguridad en la información, causa una desconocimiento en las diferentes técnicas utilizadas por los cibercriminales que cabe aclarar que ya no solamente es tener un instalado un antivirus como se acostumbraba en el siglo XX; lo que provoca un aumento de riesgos, amenazas y ataques informáticos sofisticados, y con ello el surgimiento de nuevas formas y técnicas para aprovechar vulnerabilidades de los procesos e infraestructuras. Los riesgos y amenazas que enfrenta un profesional cuando se incorpora al ciberespacio podrían dar lugar a potenciales agresiones contra la dignidad humana, la integridad de las personas, así como a la afectación de la credibilidad, reputación y patrimonio del profesional.

Riquelme (2022) menciona que, en los primeros seis meses de 2022, México experimentó 85,000 millones de ciberataques, lo que representa un aumento del 40% en comparación con 2021 y más de la mitad de los 137,000 millones de ataques registrados en América Latina, según un informe de la empresa de ciberseguridad Fortinet. El ransomware, o secuestro de información, es el tipo de ataque sofisticado más común en México y América Latina. Los países con mayor número de detecciones de ransomware son México, Colombia y Costa Rica, seguidos por Perú, Argentina y Brasil.

El 95% de los incidentes de ciberseguridad comienzan con un proceso de ingeniería social. En este proceso, el atacante busca primero contactar a alguien dentro de una

institución, banco o empresa para obtener la información que necesita, lo que puede resultar en la pérdida de autenticación. (Servín, 2023).

Los incidentes provocados por ciberataques son motivo de alarma, ya que resaltan la necesidad apremiante de contar con especialistas que posean habilidades y conocimientos en seguridad de la información, capaces de brindar servicios al profesional que se enfrenten a los ataques o riesgos antes mencionados.

1.2 Planteamiento del problema.

Con la pandemia, en el año 2020 el mundo se vio obligado a adaptarse a una nueva manera de interactuar, incluyendo la forma de relacionarse con la familia, el estilo de trabajar, el modo de adquirir productos, la forma impartir y tomar clases, entre otras actividades. La pandemia convirtió el uso de las herramientas tecnológicas en una necesidad primordial para continuar con las actividades diarias. Todo esto ocasionó que en pocos meses la cantidad de dispositivos conectados a internet aumentara considerablemente y con ello también, la cantidad de amenazas y riesgos, ya que la sociedad no tuvo tiempo de capacitarse en materia de ciberseguridad.

El desconocimiento en la seguridad de la información a nivel de operaciones e infraestructura en las actividades de las personas físicas de residentes en los municipios de Ixtapaluca y Valle de Chalco, que al no contar con la asesoría especializada en seguridad de la información y con la diversidad de ataques dirigidos a nivel de operaciones e infraestructura en móviles y computadoras de acuerdo, al estudio realizado por la empresa Deloitte (2021), los delitos cibernéticos más comunes que afectan al profesional son: Fraudes por correo electrónico, fraudes de identidad, robo de datos financieros, ransomware, ciber espionaje.

Los fraudes por correo electrónico se llevan a cabo mediante la similitud en las direcciones de correo electrónico, este correo tiene por asunto recepción de facturas o servicios, relacionados a algún supuesto premio, que al momento de abrir el enlace de la supuesta factura se produce el ataque, el cual roba la lista de contactos del destinatario con el fin de reenviar el correo, esto perjudica la reputación y credibilidad del profesional entre sus contactos.

El fraude de identidad es muy frecuente en las redes sociales, se utiliza para extorsionar, publicar información falsa o vender algún producto haciéndose pasar por otra persona, en la mayoría de los casos es posible recuperar el control de la cuenta nuevamente, pero si no se atiende a tiempo los estragos pueden perjudicar la integridad moral hasta física del profesional.

El robo de datos financieros es un delito informático que se da cuando el profesional realiza compras en línea en sitios dudosos, o comparte información bancaria por algún sistema de comunicación como Messenger, Whatsapp, Telegram, Twitter, o incluso cuando realiza compras en línea o presencialmente, actualmente las instituciones financieras están invirtiendo fuertemente en la seguridad de la información de sus clientes, para prevenir este tipo de delitos.

Los ataques de ransomware, es de los más peligrosos porque comprime toda la información del disco duro en un “rar” con una contraseña única que solo el ciber criminal puede o no tener, el ataque se puede llevar a cabo mediante correo electrónico, un mensaje en redes sociales, al reproducir un audio, al ver un video, entre otras; la infección se da de manera aleatoria y es ahí donde radica su peligrosidad.

El ciber espionaje compromete la privacidad del profesional al obtener acceso no autorizado a la información personal confidencial. Esto puede incluir datos como contraseñas, datos bancarios, historial de navegación, comunicaciones privadas, entre otros. Implica la vigilancia y el seguimiento constante de las actividades en línea de los usuarios. Esto puede incluir el monitoreo de correos electrónicos, mensajes instantáneos, llamadas telefónicas, ubicación geográfica, hábitos de navegación, entre otros. Estas prácticas invasivas pueden afectar la libertad y la intimidad de los usuarios.

Por consiguiente, se plantea la pregunta de investigación ¿Cuál será la viabilidad económica de una consultoría especializada en ciberseguridad para personas físicas establecidos en los municipios de Ixtapaluca y Valle de Chalco Solidaridad del Estado de México?

1.3 Justificación

La investigación acerca de la viabilidad económica de una consultoría especializada en ciberseguridad para personas físicas en los municipios de Ixtapaluca y Valle de Chalco Solidaridad del Estado de México surge de la imperante necesidad de salvaguardar a los individuos y profesionales de los riesgos y amenazas cibernéticas que han surgido en el contexto de la pandemia y el notable incremento en la utilización de tecnologías digitales. A continuación, algunos aspectos clave que respaldan la relevancia de esta investigación: Impacto de la Pandemia en el Uso de Tecnología, Crecimiento de Dispositivos Conectados y Riesgos Asociados, Delitos Cibernéticos Comunes, Relevancia de la Viabilidad Económica.

El impacto de la pandemia en el uso de la tecnología debido a la crisis sanitaria de 2020 obligó a la sociedad a adaptarse de manera acelerada a nuevas modalidades de trabajo, estudio y transacciones, generando un aumento significativo en la dependencia de dispositivos conectados a internet. Esta transición rápida dejó a la población expuesta a amenazas cibernéticas debido a la insuficiente capacitación en ciberseguridad.

El crecimiento de dispositivos conectados y los riesgos asociados con el rápido aumento en la cantidad de dispositivos conectados a internet conllevó un incremento proporcional en las amenazas y riesgos cibernéticos. La falta de tiempo para instruir a la población en aspectos de seguridad de la información ha dejado a numerosos individuos vulnerables a posibles ataques y delitos cibernéticos, marca la urgencia de contar con asesoría especializada en ciberseguridad.

Los delitos cibernéticos comunes que afectan a las personas físicas, tales como fraudes por correo electrónico, fraudes de identidad, robo de datos financieros, ransomware y ciberespionaje. Estos incidentes tienen repercusiones negativas tanto en la reputación como en la integridad de los individuos afectados.

La relevancia de la viabilidad económica el presente trabajo busca evaluar la existencia de un mercado potencial y una demanda real para este tipo de servicios en la región, considerando los posibles beneficios económicos para las personas físicas de los municipios de Ixtapaluca y Valle de Chalco.

Esta investigación se fundamenta en la necesidad apremiante de abordar los riesgos cibernéticos emergentes, ofrecer asesoría especializada en ciberseguridad y evaluar la viabilidad económica de implementar soluciones preventivas en los municipios mencionados.

1.4 Hipótesis.

El desarrollo de un modelo de negocio CANVAS de una consultoría en ciberseguridad para personas físicas de los municipios de Ixtapaluca y Valle de Chalco del Estado de México permitirá un emprendimiento viable de acuerdo con los indicadores financieros.

1.4.1 Variable Dependiente.

Las variables dependientes con las que contara el proyecto son las siguientes:

Emprendimiento viable económicamente

Definición conceptual. La viabilidad económica de un emprendimiento se refiere a la capacidad de un proyecto o negocio para generar beneficios y superar los costos asociados a su inversión. En otras palabras, es la evaluación de si la inversión realizada en un proyecto es inferior o igual al retorno esperado a lo largo del tiempo. (Coll Morales & Westreicher, economipedia.com/definiciones-diccionario, 2021).

Los Indicadores de la viabilidad económica son de tipo financiero como: VAN, TIR Y beneficio-costo:

VAN.

Definición conceptual. El Valor Actual Neto (VAN) es un método dinámico de valoración de inversiones. De acuerdo con González (2021) el VAN se basa en los flujos de caja futuros que un proyecto de inversión puede generar. Utiliza una tasa de descuento para convertir esos flujos futuros a su valor presente, permitiendo así sumarlos y luego restar la inversión inicial requerida por el proyecto. La fórmula algebraica para calcular el VAN es la siguiente:

$$VAN = -A + \frac{Q_1}{(1+c)} + \frac{Q_2}{(1+c)^2} + \frac{Q_3}{(1+c)^3} + \cdots + \frac{Q_n}{(1+c)^n}$$

En donde:

A es el valor del desembolso inicial de la inversión

Q_1, Q_2, …, Q_n representa los cash-flows o flujos de caja.

n representa el número de momentos temporales en que se divide el período global considerado de la duración del proyecto.

c es la tasa de descuento.

Para la presente investigación si el resultado de la VAN llegase a tener un valor positivo entonces la propuesta de emprendimiento será rentable de lo contario tendríamos un emprendimiento no viable financieramente.

TIR.

Sevilla Arias (2024) Define la tasa interna de retorno (TIR) es la rentabilidad que ofrece una inversión. Es decir, es el porcentaje de beneficio o pérdida que tendrá una inversión para las cantidades que no se han retirado del proyecto.

La TIR es un elemento crucial para el éxito de una compañía o negocio.

$$VAN = -A + \frac{Q_1}{(1 + C_{TIR})} + \frac{Q_2}{(1 + C_{TIR})^2} + \frac{Q_3}{(1 + C_{TIR})^3} + \cdots + \frac{Q_n}{(1 + C_{TIR})^n} = 0$$

donde: $\mathbf{C_{TIR}}$ es la tasa de descuento que representa la TIR.

A partir de la fórmula de la Tasa Interna de Retorno se deduce que un proyecto es rentable si $C_{TIR} \geq c$, no es rentable si $C_{TIR} < c$ y en el caso de $C_{TIR} = c$ el proyecto es aceptable. Debe tenerse en cuenta que ante dos o más proyectos de inversión alternativos debe elegirse aquel que presente una mayor TIR.

Para la presente investigación si la TIR es mayor o igual a la Tasa de descuento se deduce que tendremos un emprendimiento rentable en caso contrario tendríamos un proyecto no rentable.

BENEFICIO-COSTO

Aguilera Díaz (2007) Define como al análisis del costo-beneficio es un proceso que, de manera general, se refiere a la evaluación de un determinado proyecto, de un esquema para tomar decisiones de cualquier tipo. Ello involucra, de manera explícita o implícita, determinar el total de costos y beneficios de todas las alternativas para seleccionar la mejor o más rentable. Este análisis se deriva de la conjunción de diversas técnicas de gerencia y de finanzas con los campos de las ciencias sociales, que presentan tanto los costos como los beneficios en unidades de medición estándar

usualmente monetarias para que se puedan comparar directamente. La técnica del costo-beneficio se relaciona de manera directa con la teoría de la decisión. Pretende determinar la conveniencia de un proyecto a partir de los costos y beneficios que se derivan de él. Dicha relación de elementos, expresados en términos monetarios, conlleva la posterior valoración y evaluación.

1.4.2 Variable Independientes

Las variables independientes con las que contara el proyecto son las siguientes:

1.4.2.1 Modelo de negocio CANVAS de Osterwalder y Pigneur.

El modelo Canvas, es una herramienta visual utilizada para diseñar analizar y describir los modelos de negocio. El modelo de negocio CANVAS se compone de 9 módulos que son:

1. Segmentación de mercado. Este módulo se indicará sobre el conocimiento de las necesidades en ciberseguridad de las personas físicas.
2. Propuesta de Valor. Este módulo se medirá de acuerdo con la satisfacción de la necesidad en ciberseguridad de las personas físicas
3. Canales de Distribución La medición del módulo se medirá de acuerdo con la preferencia de las personas físicas para la comunicación, distribución y venta de los servicios o productos ofertados.
4. Relación con el cliente. Para medir este módulo es necesario evaluar la experiencia y preferencia del cliente al solicitar un servicio de ciberseguridad
5. Fuentes de ingreso. La medición de este módulo dependerá del valor que esté dispuesto a pagar y el cómo les gustaría pagar a la persona física por un servicio o producto relacionado a la ciberseguridad.
6. Recursos Clave. Se medirán de acuerdo con lo requerido en los módulos anteriores referentes a canales de distribución, propuesta de valor, fuentes de ingresos y relación con los clientes.
7. Actividades Clave. Se medirán de acuerdo con las actividades clave en los módulos anteriores referentes a fuentes de ingresos, relación con los clientes, propuesta de valor, y canales de distribución.

8. Socios clave. Se determinará la cantidad de artículos o servicios que se puedan adquirir con otros proveedores en ciberseguridad para aumentar la capacidad de servicios y reducir costes
9. Estructura de costos. Este módulo se evaluará la relación entre coste y valor, para las personas físicas de Ixtapaluca y Valle de Chalco

1.5 Objetivos

1.5.1 Objetivo general

Desarrollar un modelo de negocios de una consultoría en ciberseguridad para personas físicas de los municipios de Ixtapaluca y Valle de Chalco del Estado de México.

1.5.2 Objetivos específicos

1. Identificar el conocimiento de las personas físicas en ciberseguridad en operaciones e infraestructura en móviles y computadoras.
2. Desarrollar el modelo Canvas centrado en el valor agregado en operaciones e infraestructura de móviles y computadoras.
3. Realizar una evaluación de la viabilidad económica del modelo de negocio en la consultoría a personas físicas en operaciones e infraestructura.

1.6 Alcance y delimitación de la investigación.

La presente investigación se llevará a cabo en los municipios de Valle de Chalco e Ixtapaluca, ubicados en la zona oriente del Estado de México, como una propuesta de negocio, por la escasez de este tipo de servicios en la región y la oportunidad que esto ofrece a las personas físicas.

El proyecto estará enfocado en un inicio en atender a las personas físicas, debido a que estos se encuentran sin acceso a un servicio de ciberseguridad debido al aumento de delitos en línea como robo de identidad, robo de información personal o financiera.

La consultoría de ciberseguridad impacta en la implementación de técnicas específicas que permiten prevenir, proteger y mejorar el rendimiento de los flujos de información en las personas físicas. No solo se avocará al asesoramiento, también incluye la revisión de sistemas, implementa medidas de seguridad y elabora planes de acción. Contribuirá en la protección de equipos, aplicaciones de software, sistemas críticos y datos posibles de amenaza digital. Tiene la responsabilidad de resguardar los datos para conservar la confianza del cliente con el cumplimiento de la normativa.

La presente investigación tiene un tiempo para su desarrollo, el cual se refleja en la Tabla1 Diagrama de Gantt.

Tabla 1

Diagrama de Gantt

Actividad	Semestre 1	Semestre 2	Semestre 3	Semestre 4
Desarrollo del capítulo 1	X			
Desarrollo del capítulo 2	X	X		
Desarrollo del capítulo 3		X	X	
Análisis de resultados y conclusiones			X	X
Presentación del proyecto final				X

Nota: la presente tabla muestra el tiempo en que de desarrollaran las diferentes actividades del proyecto de investigación.

El límite sustantivo de la investigación será explorado desde la perspectiva de la administración, con un enfoque específico en la fase inicial de la etapa de planificación. En este contexto, se analizará la viabilidad del emprendimiento en el campo de la consultoría, utilizando el modelo de negocios Canvas como herramienta principal de análisis y diseño estratégico.

CAPITULO II: MARCO TEÓRICO

2.1 Antecedentes de la investigación.

Se realizo revisión documental de diferentes investigaciones relacionadas con la creación de consultorias de ciberseguridad, a continuacion se muestran los antecedentes encontrados sobe el tema.

Guevara Jurado, (2022) en su trabajo titulado “El Hacking Ético como Servicio Conexo de Consultoría en Seguridad por parte de las Empresas de Seguridad Privada” indica que la tecnología y la digitalización de las actividades cotidianas habían estado avanzando rápidamente en los últimos años, pero debido a la pandemia, este progreso se aceleró a niveles inimaginables, lo que resultó en el aumento y evolución de los ciberdelitos. Por lo tanto, es esencial que los servicios de seguridad privada también evolucionen y sean capaces de responder a los nuevos desafíos y requisitos de la era digital en la nueva normalidad. El hacking ético es una disciplina que las empresas de seguridad privada pueden incorporar en sus servicios de consultoría para enfrentar las demandas actuales en materia de ciberseguridad.

Con base en lo anterior, el objetivo general del trabajo de Guevara Jurado, (2022) es diseñar un producto de seguridad privada a nivel de consultoría que utilice el hacking ético como estrategia para diagnosticar un sistema de gestión de seguridad de la información (SGSI). Para lograrlo, se plantean los siguientes objetivos específicos: primero, establecer el estado actual de los riesgos en entornos digitales; segundo, identificar los fundamentos del hacking ético que permitan detectar brechas o vulnerabilidades en los sistemas informáticos; y por último, caracterizar los componentes de un servicio de consultoría de hacking ético para incluir en los portafolios de empresas de vigilancia y seguridad privada.

La pandemia dejo un avance y evolución exponencial en los ciberdelitos al grado que los servicios de seguridad privada se vean afectados e incluso se involucren en resolver o prevenir este tipo de delitos en la era digital evolucionada por la pandemia. Disciplinas como el hacking ético se proponen como una estrategia para el portafolio de los servicios ofrecidos por las empresas dedicadas a brindar el servicio de

seguridad privada, como estrategia para mantenerse a la vanguardia y exigencias del mercado.

El robo de identidad es uno de los delitos en línea que ha crecido más rápidamente. No obstante, la identidad también está en riesgo por medio de materiales cotidianos como el currículum vitae, la dirección de tu casa, las fotos y videos en redes sociales, y los datos financieros.

En el trabajo de tesis de Alexandra, (2021) titulado "*Diseño de un modelo de negocio para ofrecer servicios de seguridad de la información a pymes del sector salud en Bogotá*" resume que la protección de la información busca resguardarla de posibles daños por divulgación y uso no autorizado; ha ganado importancia con el aumento en el uso de datos digitales, las tecnologías de la información (TICs), la interconexión para la comunicación, negociación y prestación de servicios; así como en eventos disruptivos, como la actual pandemia. En el sector de servicios de salud, esto es especialmente relevante debido al uso de información médica, considerada confidencial y sensible, cuya divulgación no autorizada puede afectar a las personas y su integridad física y psicológica.

Aunque existen regulaciones destinadas a proteger el derecho fundamental a la privacidad y a prevenir estigmas sociales relacionados con enfermedades, el sector salud aún no otorga la importancia necesaria a la protección de estos datos, que son atractivos para los delincuentes debido a su valor en el mercado ilegal. Además, las condiciones económicas y la falta de conocimiento agravan esta situación en las pequeñas y medianas empresas (Pymes), ya que enfrentan desafíos al implementar controles para proteger la información de usuarios y pacientes.

Este trabajo tiene como objetivo identificar los factores que pueden influir en la implementación de la seguridad de la información en las Pymes del sector salud en la ciudad de Bogotá y propone un modelo de negocio basado en el Canvas de

Osterwalder & Pigneur (2011). Para ello, se realiza una revisión de la literatura entre los años 2000 y 2020 relacionada con el tema.

La economía y el desconocimiento en temas de ciberseguridad, pone en riesgo la información e identidad de los pacientes, violando el derecho a la privacidad de sus datos que se encuentra establecido en las leyes del sector salud de Bogotá. Derivado de esto la autora propone el diseño de un modelo de negocio basado en el Canvas de Osterwalder & Pigneur (2011) para pymes del sector salud de Bogotá.

En una entrevista realizada por la revista Advocatus al especialista en José Álvaro Quiroga León, (2021) en la pregunta 1. Tras el aumento de las transacciones en línea durante el 2020, ¿Qué medidas deben emplear las entidades financieras y comerciales para garantizar la seguridad de sus usuarios? Efectivamente, la situación de emergencia sanitaria ha limitado nuestra movilización y con ello disminuyen nuestras actuaciones presenciales y aumentan las actividades en línea. Ello ha hecho visible la necesidad de seguridad en este tipo de actividades, pero los riesgos ni son nuevos ni están limitados a entidades financieras o comerciales.

Continúa explicando José Álvaro Quiroga León, el crecimiento explosivo de actividades en línea y los servicios en los que su uso es masivo son un indicador de la importancia de la protección de la información en general y de la información personal en particular, pero también los servicios no masivos requieren de medidas de protección. Pensemos en el psicólogo, el médico particular, el cirujano plástico o el abogado y en la información sensible que manejan, aun sin ser masiva ni comercial. Ciertamente, regresando al tema, la masividad es un elemento de complejidad que debe ser atendido, además, porque en el entorno financiero o comercial el tratamiento inadecuado de la información personal de los clientes tendrá gran repercusión reputacional, más allá de las contingencias administrativas sancionadoras.

Por eso, la primera medida que se debe tomar es comprender que la responsabilidad sobre la información de los clientes no es solo un tema de cumplimiento normativo o

sólo un tema tecnológico, es un tema que atañe al “diseño del negocio”, que lejos de ser un sobre costo o el efecto de una regulación incómoda, es un valor que puede ser sumado a la empresa.

De acuerdo con León,(2021) en lo anteriormente explicado en esta primera parte de la entrevista menciona a los servcios no masivos y la necesidad de tener medidas de proteccion de la informacion sensible que poseen y manejan los profesionistas y si esta informacion no es protegida de forma adecuada existe una repercusion en la reputacion del profesionista, ademas de las administrativas y legales. La informacion del cliente es de suma importancia.

En el articulo de Ciberseguridad: Por donde empezar de Medina,(2021) señala que la Ciberseguridad no se trata de hardware, software y personas certificas, este concepto va más allá de una mirada a un conjunto de protocolos, cumplimiento de normas o seguimiento de buenas prácticas. Entonces se debe entender de una manera sistémica que los ciber delicuentes dentro del sistema informatico buscaran el elemento más vulnerable de la organización. Toma sentido pensar que la capacitación y la concientización de todos los miembros de la organización ayudarán considerablemente a soportar las vulnerabilidades que se puedan dar en una organización. Se debe de iniciar por la capacitación de creación de claves seguras, manejo y actualización de los sistemas operativos de los equipos de casa y de oficina, el correcto uso del correo de la organización y el personal, el aseguramiento de las redes que se crean, son de los pequeños detalles que fortalezcan parte de la seguridad de informacion y sistemas dentro y fuera de la organización.

En su trabajo MOLINA, (2021) indica que la propuesta de implementación estratégica de servicios de ciberseguridad basado en el sistema de niveles de madurez CMMI y los objetivos de control de la normativa ISO 27002 parte desde la ejecución del servicio de evaluación de seguridad del cual se obtiene un análisis GAP que permite identificar brechas y puntos específicos donde se requiere generar controles y mejoras que

mitiguen los riesgos cibernéticos ofreciendo el beneficio a los clientes de priorizar sus recursos de seguridad en las áreas de mayor criticidad.

En los trabajos anteriores se comienzan ya a formular algunos planes o modelos de negocios entorno a la seguridad de los sistemas informaticos de la industria, algunos trabajos poco hablan sobre la seguridad de los sistemas de información que estan fuera de la organización como los son las computadoras o celulares personales que utilizan los profesionales para realizar sus actividades del dia a dia, que en ocasiones ocupan la infraestructura tecnologica de la empresa para mantenerse comunicados

2.2 Marco histórico

2.2.1 Antecedentes de la consultoría

La consultoría, como disciplina estratégica y de gestión, ha evolucionado a lo largo del tiempo, influenciada por diversos factores históricos y socioeconómicos. Martínez (2012) en su trabajo titulado “Implementación de una nueva metodología para el modelado de procesos de negocio aplicada en una casa consultora enfocada a las tecnologías de información” menciona que el proceso de la consultoría tiene sus orígenes en la Revolución Industrial, siendo esta época donde se realizaron grandes avances tecnológicos, principalmente dentro de los talleres de producción; y por medio de la industrialización se establecieron las primeras líneas de producción, lo cual provocó la necesidad de implementar métodos y procedimientos sistemáticos que ayudaran a aumentar la productividad y eficiencia de las empresas; seguida por la necesidad de mejorar las relaciones entre los individuos miembros de la organización.

Durante el auge de la Revolución Industrial (siglo XIX) se inició la organización científica del trabajo con las aportaciones de Frederick Taylor, Frank Gilbreth, Henry Gantt y Harrington Emerson, dando empuje a la consultoría como una forma de incrementar la productividad y la eficiencia de las fábricas y talleres, a través de la disminución de los costos, tiempos y movimientos. Frederick Taylor realizó un estudio

de las condiciones y métodos de manufactura en los patios de acarreo de la Bethelem Steel Company, con el objetivo de resolver los problemas de eficiencia de las líneas de producción.

Con el paso del tiempo y gracias a las aportaciones de Taylor surgieron otros investigadores como Frank Gilbreth, quién junto con su esposa Lillian, en su obra “La ciencia de la administración enfocada a la mejor forma de realizar el trabajo”, hace referencia a que el adelanto y mejoramiento de los sistemas jamás condujo a la mejor forma de realizar el trabajo, sin embargo a través de sus estudios de tiempos y movimientos ayudo a los trabajadores a emplear su capacidad de producción, volviendo eficientes los movimientos, publicando su primer artículo denominado “Estudio de movimiento”. Las experiencias desarrolladas tanto en el campo administrativo como en el de la Ingeniería Industrial se replicaron de una organización a otra e inclusive a otras áreas del conocimiento; así qué a principios del siglo XX aparece la figura del consultor como el profesional que ayuda a la solución de problemas y como un facilitador del proceso de aprendizaje.

2.2.2 Historia modelo de negocio canvas

El modelo de negocio Canvas o de lienzo fue creado por Alexander Osterwalder en su tesis doctoral en 2004, donde propone una ontología que se compone de nueve bloques y unas reglas de interrelaciones entre ellos. Esta es una herramienta que facilita y da claridad sobre las actividades de diseño, evaluación e innovación de modelos de negocio, tanto por su carácter holístico como por la sencillez en la que expresa sus conceptos.

2.3 Base Teóricas

2.3.1 Administración.

Para comprender la administración de manera integral, es fundamental explorar su evolución histórica, examinar los acontecimientos relevantes en situaciones comparables del pasado y establecer conexiones con experiencias y conocimientos contemporáneos. Por tanto, conocer el origen y desarrollo histórico de la administración adquiere una relevancia crucial.

2.3.1.1 Conceptos de administración

La administración, como disciplina fundamental en el ámbito empresarial y organizacional, ha sido objeto de estudio y reflexión a lo largo de la historia. En el artículo "Origen y Desarrollo de la Administración", publicado en la revista Perspectiva, (2007), este estudio ofrece los siguientes conceptos:

- “Administrar es prever, organizar, dirigir, coordinar y controlar a través de la gerencia”. (Henri Fayol).
- “La Administración es una ciencia social que persigue la satisfacción de objetivos institucionales por medio de una estructura y a través del esfuerzo humano coordinado.” (José Antonio Fernández Arena).
- “La Administración es el conjunto sistemático de reglas para lograr la máxima eficiencia en las formas de estructurar y manejar un organismo social”. (Agustín Reyes Ponce). Este autor añade que la Administración es la técnica de la coordinación de las cosas y personas que integran una empresa.

Por otro lado Münch Lourdes en su libro “Administración. Gestión organizacional, enfoques y proceso administrativo” señala el siguiente concepto de administración:

“La administración es un proceso a través del cual se coordinan y optimizan los recursos de un grupo social con el fin de lograr la máxima eficacia, calidad, productividad y competitividad en la consecución de sus objetivos.” (Lourdes, 2010).

La administración es una disciplina esencial en todo tipo de organización, siendo incluso considerada como el método más eficiente para asegurar su competitividad.

2.3.1.2 Características de la disciplina administrativa

La administración posee ciertas características que la diferencian de otras disciplinas, según lo planteado en "Administración: Gestión Organizacional, Enfoques y Proceso Administrativo" de Münch Lourdes, (2010):

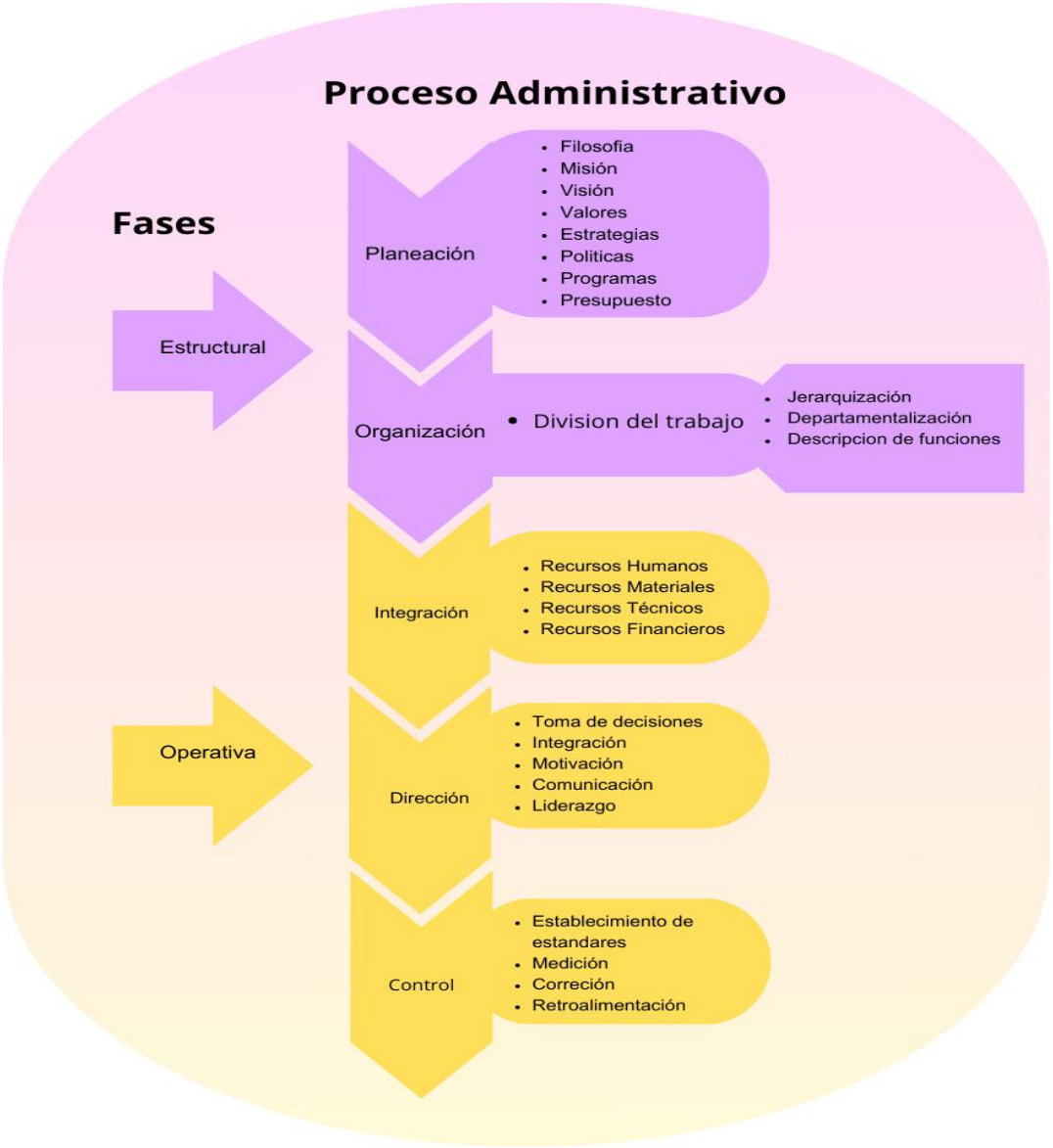
- Universalidad: Se destaca su indispensable aplicación en cualquier grupo social, sea una empresa pública o privada, así como en cualquier tipo de institución.
- Valor instrumental: Se reconoce su enfoque eminentemente práctico, considerándola como un medio para alcanzar los objetivos de un grupo.
- Multidisciplinar: La administración se beneficia de conocimientos provenientes de varias ciencias y técnicas, lo que la convierte en un campo interdisciplinario.
- Especificidad: A pesar de su relación con diversas ciencias, la administración tiene un ámbito de acción específico, lo que la distingue claramente de otras disciplinas.
- Versatilidad: Los principios administrativos son flexibles y se adaptan a las necesidades particulares de cada grupo social donde se aplican, lo que le confiere una gran versatilidad y capacidad de adaptación.

2.3.1.3 Proceso administrativo.

El proceso administrativo, considerado la metodología fundamental para aplicar cualquier enfoque de gestión o administración, requiere para la implementación de nuevas corrientes administrativas. A continuación, se ofrece un resumen de las etapas, fases, elementos y principios que integran dicho proceso. Como se puede observar en la figura 1. Fases y elementos del proceso.

Figura 1

Fases, elementos del proceso administrativo



Nota: Diagrama de proceso administrativo.

2.3.2 Modelo de negocios

En el libro Business Model Generation de Osterwalder y Pigneur, (2009) se describe un modelo de negocios como la forma racional en la que un negocio crea el valor a través de la creación y la entrega. El modelo Canvas, también conocido como Business Model Canvas o lienzo de modelo de negocio, es una herramienta visual

utilizada para describir, analizar y diseñar modelos de negocio. (Osterwalder & Pigneur, 2009).

El modelo Canvas consta de nueve bloques o componentes clave que representan los aspectos fundamentales de un modelo de negocio. Estos bloques son los siguientes:

1. Segmentos de clientes: Se refiere a los diferentes grupos de personas o empresas a los que se dirige el negocio.
2. Propuesta de valor: Describe el conjunto de productos o servicios que se ofrecen a los clientes y cómo se diferencian de la competencia.
3. Canales: Representa los medios utilizados para llegar a los clientes y entregarles la propuesta de valor.
4. Relación con los clientes: Describe el tipo de relación que se establece con los clientes, ya sea personalizada, automatizada, a través de comunidades, etc.
5. Fuentes de ingresos: Son las diferentes formas en las que el negocio genera ingresos a través de la venta de productos, servicios, suscripciones, publicidad, entre otros.
6. Recursos clave: Son los activos necesarios para hacer funcionar el modelo de negocio, como infraestructura física, tecnología, capital humano, entre otros.
7. Actividades clave: Son las acciones o tareas principales que se realizan para que el modelo de negocio funcione correctamente.
8. Alianzas clave: Representa las colaboraciones o asociaciones estratégicas con otras empresas u organizaciones que son fundamentales para el éxito del negocio.
9. Estructura de costos: Describe los costos asociados con la operación del negocio, incluyendo costos fijos, variables, de personal, de marketing, entre otros.

El modelo Canvas proporciona una visión general del negocio de forma concisa y permite identificar las interrelaciones entre los diferentes componentes. Es una

herramienta flexible y se puede utilizar tanto para diseñar nuevos modelos de negocio como para analizar y mejorar modelos existentes.

2.3.3 Viabilidad económica

Coll Morales, (2021) menciona en el artículo titulado “Viabilidad económica” que existe viabilidad económica cuando, tras un riguroso análisis económico y financiero, observamos que la inversión que un día llevamos a cabo es inferior al retorno que, a lo largo del tiempo, esperamos obtener por haberla realizado. Es decir, cuando el coste de la inversión es superado por el beneficio que esta genera, reflejándose en un análisis de viabilidad.

Este análisis, dado que nos dice si el proyecto dará pérdidas o ganancias, nos dirá si la inversión que vamos a acometer es la inversión correcta. Es decir, si debemos invertir en ese proyecto o, por el contrario, y ante un análisis que nos muestra que el proyecto no es viable, debemos optar por otro proyecto, u otro activo.

Habitualmente, cuando queremos saber si un proyecto es viable o no económicamente hablando, atendemos a ratios como el VAN o la TIR. En ocasiones, realizamos el clásico análisis costo-beneficio. No obstante, debemos saber que esta viabilidad económica viene determinada, también, por otros factores. Entre estos factores podemos destacar aspectos legales, como la regulación del mercado, o incluso factores relacionados con la competencia, pudiendo determinar la viabilidad la propia competencia dentro del mercado.

De acuerdo con Pérez, (2021) el estudio de viabilidad no solo minimiza riesgos, sino que también:

- Identifica limitaciones y supuestos.
- Descubre oportunidades.
- Estudia el funcionamiento actual de la organización.
- Concreta los necesidades del proyecto.

- Valora distintas alternativas.
- Facilita el acuerdo sobre la línea de acción.
- Define claramente el problema o la oportunidad de negocio.
- Establece el ámbito de aplicación de manera precisa para evitar confusiones.
- Informa sobre la estructura y partes de la empresa, incluyendo los participantes del proyecto y las áreas afectadas.
- Proporciona una perspectiva completa de las alternativas.
- Descubre nuevas oportunidades de negocio o formas de optimizar resultados.
- Identifica oportunidades de innovación a través de la investigación.
- Detecta señales de advertencia sobre la viabilidad del proyecto.
- Aumenta la probabilidad de éxito al identificar factores que podrían afectar el proyecto.
- Proporciona información de calidad para decisiones basadas en datos objetivos.
- Ofrece documentación completa fruto de una investigación exhaustiva.
- Asegura la financiación de instituciones de crédito y otras fuentes.
- Atrae inversión de capital.
- Facilita la introducción de cambios necesarios.
- Permite establecer directrices aplicables a futuros proyectos, lo que puede ahorrar tiempo y dinero significativamente.
- Debe utilizarse como una guía y no como una llamada a la acción inmediata, por lo que sus conclusiones deben integrarse en la planificación y no tomarse como prioridades urgentes.
- Es esencial evaluar las diferentes alternativas de solución para cada problema.
- Se considera la adecuación del uso de las estructuras existentes y de las alternativas.
- Se establecen prioridades basadas en su pragmatismo y viabilidad.
- Comienza con un análisis del costo total estimado del proyecto.
- También se calcula el costo de otras alternativas, además de la solución recomendada, para ofrecer una comparación económica.

- Es recomendable complementarlo con un programa de proyecto que muestre la ruta del proyecto y las fechas de inicio y finalización de las actividades.
- Concluye con el cálculo del costo total, aspecto crucial para determinar la viabilidad del proyecto.
- A este cálculo se le añade un resumen de los costos y una evaluación basada en un análisis de costo-beneficio y la rentabilidad de la inversión.
- Justifica el rigor y la precisión del estudio de viabilidad.
- Permite tomar una decisión sobre el proyecto.
- Permite comprender mejor el sistema y los mecanismos de desarrollo de cada producto.

2.3.3.1 Tasa mínima aceptable de rendimiento

Baca Urbina, (2013), en su libro titulado “Evaluacion de proyectos” en su septima edicion menciona en su apratado de Costo de capital o tasa minima aceptable de rendimiento (TMAR) la define como:

$$TMAR = i + f + if$$

$donde$:

$i = premio\ al\ riesgo$;

$f = inflación$

La TMAR que un inversionista exigiría a una inversión se calcula sumando dos componentes: primero, la ganancia debe compensar los efectos de la inflación y, segundo, debe incluir una prima por el riesgo asumido al invertir. Al evaluar un proyecto con un horizonte temporal de cinco años, la TMAR calculada debe ser válida tanto en el momento de la evaluación como durante todo el horizonte.

Para calcular la TMAR, se debe utilizar el promedio del índice de inflación proyectado para los próximos cinco años. Estas proyecciones pueden obtenerse de diversas fuentes, tanto nacionales (como el Banco de México) como internacionales (como

Ciemex-Wefa y otras). Generalmente, se considera que un premio al riesgo vista como la tasa de crecimiento real del dinero invertido después de ajustar por inflación, debe estar entre el 10% y el 15%. Sin embargo, esto no es completamente satisfactorio, ya que el valor del premio debe depender del riesgo específico de cada inversión, y cada inversión tiene sus propias características.

Baca Urbina, (2013), da el siguinete ejemplo:
Para realizar un proyecto se pretende un capital de $20, 000, 000. Los inversionistas aportan 50%, otras empresas aportan 25%, y el banco aporta el 25% restante.

Las tasas mínimas de cada uno son:
Inversionistas:

$$Inversionistas: TMAR = 12\%\ inflación + 10\%\ premio\ al\ riesgo + 0.12\ \times 0.1 = 0.232$$

$$Otras\ empresas: TMAR = 12\%\ inflación + 12\%\ premio\ al\ riesgo + 0.12 \times .12 = 0.2544$$

$$Banco\ TMAR = 25\%$$

La tasa mínima aceptable de rendimiento que los inversionistas y otras empresas que aportan capital exigen es muy similar, ya que consideran la inversión desde una perspectiva privada. Para su horizonte de planeación de cinco años, buscan compensar la inflación, y han calculado que el índice inflacionario promedio para ese periodo es del 12%. La prima de riesgo de las otras empresas es ligeramente superior (dos puntos porcentuales) a la exigida por los inversionistas mayoritarios, lo cual es habitual, ya que el financiamiento privado siempre resulta más costoso que el bancario. La TMAR bancaria se refiere simplemente al interés que una institución financiera cobra por otorgar un préstamo, y en este caso, se asume una tasa de interés preferencial. Con esta información, se puede determinar la TMAR del capital total, calculándola mediante una ponderación del porcentaje de contribución y la TMAR requerida por cada parte.

$Accionista$	$\%\ aportacion$		$TMAR$		$Ponderación$
$Inversionista\ privado$	0.50	$\times$	0.232	$=$	0.116
$Otras\ empresas$	0.25	$\times$	0.2544	$=$	0.0636
$Instituciones\ financieras$	0.25	$\times$	0.25	$=$	0.0625
			$TMAR\ global\ mixta$	$=$	0.2421

La Tasa Mínima Aceptable de Retorno (TMAR) del capital total de $20,000,000 resultó ser del 24.21%. Esto significa que la empresa debe obtener al menos este rendimiento para poder pagar un 23.2% de interés sobre los $10,000,000 aportados por los inversionistas mayoritarios, un 25.44% de interés sobre los $5,000,000 aportados por otras empresas, y un 25% de interés sobre la contribución bancaria de $5,000,000. Esto ilustra claramente por qué se le llama TMAR. Si la empresa no logra un rendimiento del 24.21% (el mínimo necesario para operar), no podría cubrir el pago de intereses a los otros accionistas ni su propia TMAR, de ahí su denominación como tasa mínima aceptable.

La TMAR se basa en varios factores, como el costo de oportunidad de los fondos invertidos, el riesgo asociado con la inversión y las expectativas de los inversores. Representa el rendimiento mínimo que los inversores esperan obtener para compensar el riesgo asumido y renunciar a otras oportunidades de inversión.

Al evaluar proyectos de inversión, se comparan los rendimientos esperados con la TMAR. Si el rendimiento esperado es igual o superior a la TMAR, se considera que la inversión es viable y puede generar beneficios suficientes para compensar el riesgo. Si el rendimiento esperado es inferior a la TMAR, es posible que se rechace la inversión.

En conclusión, la TMAR es la tasa mínima de rendimiento que una inversión debe alcanzar para ser considerada aceptable y justificar el uso de los recursos invertidos.

2.3.3.2 Valor Presente Neto o Valor Actual Neto

Baca Urbina, (2013) define el valor presente neto como la suma de los flujos descontados en el presente y restar la inversión inicial equivale a comparar todas las ganancias esperadas contra todos los desembolsos necesarios para producir esas ganancias, en términos de su valor equivalente en este momento o tiempo cero. Es claro que para aceptar un proyecto las ganancias deberán ser mayores que los desembolsos, lo cual dará por resultado que el VPN sea mayor que cero. Para calcular el VPN se utiliza el costo de capital o TMAR.

La VAN, o Valor Presente Neto (VPN), es una herramienta utilizada en finanzas para evaluar la viabilidad y rentabilidad de un proyecto o inversión. Representa la diferencia entre los flujos de efectivo generados por un proyecto y el costo inicial de la inversión, descontados al valor presente.

La ecuación para calcular el VPN para el periodo de cinco años es:

$$VPN = -P + \frac{FNE_n}{(1+i)^n}$$

El cálculo de la VAN implica determinar los flujos de efectivo futuros esperados del proyecto, teniendo en cuenta los ingresos y gastos proyectados a lo largo de su vida útil. Estos flujos de efectivo se descuentan utilizando una tasa de descuento apropiada, que refleja el costo de oportunidad de los fondos y el riesgo asociado al proyecto. El descuento se realiza para reflejar el valor del dinero en el tiempo, considerando que un dólar recibido en el futuro vale menos que un dólar recibido hoy.

Si la VAN de un proyecto es positiva, significa que los flujos de efectivo futuros, descontados al valor presente, superan el costo inicial de la inversión. Esto indica que el proyecto tiene un potencial de generación de valor y se considera favorable. Por el contrario, si la VAN es negativa, indica que los flujos de efectivo esperados no son suficientes para recuperar la inversión inicial y se considera desfavorable.

En resumen, la VAN es una medida utilizada para evaluar la rentabilidad de un proyecto al considerar el valor temporal del dinero y el riesgo asociado. Ayuda a los inversores y empresas a tomar decisiones informadas sobre la asignación de recursos y la selección de proyectos.

2.3.3.3 TIR

Sevilla Arias (2014) en el articulo titulado “Tasa interna de retorno (TIR): ¿Qué es y cómo se calcula?**”** define a la tasa interna de retorno (TIR) como la rentabilidad que ofrece una inversión y se mide en porcentaje sobre la inversión realizada.

La Tasa Interna de Retorno (TIR) es la tasa de descuento que, en el momento inicial, iguala los cobros futuros con los pagos, resultando en un Valor Actual Neto (VAN) igual a cero. Por esta razón, para calcularla, es necesario conocer los flujos de caja que se generarán con la inversión. Una vez que se tiene una previsión completa de los cobros, despejamos la TIR para determinar el tipo de interés mínimo necesario para que la inversión no genere ninguna rentabilidad. Que se expresa de acuerdo a la siguiente formula matematica:

$$TIR = I_0 - \sum_{t=1}^{n} \frac{f_t}{1 + (r)^t} = 0$$

Donde:

f_t son los flujos de dinero en cada periodo t.

I_0 es la inversión realiza en el momento inicial (t = 0)

n es el número de periodos de tiempo.

r es la tasa de descuento

Cuando la Tasa Interna de Retorno (TIR) es superior a cero, significa que el proyecto generará ganancias. En cambio, si la TIR es negativa, es mejor evitarlo, ya que resultará en pérdidas económicas.

2.3.3.4 Beneficio/Costo

Aguilera Díaz (2007) Define el análisis del costo-beneficio como un proceso que, de manera general, se refiere a la evaluación de un determinado proyecto, de un esquema para tomar decisiones de cualquier tipo. Esto implica, de manera explícita o implícita, calcular el total de costos y beneficios de todas las opciones para elegir la más rentable. Este análisis combina diversas técnicas de gestión y finanzas con las ciencias sociales, presentando tanto los costos como los beneficios en unidades de medida estándar, generalmente monetarias, para permitir una comparación directa.

Inicialmente, este método se aplicó en proyectos sociales con apoyo gubernamental, cuando no era necesario que las inversiones del gobierno fueran rentables económicamente, de ahí su nombre de costo-beneficio. Para aprobar un proyecto de inversión, el cociente debía ser uno, lo que significaba que solo era necesario recuperar los costos incurridos, sin necesidad de rentabilidad económica. Con el tiempo y la escasez de recursos económicos del gobierno, este criterio cambió, y ahora todos los servicios gubernamentales tienen un costo. Aunque los proyectos de inversión gubernamentales para beneficio social no deben ser lucrativos como los proyectos privados, tampoco se espera que el gobierno invierta sin obtener alguna retribución monetaria. Actualmente, el objetivo del gobierno en sus inversiones es no solo recuperar la inversión realizada, sino también obtener una ganancia que al menos compense los efectos de la inflación.

Formalmente, si la inflación es del 5% anual, tanto los costos como los beneficios económicos obtenidos a lo largo del tiempo deben descontarse a esa tasa para traerlos a valor presente. Solo se deben aceptar proyectos de inversión con una relación costo-beneficio menor a uno, o dicho de otra manera, que la relación beneficio-costo sea mayor o igual a uno, lo que significa que los beneficios siempre superan a los costos. Para proyectos de inversión privada, la determinación del Valor Presente Neto (VPN) y la Tasa Interna de Retorno (TIR) son definitivamente los indicadores clásicos de rentabilidad económica.

2.3.4 Consultoría

El autor Martínez Valencia, (2012) se describe la consultoría como un servicio que se encarga de identificar e investigar problemas relacionados con las políticas, procedimientos y métodos dentro de las organizaciones. Su objetivo es mejorar el funcionamiento de estas mediante el desarrollo y la asistencia en la implementación de planes de acción adecuados.

2.3.4.1 Consultor

Un consultor es, básicamente, alguien que ofrece asesoramiento o brinda servicios de carácter profesional o semiprofesional a cambio de una compensación. (Cohen, 2003)

El consultor puede desempeñar distintos roles:

a) Consultor de recursos: En este rol, el consultor ofrece principalmente un servicio especializado, actuando como asesor experto en un área específica.
b) Consultor de procesos: En este rol, el consultor asiste al cliente en la percepción, comprensión y acción sobre los procesos que se desarrollan en su entorno, con el objetivo principal de fomentar cambios.

2.3.4.2 Clasificación de la consultoría

Martínez Valencia, (2012) menicona que las consultorías se pueden clasificar según su alcance en:

a) Integrales: Implican cambios en toda la organización, considerando todos los procesos y subsistemas. Es común hablar de consultoría integral colaborativa, una de las más frecuentes hoy en día.
b) Parciales: Se enfocan en procesos de cambio o asesoría en uno o varios subsistemas o procesos específicos de la organización.

Independientemente del alcance, es crucial recordar que la organización es un sistema. Cualquier cambio debe considerar su impacto en el resto del sistema, ya que optimizar partes individuales rara vez optimiza el sistema completo.

Según las circunstancias específicas, la consultoría puede abordar tres tipos de problemas:

a) De corrección: Rectificar una situación deteriorada en comparación con ciertos estándares.
b) De perfeccionamiento: Mejorar una situación existente hasta un nivel óptimo.
c) De creación: Generar una nueva situación.

Las tareas en el trabajo de consultoría pueden incluir:

a) Diagnóstico: Identificación del estado de los procesos.
b) Estudios especiales: Desde encuestas sobre la opinión de los consumidores hasta investigaciones técnicas y económicas sobre inversiones para el desarrollo.
c) Elaboración de soluciones: Proporcionar soluciones concretas, como mejorar el diseño de una planta.
d) Ayuda en la aplicación de soluciones: Asistencia efectiva para interpretar y tomar medidas concretas para implementar las soluciones.
e) Asesorar: Dar consejos o dictámenes sobre los asuntos para los que se han solicitado sus servicios, proporcionando criterios.

2.3.5 Ciberseguridad

La ciberseguridad consiste en proteger equipos, redes, aplicaciones de software, sistemas críticos y datos contra amenazas digitales. Las organizaciones deben salvaguardar los datos para mantener la confianza de los clientes y cumplir con las normativas. Para ello, emplean medidas y herramientas de ciberseguridad que protegen la información confidencial del acceso no autorizado y previenen

interrupciones en las operaciones empresariales debido a actividades de red no deseadas. La implementación de la ciberseguridad en las organizaciones se logra optimizando la defensa digital entre personas, procesos y tecnologías. (Amazon Web Services Inc, 2023)

2.4 Marco legal

Cada vez es más frecuente oír sobre ciberataques que afectan tanto a instituciones gubernamentales como a empresas privadas e individuos. En México, esta situación se ha vuelto más preocupante, ya que hasta 2022 no existía una legislación clara en materia de ciberseguridad.

En este contexto, se ha propuesto una nueva Ley que busca establecer criterios unificados y claros sobre ciberseguridad. A continuación, se detallan esta nueva ley y sus implicaciones.

2.4.1Nueva ley de ciberseguridad en México

iDISC Information Technologies (2023) menciona que actualmente, México carece de una legislación específica en ciberseguridad. Esto ha resultado en que numerosas instituciones gubernamentales, empresas privadas e individuos sean blanco de ciberataques. Aunque desde 2018 se han presentado 11 propuestas de leyes sobre ciberseguridad, ninguna ha sido aprobada.

Fuentes Rivera (2023) menciona el hackeó a la Secretaría de la Defensa Nacional (Sedena) el 19 de septiembre del 2022, puso en marcha la creación de la «versión cero» de una Ley Federal de Ciberseguridad, preparada por el Senado de la República y la Comisión de Ciencia y Tecnología e Innovación de la Cámara de Diputados. Para ello, han buscado y analizado estudios nacionales e internacionales para comprender mejor el vacío legal en que se encuentra el país actualmente.

Fuentes Rivera (2023) indica que se anticipaba que la nueva Ley Federal de Ciberseguridad se publicara en diciembre de 2022. No obstante, hasta el momento de esta investigación, aún no está disponible para el público en general.

Esta propuesta de Ley se compone de 11 títulos que contienen 71 artículos, y se centra en cuatro aspectos clave:

- Garantizar la seguridad nacional mediante la protección del espacio digital.
- Crear un marco legal para sancionar o tipificar los ciberataques.
- Realizar pruebas de penetración o pentesting anuales en instituciones públicas y privadas.
- Establecer una Agencia Nacional de Ciberseguridad bajo la supervisión del Ejecutivo, siguiendo los modelos de la Unión Europea, Estados Unidos y Brasil.

2.4.2 Una nueva comisión

El 10 de enero de 2023, el gobierno federal anunció la formación de la Comisión Intersecretarial de Tecnologías de Información y Comunicación y de Seguridad de la Información (CITICSI). Esta comisión tiene como propósito coordinar e implementar las políticas federales relacionadas con TIC y seguridad de la información, fomentando actividades y estrategias para su aprovechamiento. Por lo tanto, es probable que sus decisiones influyan en el contenido específico de la nueva ley de ciberseguridad.

2.4.3 Leyes que abordan la ciberseguridad

Algunas de las leyes, reglamentos y normativas vigentes en México que mencionan la ciberseguridad incluyen:

- Constitución Política de los Estados Unidos Mexicanos.
- Ley Federal de Telecomunicaciones y Radiodifusión.
- Norma Federal de Transparencia y Acceso a la Información Pública.
- Ley Federal del Derecho de Autor.

- Ley Federal de Protección de Datos Personales en Posesión de Particulares.
- Ley General de Títulos y Operaciones de Crédito.
- Código Penal Federal.
- Estrategia Nacional de Ciberseguridad 2017.
- Programa Nacional de Seguridad 2014-2018.

Es probable que, para implementar la nueva Ley de Ciberseguridad, sea necesario modificar estas leyes y normativas para mantener la coherencia legislativa.

¿Quién se encarga de la ciberseguridad en México? De acuerdo con Fuentes Rivera (2023) actualmente, tres organismos tienen competencias en esta área: el CERT-MX, la Policía Federal y el INAI.

- CERT-MX. El Centro de Respuesta a Incidentes Cibernéticos de la Dirección General Científica de la Guardia Nacional se encarga de proporcionar apoyo en la respuesta a incidentes cibernéticos que afectan a instituciones con infraestructura crítica de información en el país. Además, se aseguran de que las instituciones gubernamentales cumplan con el Manual Administrativo de Aplicación General de Tecnologías de Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI), basado en normas internacionales como la ISO 27001.
- Policía Federal. La División Científica de la Policía Federal de México se dedica a investigar y monitorear las actividades delictivas realizadas en Internet. Colaboran estrechamente con el CERT-MX.
- INAI. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) se encarga de asegurar que el público tenga acceso a la información y de proteger los datos personales.

CAPITULO III: METODOLOGIA

3.1 Tipo y Diseño de investigación

3.1.1 Diseño de la investigación

Los métodos mixtos representan un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada (denominadas meta inferencias) y lograr un mayor entendimiento del fenómeno bajo estudio (Hernández-Sampieri y Mendoza, 2008).

De acuerdo con la definición anterior por Hernández-Sampieri y Mendoza (2008), el diseño de la presente investigación es mixto esto debido a que en la pregunta del planteamiento del problema se determinara la viabilidad económica del proyecto y para ello se utilizaran datos del tipo cuantitativo; el desarrollo del modelo canvas recolecta datos de tipo cualitativo.

3.1.2 Tipo de investigación.

Según Tamayo (2003), en su libro Proceso de Investigación Científica, la investigación descriptiva “comprende la descripción, registro, análisis e interpretación de la naturaleza actual, y la composición o proceso de los fenómenos. El enfoque se hace sobre conclusiones dominantes o sobre grupo de personas, grupo o cosas, se conduce o funciona en presente”.

Para (Sabino, 1992), en su libro Proceso de investigación, menciona que la investigación de tipo descriptiva que “su preocupación primordial radica en describir algunas características fundamentales de conjuntos homogéneos de fenómenos. Las investigaciones descriptivas utilizan criterios sistemáticos que permiten poner de manifiesto la estructura o el comportamiento de los fenómenos en estudio, proporcionando de ese modo información sistemática y comparable con la de otras fuentes”.

La presente investigación es de tipo descriptiva con el fin de analizar y describir detalladamente las diferentes facetas relacionadas con el desarrollo del modelo de negocio para una consultoría de ciberseguridad dirigida a profesionales.

3.2 Población y muestra.

3.2.1 Población

La presente investigación se centra en el estudio de la población de los municipios de Ixtapaluca y Valle de Chalco, ambos ubicados en el Estado de México, en la tabla 2. Población de los municipios de Ixtapaluca y Valle de Chalco se observa la población total de cada uno de los municipios, también se presenta la población total por ambos municipios.

Tabla 2. Población de los municipios de Ixtapaluca y Valle de Chalco

Municipio	Población total
Ixtapaluca	542,211
Valle de Chalco	391,731
total	933,942

Nota: *Elaboracion propia*

3.2.2 Muestra

La importancia de una muestra de población radica en su capacidad para reflejar las características de la población total sin necesidad de examinar cada entidad individualmente. Esto no solo optimiza recursos y tiempo, sino que también proporciona una base sólida para tomar decisiones informadas y desarrollar soluciones de ciberseguridad que se adapten a las particularidades de cada organización.

Para obtener la muestra correspondiente a este proyecto, se ha seguido el procedimiento detallado en la tabla 3, la cual presenta los datos de población y muestra segmentados.

Tabla 3

Datos de población y muestra por segmentación

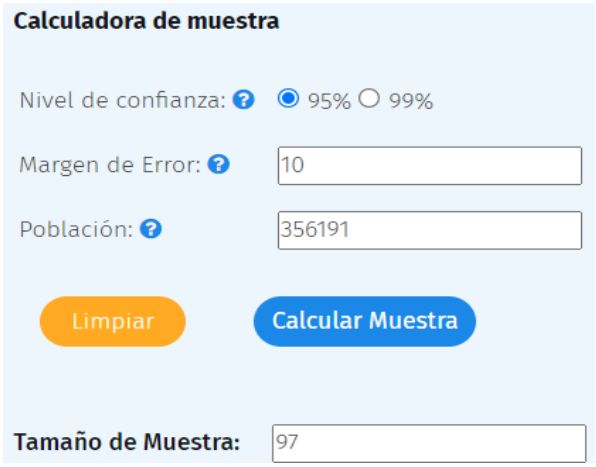
Variable de segmentación	Población	Ixtapaluca		Valle de Chalco		Total
		%	Cant.	%	Cant.	Cant.
Geográfica	Población	100%	542,211	100%	391,731	933,942
Demográfica	Población *25-60 años*	64.15%	347,828.36	63.26%	247,809.03	595,638
Demográfica	Económicamente activa	59.8%	208,001.36	59.8%	148,189.80	**356,191.16**

Nota: Los datos fueron obtenidos con relación al indicador de economía del año 2020, fuente: INEGI

Utilizando la herramienta de calculadora de muestra Question Pro con un margen de error del 10% y un nivel de confianza del 95% se obtiene un tamaño de muestra de 97 que son los instrumentos a aplicar para validar nuestra investigación.

Figura 2

Calculadora de muestra de Question Pro



Nota. Página de Question Pro

La metodología utilizada para escoger los 97 en Ixtapaluca y Valle de Chalco es por estratos.

3.3 Instrumentos.

Se implementa una matriz de operacionalizacion de las variables con el fin de que se incluyan y midan como el modelo Canvas y abarque los aspectos técnicos, económicos y sociales, cual desempeña un papel crucial como componente estratégico para evaluar la eficacia y pertinencia de los elementos del instrumento, específicamente al cuestionario diseñado para la recolección de datos.

La tabla 4 Matriz de operacionalizacion, se describen las variables a continuación:

Tabla 4

Matriz de operacionalización

Variables	Dimensión	Indicador	Ítems	Categorías
Modelo de negocio CANVAS (Osterwalder y Pigneur)	**1. Segmentos de clientes:** Se refiere a los diferentes grupos de personas o empresas a los que se dirige el negocio.	Profesionales economicamente activos	¿Cuál es tu profesión? ¿Indica en que área te encuentras ejerciendo tu profesión (RH, contabilidad, logística, finanzas, educación, ventas, etc)?	
Monitoreo del Modelo de Negocio Canvas	**2. Propuesta de valor:** Describe el conjunto de productos o servicios que se ofrecen a los clientes y cómo se diferencian de la competencia.	Servicios de consultoria en linea o presencial realacionados a ciberseguridad para personas fisicas a un bajo costo las 24- 7	Ha sido víctima de algún de los siguientes delitos cibernéticos. (puede seleccionar más de una opción)	a) robo de identidad b) secuestro de información c) espionaje cibernético d) fraude por correo electrónico e) Ninguno de los anteriores
Evaluar la propuesta de valor utilizando la estrategia de océano azul	**3. Canales:** Representa los medios utilizados para llegar a los clientes y entregarles la propuesta de valor.	Redes sociales.	¿Con que frecuencia utiliza las redes sociales (Facebook, whatssap, Instagram, tiktok)?	a) Todo el día b) 1 hrs- 4hrs c) menos de 1hr
		Sitio web.	En términos de tecnológicos ¿Con que frecuencia participas en comunidades digitales?	a) Siempre

Variables	Dimensión	Indicador	Ítems	Categorías
	4. Relación con los clientes: Describe el tipo de relación que se establece con los clientes, ya sea personalizada, automatizada, a través de comunidades, etc.	Personalizada.	Los servicios de consultoría como te gustaría recibirlos	a) remota b) presencial c) telefónica d) remota y telefónica e) remota y presencial f) presencial y telefónica
		Remotamente	¿Cuál es la opinión que te generan los servicios remotos?	a) Resuelve el problema en el menor tiempo posible y es económico. b) Ahorro tiempo y dinero al contratarlos. c) Me generan desconfianza. d) Nunca e utilizado un soporte remoto.
BENEFICIO COSTO	**5. Fuentes de ingresos:** Son las diferentes formas en las que el negocio genera ingresos a través de la venta de productos, servicios, suscripciones, publicidad, entre otros.	Venta de software con licencia	De los siguientes productos ¿selecciona cuales consumes de manera ilegal?	a) software de oficina b) software contable o administrativo c) software de diseño d) juegos e) películas
		Cursos	¿selecciona los cursos que sean de tu interés?	a) ciberseguridad básica b) capacitación profesional c) capacitación en tu oficio o campo profesional
			Cuanto pagarías por un curso	a) 350 b) 450 c) 500 o más
		Servicio de ciberseguridad	Selecciona la opción que consideres ideal por 1hr de servicio de consultoría en ciberseguridad.	a) $800 b) $1000 c) $ 1500
BENIFICIO COSTO	**6. Recursos clave**: Son los activos necesarios para hacer funcionar el modelo de negocio, como infraestructura física, tecnología, capital humano, entre otros.	Conexión a internet. Equipo de computo. Software especializado Experto en ciberseguridad.	Selecciona cuales son los recursos con los que cuentas en tu hogar u oficina	a) internet b) computadora c) móvil d) asistentes e) electrodomésticos inteligentes
VAN	**7. Actividades clave:** Son las acciones o tareas principales que se realizan para que el modelo de negocio funcione correctamente.	Capacitación del personal Seguimiento a cliente Auditar procesos	¿Utiliza alguno de los siguientes servicios en línea especializados?	a) Banca en línea b) Servicio de streaming c) Aperturas de cuentas d) Consulta de correo electrónico

Variables	Dimensión	Indicador	Ítems	Categorías
TIR	**8. Alianzas clave:** Representa las colaboraciones o asociaciones estratégicas con otras empresas u organizaciones que son fundamentales para el éxito del negocio.		¿A Utilizado alguno de los siguientes servicios de consultoría en tecnología?	a) Capacitación en tecnología. b) Compras de productos tecnológicos c) Solución de problemas
TIR	**9. Estructura de costos:** Describe los costos asociados con la operación del negocio, incluyendo costos fijos, variables, de personal, de marketing, entre otros.		¿Cuánto estaría dispuesto a pagar por los servicios de una consultoría especialista en ciberseguridad? ¿solicitarías el servicio cada qué?	a) Menos de $1,000 b) $1,000 - $5,000 c) Mas de $5,000 a) surge el problema. b) Contratar el servicio mensual c) Contratar el servicio anualmente

Nota: *Elaboracion propia*

3.3.1 Validacion del instrumento

Utilizando la matriz de operacionalización de las variables, se elabora un cuestionario de 15 preguntas, tal como se muestra en el anexo 1.

Se valida el instrumento con el coeficiente alfa de Cronbach que es la forma más sencilla y conocida de medir la consistencia interna y es la primera aproximación a la validación del constructo de una escala. El coeficiente alfa de Cronbach debe entenderse como una medida de la correlación de los ítems que forman una escala.

Para el cálculo del alfa de Cronbach se empleo la formula siguiente:

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\Sigma v_i}{v_t}\right]$$

$\alpha = alfa\ de\ cronbach$

$k = numero\ de\ items$

$v_i = varianza\ de\ cada\ item$

$v_t = varianza\ del\ total$

3.3.1.1 Interpretacion de la escala de alfa de Cronbach

El valor mínimo aceptable para el coeficiente alfa de Cronbach es 0,70; por debajo de ese valor la consistencia interna de la escala utilizada es baja. Por su parte, el valor máximo esperado es 0,90; por encima de este valor se considera que hay redundancia o duplicación (Celina Oviedo & Campo Arias, 2005), como se observa en la tabla 5 Rangos del Alfa de Cronbach.

Tabla 5

Rangos del Alfa de Cronbach

Alfa de Cronbach	Consistencia Interna
α ≥ 0.9	Excelente
0.8 ≤ α < 0.9	Bueno
0.7 ≤ α < 0.8	Aceptable
0.6 ≤ α < 0.7	Cuestionable
0.5 ≤ α < 0.6	Pobre
α < 0.5	Inaceptable

Nota: Fuente:(Pérez León, 2022)

Sutituyendo los variables por los valores en la formula del alfa de Cronbach

Numero de items $k = 15$

Varianza asociada a cada item $v_i = 9.494$

Varianza total de la escala $v_t = 35.814$

Alfa de Cronbach $\alpha = 0.79$

Debido a que el coeficiente es de 0.79 se deduce que la encuesta es aceptable.

3.4 Procedimientos

Mediante la utilización una matriz de operacionalización de las variables se diseña una encuesta con 15 ítems, para la recolección de resultados, la misma se aplica utilizando

el aplicativo de Google Forms, se distribuye en la muestra de 97 individuos de los municipios de Valle de Chalco e Ixtapaluca, una vez recolectada la información se realiza el análisis del alfa de Cronbach para verificar la confiabilidad de la encuesta.

El siguiente paso es comenzar con el análisis cualitativo y cuantitativo de los resultados para dar comprobar la hipótesis alternativa. Posteriormente realizar el modelo de negocios Canvas de Osterwalder para una consultoría de ciberseguridad en Ixtapaluca y Valle de Chalco.

3.4.1 Matriz de consistencia

La matriz de consistencia es una herramienta esencial que ayuda a ordenar y plantear la información requerida para elaborar un tema de investigación. Esta matriz consta de varios cuadros ordenados en filas y columnas que permiten al investigador verificar la coherencia y la lógica entre el título, el problema, los objetivos, las hipótesis, las variables, el tipo, el método, el diseño y los instrumentos de investigación. Además, la matriz incorpora la población y la muestra de estudio.

A manera de resumen se presenta el proyecto de investigación en la tabla 6 se muestra la matriz de consistencia desde el inicio del proceso con la pregunta de investigación hasta la hipótesis que son propias de comprobación estadística.

Tabla 6

Matriz de consistencia

Pregunta de investigación	Objetivo	H Principal	H Alternativa	H Nula	Metodología	instrumentos	variables	indicadores
¿Cuál será la viabilidad económica de una consultoría especializada en ciberseguridad para personas físicas establecidos en los municipios de Ixtapaluca y Valle de Chalco Solidaridad del Estado de México?	Desarrollar un modelo de negocios de una consultoría en ciberseguridad para personas físicas de los municipios de Ixtapaluca y Valle de Chalco del Estado de México.	El desarrollo de un modelo de negocio CANVAS de una consultoría en ciberseguridad para personas físicas de los municipios de Ixtapaluca y Valle de Chalco del Estado de México permitirá un emprendimiento viable de acuerdo con los indicadores financieros.	Si el resultado de la VAN llegase a tener un valor positivo y la TIR es mayor o igual a la Tasa de descuento, entonces la propuesta de valor del modelo canvas será rentable	Si el resultado de la VAN llegase a tener un valor negativo y la TIR es menor a la Tasa de descuento, entonces la propuesta de valor del modelo canvas no será rentable	Mixta	Matriz de operacionalización de las variables. Encuesta Modelo Canvas	Dependientes: Viabilidad económica. Independientes: Propuesta de valor del modelo de negocios Canvas	VAN TIR

Nota. Elaboración propia del autor.

CAPITULO IV: Resultados y Discusión

4.1 Presentación y análisis de resultados

El propósito del presente capitulo es la presentación, análisis e interpretación del instrumento para dar una mayor validez al presente trabajo de investigación que se ha aplicado a la muestra de estudio, para obtener resultados que permitan concluir la viabilidad económica de una consultoría a personas físicas de los municipios de valle de Chalco e Ixtapaluca en el Estado de México.

Como característica principal del cuestionario, cabe mencionar que es de selección múltiple para que así sea de fácil manejo para el entrevistado y también tabular los datos con mejor objetividad.

La aplicación del mencionado cuestionario se la realizó por medio de la aplicación Google Forms a las personas físicas de los municipios mencionados. Cabe destacar que la muestra fue de 97 personas y por tanto se procedió a realizar a todas las personas de la muestra.

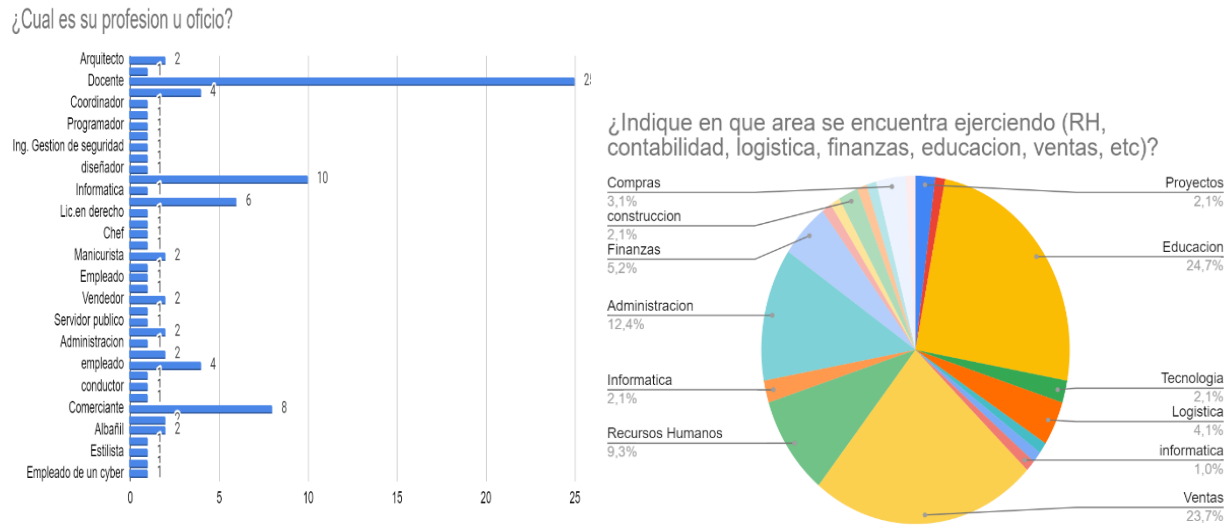
4.1.1 Resultados de la encuesta a las personas físicas de los municipios de Valle de Chalco e Ixtapaluca

Para la presentación de los resultados, se realiza de forma gráfico debido a que es la mejor forma de desplegar y dar a conocer lo recabado, estos gráficos de presentación muestran datos cuantitativos para la interpretación.

En la Figura 3 Segmento de clientes se observa que 25 de los 97 encuestados son docentes por lo que el 24.7% está relacionado a la educación, seguido del 23.7% relacionado a las ventas y un 12.4% a la administración.

Figura 3

Segmentó de clientes



Nota: Elaboración propias del autor y fuente: trabajo de campo.

Interpretación. El segmento de los clientes deberá de estar dirigido a las personas físicas con actividades relacionadas a educación, ventas, actividades administrativas y en recursos humanos.

En la Figura 4 Propuesta de valor se observa que 25.8% experimento o fue víctima de robo de identidad seguido de un 16.5 % a fue víctima del robo de datos financieros y un 9.3% relacionado fue víctima de fraude por correo electrónico.

Figura 4

Propuesta de valor

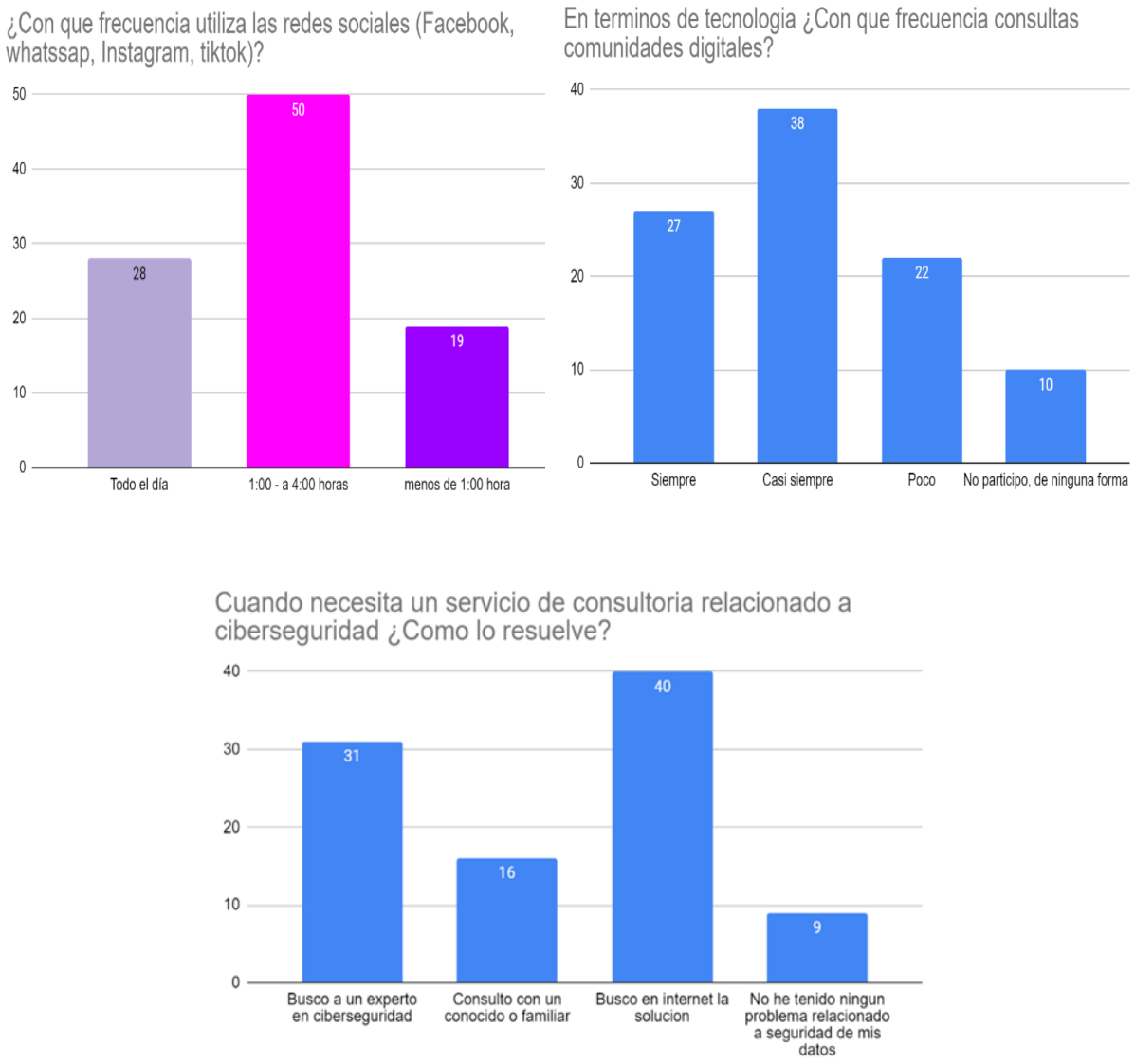
Nota: Elaboración propias del autor y fuente: trabajo de campo.

Interpretación. Existe una necesidad en la especialización y capacitación de las personas físicas victimas de los delitos de robo de identidad, robo de datos y fraude por correo electrónico por lo que la propuesta de valor deberá de estar centrada en solventar este tipo de delitos.

En la Figura 5 Medios utilizados para llegar a los clientes y entregarles la propuesta de valor se puede observar que el 50% de los encuestados utiliza en promedio 4hrs al día las redes sociales mientras que 38% consulta alguna comunidad digital relacionada a tecnología; mientras que el 31% busca aun experto en ciberseguridad y el 40% en internet la solución para resolver alguna problemática en ciberseguridad.

Figura 5

Medios para llegar a los clientes



Nota: Elaboración propias del autor y fuente: trabajo de campo.

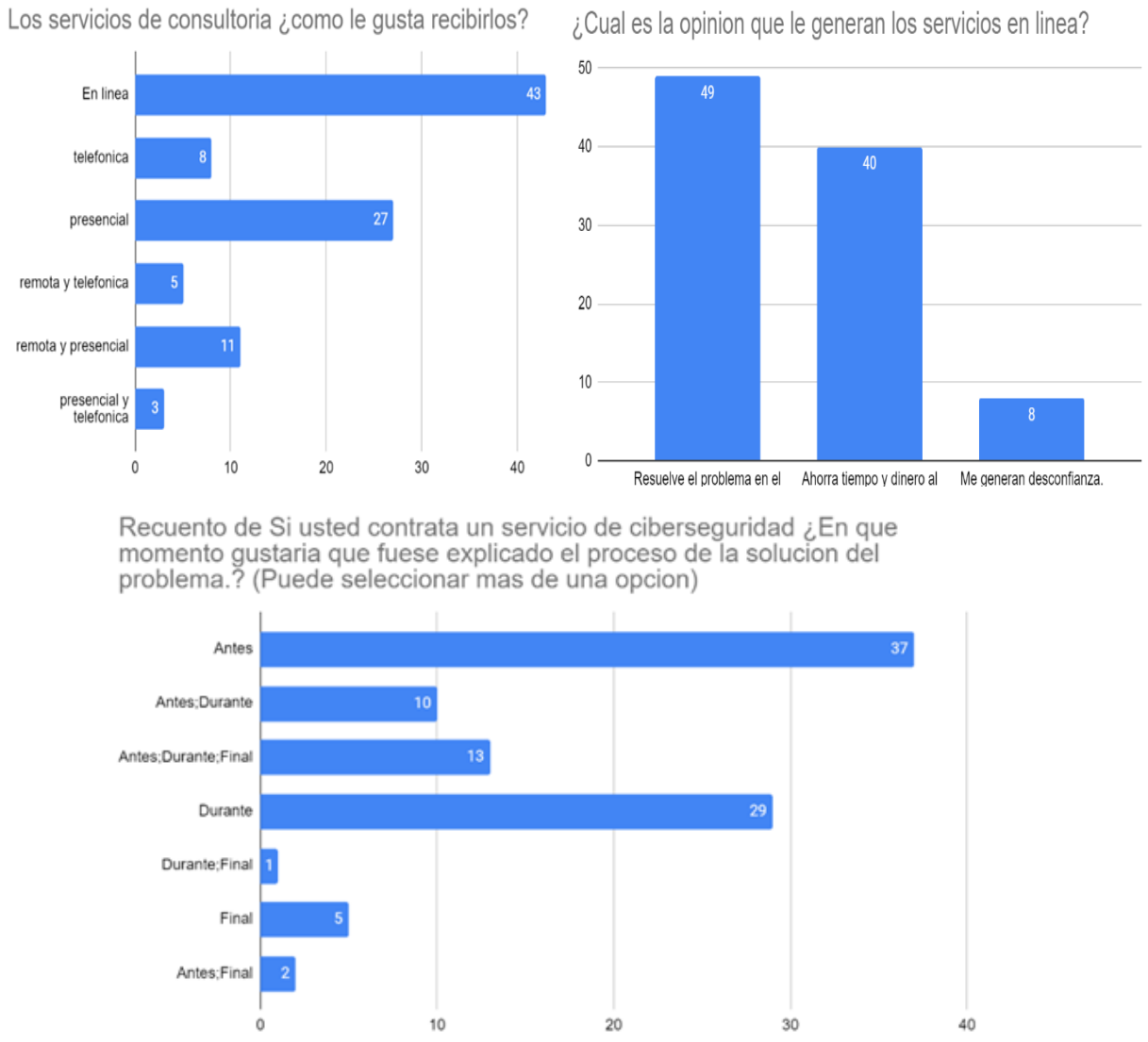
Interpretación. Los canales que se pueden explotar para dar a conocer la propuesta de valor de la consultoría son redes sociales y crear una comunidad digital para las personas fiscas de los municipios de Valle de Chalco e Ixtapaluca.

Análisis. En la Figura 6 Relación con el cliente, como se observa el 43% le gustaría recibir consultoría en línea reforzado con un 49% opina que los servicios en línea

resuelven los problemas en menos tiempo y son más económicos, también se puede observar que 37% de los encuestados les gustaría que fuese explicado antes el proceso de la posible solución.

Figura 6

Relación con el cliente



Nota: Elaboración propias del autor y fuente: trabajo de campo.

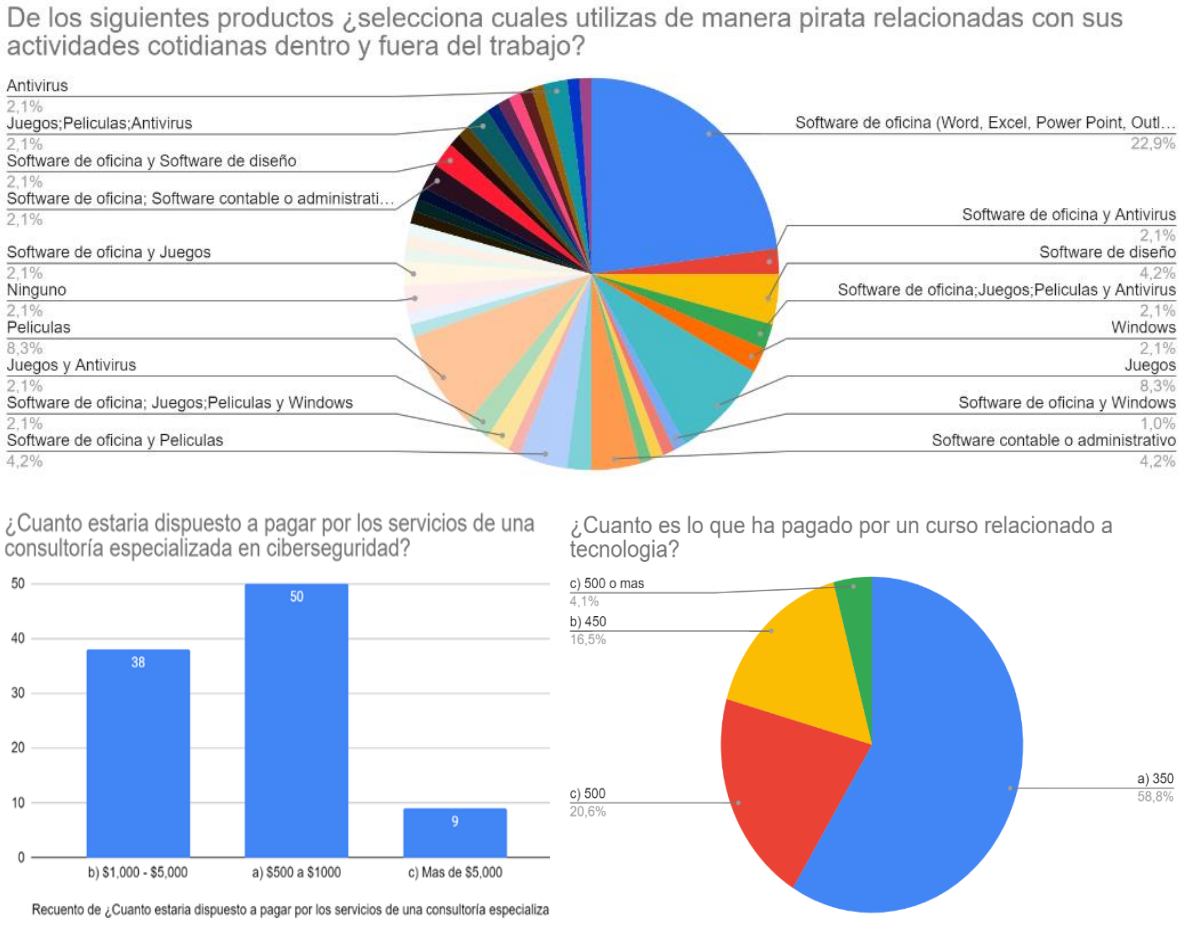
Interpretación. Se debe de ofrecer el servicio de consultoría en línea utilizando plataformas explicando antes el proceso de solución para obtener la opinión positiva

que del cliente sobre los servicios de consultoría en línea en los municipios de Valle de Chalco e Ixtapaluca.

En la Figura 7 fuentes de ingresos se observa que el 22.9% sigue consumiendo software de oficina de dudosa procedencia, el 50% se encuentra dispuesto a pagar por un servicio de consultoría entre $500 pesos a $1000 pesos y un 58.8% a pagado $350 pesos por un curso a fin a la tecnología.

Figura 7

Fuentes de ingresos



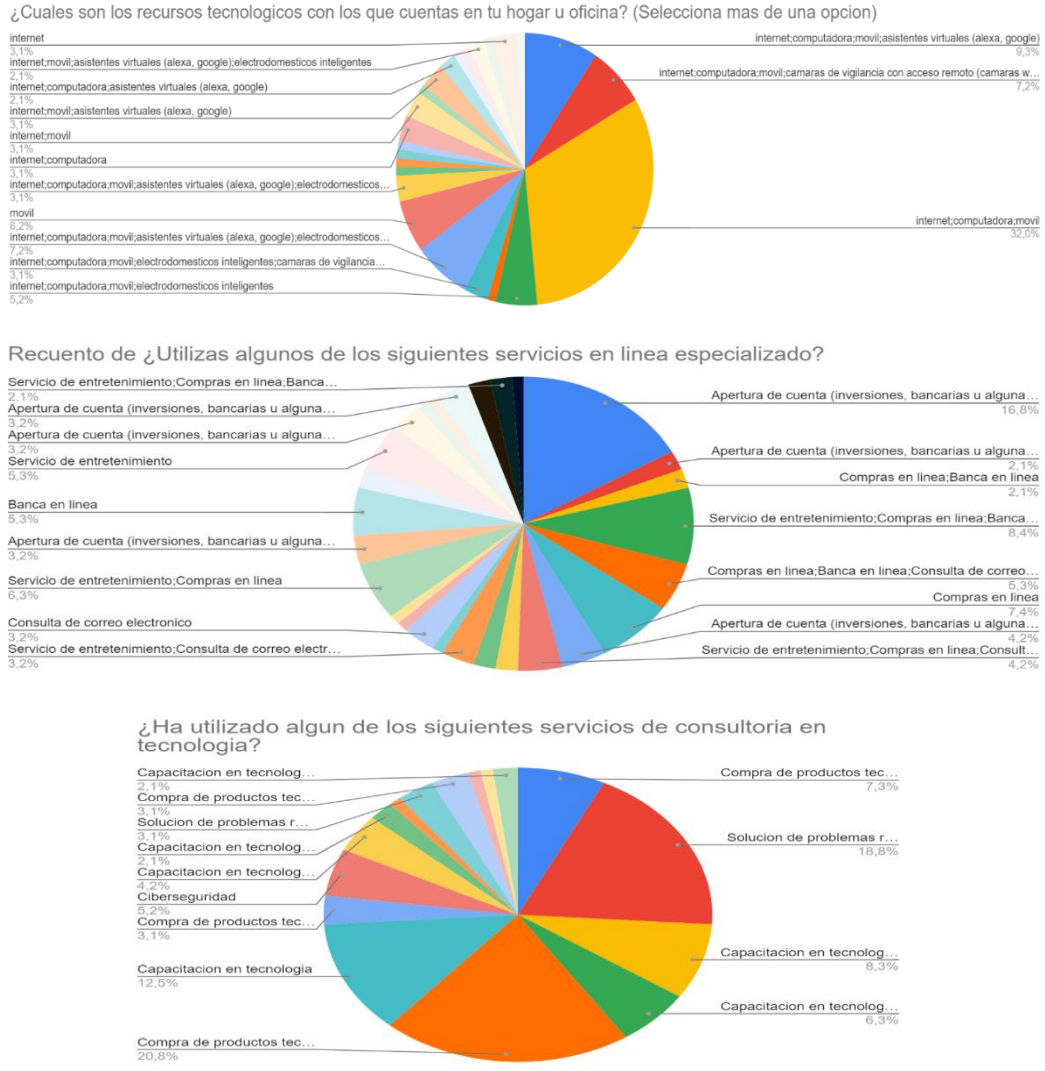
Nota: Elaboración propias del autor y fuente: trabajo de campo.

Interpretación. La mayor fuente de ingresos para el presente trabajo de investigación se obtendría de los servicios especializados en ciberseguridad, seguida del ofrecimiento de capacitaciones a los clientes y por último la venta software legal, buscando que se encuentre en el rango de precio de $350 pesos a $1000 pesos.

En la Figura 8 Recursos de la persona físicas se observa que el 32% cuenta con una computadora, internet o dispositivo móvil, mientras que el 16.8% utiliza el servicio de banca en línea y el 20.8% realiza compras en línea.

Figura 8

Recursos de la persona física



Nota: Elaboración propias del autor y fuente: trabajo de campo.

Interpretación. La mayor parte de las personas físicas encuestadas cuentan con los recursos mínimos en infraestructura necesarios de tal manera que se pueda ofrecer el servicio de consultoría en línea, tienen conocimiento sobre la utilización de algunos servicios como, por ejemplo, manejo de apertura de cuentas bancarias, compras en línea, cursos en línea; las personas físicas necesitan un consultor en ciberseguridad por el tipo de actividades que realizan.

4.2 Prueba de hipótesis

Los recursos con los que cuenta en el hogar u oficina los utiliza con frecuencia para consultar comunidades tecnológicas

Tabla 7

Contingencia

	En términos de tecnología ¿Con que frecuencia consultas comunidades digitales?				
¿Cuáles son los recursos tecnológicos con los que cuentas en tu hogar u oficina? (Selecciona mas de una opción)	**Casi siempre**	**No participo, de ninguna forma**	**Poco**	**Siempre**	**Total**
cámaras de vigilancia con acceso remoto (cámaras wifi)	0	0	0	1	1
computadora	0	0	0	1	1
computadora; asistentes virtuales (Alexa, Google)	0	1	0	0	1
internet	3	0	0	0	3
internet; computadora	1	0	1	1	3
internet; computadora; asistentes virtuales (Alexa, Google)	1	0	1	0	2
internet; computadora; cámaras de vigilancia con acceso remoto (cámaras wifis)	1	0	0	0	1
internet; computadora; móvil; asistentes virtuales (Alexa, Google); electrodomésticos inteligentes; cámaras de vigilancia con acceso remoto (cámaras wifi)	0	1	0	0	1
internet; computadora; móvil	13	0	9	10	32
internet; computadora; móvil; asistentes virtuales (Alexa, Google)	5	0	3	1	9

¿Cuáles son los recursos tecnológicos con los que cuentas en tu hogar u oficina? (Selecciona mas de una opción)	En términos de tecnología ¿Con que frecuencia consultas comunidades digitales?				
	Casi siempre	No participo, de ninguna forma	Poco	Siempre	Total
internet; computadora; móvil; asistentes virtuales (Alexa, Google);cámaras de vigilancia con acceso remoto (cámaras wifi)	0	0	0	1	1
internet; computadora; móvil; asistentes virtuales (Alexa, Google);electrodomésticos inteligentes	0	1	1	1	3
internet; computadora; móvil; asistentes virtuales (Alexa, Google);electrodomésticos inteligentes; cámaras de vigilancia con acceso remoto (cámaras wifi)	6	0	0	1	7
internet; computadora; móvil; asistentes virtuales (Alexa, Google);electrodomésticos inteligentes; cámaras de vigilancia con acceso remoto (cámaras wifi)	0	0	1	0	1
internet; computadora; móvil; cámaras de vigilancia con acceso remoto (cámaras wifi)	4	0	1	2	7
internet; computadora; móvil; electrodomésticos inteligentes	2	0	1	2	5
internet; computadora; móvil; electrodomésticos inteligentes; cámaras de vigilancia con acceso remoto (cámaras wifi)	1	0	1	1	3
internet; móvil	0	1	0	2	3
internet; móvil; asistentes virtuales (Alexa, Google)	0	3	0	0	3
internet; móvil; asistentes virtuales (Alexa, Google);electrodomésticos inteligentes	1	1	0	0	2
internet; móvil; cámaras de vigilancia con acceso remoto (cámaras wifi)	0	0	1	0	1
internet; móvil; electrodomésticos inteligentes	0	1	0	0	1
móvil	0	1	2	3	6
Total	38	10	22	27	97

Pruebas de χ^2

¿Cuáles son los recursos tecnológicos con los que cuentas en tu hogar u oficina? (Selecciona mas de una opción)	En términos de tecnología ¿Con que frecuencia consultas comunidades digitales?				
	Casi siempre	No participo, de ninguna forma	Poco	Siempre	Total

	Valor	gl	p
χ^2	107	66	0.001
N	97		

Los usuarios con infraestructura básica (internet, computadora, móvil) consultan con mayor frecuencia las comunidades digitales.

4.3 Presentación de resultados

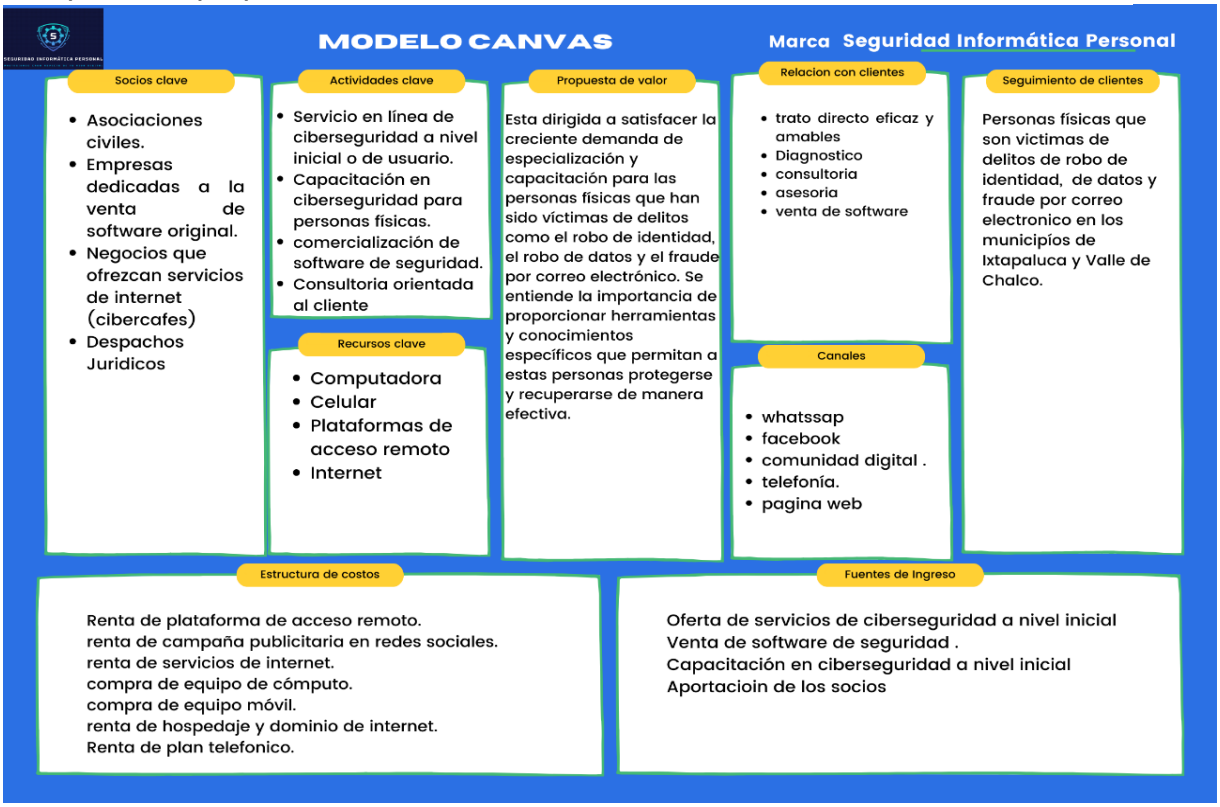
4.3.1 Análisis de negocio

4.3.1.1 Propuesta de valor

La propuesta de valor como se observa en la figura 9 bloque de propuesta de valor en el modelo canvas. se dirige a satisfacer la creciente demanda de especialización y capacitación para las personas físicas que han sido víctimas de delitos como el robo de identidad, el robo de datos y el fraude por correo electrónico. Esto implica ofrecer servicios de ciberseguridad, capacitación y venta de software que se ajusten a las necesidades específicas de cada tipo de profesional, y que sean de calidad con sustento científico y tecnológico para garantizar su seguridad. Este tipo de servicios deben ser certificados y de fácil acceso, permitiendo a las personas con físicas llevar a cabo sus actividades diarias de manera independiente y segura. Se entiende la importancia de proporcionar herramientas y conocimientos específicos que permitan a estas personas protegerse y recuperarse de manera efectiva.

Figura 9

Bloque de la propuesta de valor en el modelo canvas



Nota. Elaboración propia del autor.

4.3.2. Análisis estratégico.

4.3.2.1 Misión

En Seguridad informática personal, nos comprometemos a empoderar a las víctimas de delitos cibernéticos mediante capacitaciones especializadas y recursos que les permitan comprender, prevenir y mitigar impactos negativos.

4.3.2.2 Visión

En Seguridad informática personal, nuestra visión es crear es ser líderes en la creación de un entorno digital seguro y confiable para todos. Comprometidos a innovar continuamente y a proporcionar soluciones personalizadas que fortalezcan la confianza y seguridad en un mundo cada vez más interconectado.

4.3.2.3. Análisis externo

El Análisis Externo se encarga de identificar y evaluar todos los elementos fuera de la consultora que ejerzan influencia en la misma. Para ello, se utilizarán las herramientas de diagnóstico PESTEL y las cinco fuerzas de Porter, que permitan reconocer las posibles oportunidades y amenazas que se pueden presentar en la consultora “Seguridad informática personal”.

4.3.2.3.1 Análisis PESTEL

En la figura 10 Análisis PESTEL se presenta para para comprender los factores políticos, económicos, sociales, tecnológicos, ecológicos y legales en el que opera la consultoría Seguridad informática personal.

Figura 10

Análisis PESTEL

Nota. Elaboración propia del autor.

4.3.2.3.1.1 Político

Regulaciones gubernamentales: La empresa debe estar al tanto de las regulaciones relacionadas con la protección de datos y la ciberseguridad, ya que pueden influir en sus operaciones y servicios.

Políticas de seguridad cibernética: Las políticas y estrategias gubernamentales en materia de seguridad cibernética pueden afectar la demanda de los servicios ofrecidos por la empresa.

4.3.2.3.1.2 Económico

Condiciones económicas globales y locales: Las condiciones económicas, como el crecimiento del PIB, la tasa de desempleo y la inflación, pueden afectar el presupuesto de las organizaciones para invertir en seguridad cibernética.
Costo de los servicios: La empresa debe considerar cómo las fluctuaciones económicas pueden influir en la capacidad de sus clientes para pagar por sus servicios.

4.3.2.3.1.3 Social

Conciencia sobre la seguridad cibernética: El aumento de la conciencia sobre la importancia de la seguridad cibernética puede aumentar la demanda de los servicios de la empresa.

Cambios en el comportamiento del consumidor: Los cambios en el comportamiento de los consumidores, como el aumento del uso de dispositivos móviles y las compras en línea, pueden cambiar las necesidades de seguridad cibernética de las personas.

4.3.2.3.1.4 Tecnológico

Avances tecnológicos: Los avances en tecnología pueden ofrecer nuevas oportunidades para mejorar los servicios de seguridad cibernética, pero también pueden crear nuevas amenazas.

Cambios en la infraestructura de TI: La empresa debe estar al tanto de los cambios en la infraestructura de TI que puedan afectar la seguridad de sus clientes.

4.3.2.3.1.5 Ambiental

Impacto ambiental de la tecnología: La empresa debe considerar el impacto ambiental de sus operaciones y servicios, así como las implicaciones de seguridad cibernética relacionadas con la sostenibilidad.

4.3.2.3.1.6 Legal

Normativas de privacidad de datos: Las regulaciones de privacidad de datos, que llegasen a crear con influencia en las prácticas de seguridad cibernética de los individuos.

Responsabilidad legal: La empresa debe cumplir con las leyes y regulaciones relacionadas con la seguridad cibernética y puede enfrentar consecuencias legales si no lo hace.

Este análisis proporciona una visión general de los factores externos que pueden influir en la empresa de Seguridad Informática Personal y ayuda a identificar oportunidades y amenazas en su entorno operativo.

4.3.2.3.2 Análisis de las cinco fuerzas de Porter

En la figura 11 análisis de las cinco fuerzas de Porter proporciona una comprensión del entorno competitivo en el que opera la empresa de consultoría denominada “Seguridad Informática Personal”, permite a identificar las oportunidades y amenazas que enfrenta en su mercado.

Figura 11

Análisis de las cinco fuerzas de Porter

Nota. Elaboración propia del autor.

4.3.2.3.2.1 Rivalidad entre competidores existentes

En la industria de ciberseguridad, la rivalidad entre competidores puede ser alta debido a la proliferación de empresas como Asociación Mexicana Contra Delitos Cibernéticos A.C, Veritas Technologies LLC, que ofrecen servicios similares.

Sin embargo, la especialización y experiencia pueden ayudar a la consultoría a diferenciarse y mantener una ventaja competitiva.

4.3.2.3.2.2 Amenaza de nuevos participantes

La amenaza de nuevos participantes en la industria de la ciberseguridad puede ser moderada a alta, especialmente con el aumento de la conciencia sobre la importancia de la seguridad cibernética, altos costos de desarrollo de tecnología, regulaciones gubernamentales y la necesidad de reputación y confianza en el mercado; las empresas con tecnologías innovadoras o enfoques disruptivos pueden superar estas barreras y entrar en el mercado con éxito organizaciones como Consejo de Seguridad de la Información y Ciberseguridad (CONSEJOSI) es una organización sin fines de lucro ubicada en Monterrey, que se dedica a la seguridad de la información y ciberseguridad, proporcionando asesoría y capacitación en estas áreas.

4.3.2.3.2.3 Poder de negociación de los proveedores

En la industria de la ciberseguridad, el poder de negociación de los proveedores puede ser moderado, especialmente para proveedores de tecnología y software especializado, como por ejemplo Kaspersky o Microsoft.

Sin embargo, las empresas pueden diversificar sus fuentes de proveedores o desarrollar sus propias soluciones internas para reducir la dependencia de proveedores externos.

4.3.2.3.2.4 Poder de negociación de los compradores

El poder de negociación de los compradores en la industria de la ciberseguridad puede ser alto, especialmente para personas físicas que pueden presionar para obtener

precios más bajos, mejores términos de contrato y servicios personalizados para satisfacer sus necesidades específicas de seguridad cibernética.

4.3.2.3.2.5 Amenaza de productos o servicios sustitutos

La amenaza de productos o servicios sustitutos en la industria de la ciberseguridad puede ser moderada, ya que los clientes pueden recurrir a soluciones internas o alternativas como una profesional de las tecnologías de la información para abordar sus necesidades de seguridad cibernética.

Sin embargo, la empresa puede diferenciarse ofreciendo servicios especializados y soluciones integrales que sean difíciles de replicar con alternativas sustitutas.

4.3.2.4 Análisis interno

Los Análisis Interno tienen como finalidad identificar las fortalezas y debilidades internas que pueda tener la consultora “Seguridad Informática Personal” para ello, se utilizarán la herramienta de Cadena de valor. Con la finalidad de realizar las correcciones necesarias a las debilidades existentes. Al mismo tiempo robustecer las fortalezas que posee la consultora. Toda esta actividad permitirá mejorar los métodos internos de la consultora proyectándolo al exterior de esta.

4.3.2.4.1 Cadena de valor

La cadena de valor para la empresa de consultoría “Seguridad Informática Personal” se enfoca en proporcionar un servicio integral que permita cubrir desde la evaluación inicial de las necesidades del cliente hasta la implementación y soporte continuo de soluciones de ciberseguridad.

Este enfoque integral y bien estructurado proporciona a los clientes una seguridad mejorada y un soporte continuo, lo que a su vez fortalece la posición de la empresa en el mercado y fomenta la fidelidad del cliente.

Las actividades primarias identificadas de la cadena de valor son las siguientes:

- Inbound Logistics (Logística de entrada): Recepción y análisis de la información sobre sistema operativo, el proveedor de internet y aplicaciones utilizada por la persona física.
- Operations (Operaciones): Evaluación de la infraestructura de TI de la persona física, análisis de vulnerabilidades.
- Outbound Logistics (Logística de salida): Entrega de informes detallados sobre hallazgos y recomendaciones de seguridad.
- Marketing and Sales (Marketing y ventas): Promoción de servicios de consultoría, generación de leads, y cierre de contratos.
- Service (Servicio): Implementación de soluciones de seguridad, asesoramiento continuo, capacitación a la persona física y soporte técnico.

Las actividades de apoyo identificadas son las siguientes:

- Infrastructure (Infraestructura): Proveedor de internet, dispositivos de red, mantenimiento de equipos y herramientas de análisis de seguridad.
- Human Resources (Recursos Humanos): Selección, capacitación y retención de talento especializado en ciberseguridad.
- Technology (Tecnología): Desarrollo y actualización de herramientas de análisis y monitoreo de ciberseguridad.
- Procurement (Adquisiciones): Adquisición de software, hardware y servicios necesarios para la operación de la consultoría.

La relación de las actividades primarias con las actividades de apoyo en el contexto de la consultoría en ciberseguridad se desglosa a continuación para la consultoría “Seguridad Informática Personal”:

Inbound Logistics (Logística de entrada):

- Infrastructure (Infraestructura): Asegurar la disponibilidad y el rendimiento del proveedor de internet y dispositivos de red para la correcta recepción y análisis de la información.
- Technology (Tecnología): Utilizar herramientas avanzadas para recolectar y analizar datos sobre el sistema operativo, aplicaciones y otros elementos relevantes.
- Procurement (Adquisiciones): Adquirir el software y hardware necesario para realizar el análisis inicial de manera eficiente.

Operations (Operaciones):

- Infrastructure (Infraestructura): Mantener una infraestructura de TI robusta que permita realizar evaluaciones detalladas y análisis de vulnerabilidades sin interrupciones.
- Human Resources (Recursos Humanos): Contar con personal capacitado en la evaluación de infraestructuras de TI y análisis de vulnerabilidades.
- Technology (Tecnología): Implementar y actualizar constantemente las herramientas necesarias para el análisis y evaluación de vulnerabilidades.
- Procurement (Adquisiciones): Adquirir herramientas especializadas de análisis de vulnerabilidades y equipos necesarios para la evaluación.

Outbound Logistics (Logística de salida):

- Infrastructure (Infraestructura): Asegurar que los sistemas de entrega de informes (correo electrónico seguro, plataformas de informes en línea) funcionen correctamente.
- Technology (Tecnología): Desarrollar y mantener plataformas seguras y eficientes para la entrega de informes y recomendaciones.

- Human Resources (Recursos Humanos): Personal capacitado en la redacción y presentación de informes claros y detallados.
- Procurement (Adquisiciones): Adquirir software de generación de informes y plataformas de comunicación seguras.

Marketing and Sales (Marketing y ventas):

- Infrastructure (Infraestructura): Tener una infraestructura que soporte las actividades de marketing digital, sitios web, y gestión de relaciones con clientes (CRM).
- Human Resources (Recursos Humanos): Personal especializado en marketing y ventas con conocimientos en ciberseguridad.
- Technology (Tecnología): Utilizar herramientas de marketing digital y CRM para la promoción de servicios y generación de leads.
- Procurement (Adquisiciones): Adquirir software de marketing y CRM necesarios para la gestión de campañas y clientes.

Service (Servicio):

- Infrastructure (Infraestructura): Disponer de sistemas y redes que faciliten la implementación de soluciones y soporte técnico.
- Human Resources (Recursos Humanos): Contar con personal altamente capacitado para la implementación de soluciones de seguridad, asesoramiento y capacitación continua.
- Technology (Tecnología): Implementar y actualizar herramientas de ciberseguridad y plataformas de capacitación.
- Procurement (Adquisiciones): Adquirir soluciones de software y hardware necesarias para la implementación y soporte técnico.

A continuación, se muestra la descripción a detalle de cada actividad de apoyo para la consultoría de “Seguridad informática personal” en infraestructura, los recursos humanos, la tecnología y las adquisiciones forman la columna vertebral que permite

el funcionamiento adecuado y eficiente de las actividades primarias en la consultoría de “Seguridad Informática Personal”.

Las ventajas competitivas que se pueden identificar para para la consultora “Seguridad Informática Personal” se relacionan con la eficiencia y la calidad en la prestación de sus servicios, así como con la innovación y el talento especializado. A continuación, se presentan las ventajas competitivas identificadas:

- **Infraestructura Sólida y Confiable:**
  Proveedor de internet y dispositivos de red confiables: Permiten una recepción y análisis de información sin interrupciones, crucial para evaluar la infraestructura de TI de los clientes.
  Sistemas y redes eficientes para la implementación de soluciones: Aseguran que las soluciones de seguridad se implementen de manera eficaz y que el soporte técnico sea continuo.
- **Tecnología Avanzada:**
  Herramientas de análisis y monitoreo de ciberseguridad: Desarrollo y actualización constante de herramientas que permiten detectar vulnerabilidades y amenazas de manera efectiva.
  Plataformas seguras para la entrega de informes: Garantizan la confidencialidad y seguridad en la comunicación con los clientes.
- **Recursos Humanos Especializados:**
  Talento capacitado en ciberseguridad: Selección, capacitación y retención de expertos en ciberseguridad, lo cual asegura un alto nivel de competencia y conocimiento actualizado.
  Personal de marketing y ventas especializado en ciberseguridad: Facilita una promoción efectiva y la generación de leads de calidad, mejorando el cierre de contratos.
- **Adquisiciones Estratégicas:**
  Software y hardware especializados: Adquisición de herramientas y equipos necesarios para realizar análisis detallados y ofrecer soluciones efectivas.

Soluciones de software de marketing y CRM: Facilitan la gestión de campañas de marketing y la relación con los clientes, mejorando la eficiencia operativa.

- **Enfoque en el Cliente:**

  Informes detallados y recomendaciones personalizadas: Proporcionan a los clientes un valor añadido al recibir no solo un diagnóstico, sino también soluciones específicas y aplicables.

  Asesoramiento continuo y capacitación: Aseguran que los clientes estén siempre al tanto de las mejores prácticas de seguridad y que sus sistemas se mantengan protegidos.

Estas ventajas competitivas permiten a la consultora diferenciarse en el mercado, ofreciendo servicios de alta calidad, manteniendo la confianza de los clientes y asegurando una operación eficiente y efectiva.

4.3.2.4.2 Análisis FODA

En el vertiginoso paisaje digital actual, la ciberseguridad se ha erigido como un pilar fundamental para la estabilidad y el éxito de las organizaciones. La creciente sofisticación de las amenazas cibernéticas demanda una respuesta estratégica y proactiva por parte de las empresas, que deben estar equipadas con las herramientas y los conocimientos necesarios para salvaguardar sus activos digitales. En este contexto, la presente consultoría de “Seguridad Informática Personal” se erige como un faro guía, como se puede observar en la figura 12 Análisis FODA donde se realiza un análisis exhaustivo de las fortalezas, debilidades, oportunidades y amenazas, que enfrenta la empresa en el ámbito de la ciberseguridad. A través de este proceso de diagnóstico, no solo identifica los puntos críticos de vulnerabilidad, sino que también perfilan las estrategias personalizadas para fortalecer una postura defensiva y proteger su infraestructura digital de manera eficaz y sostenible.

Figura 12

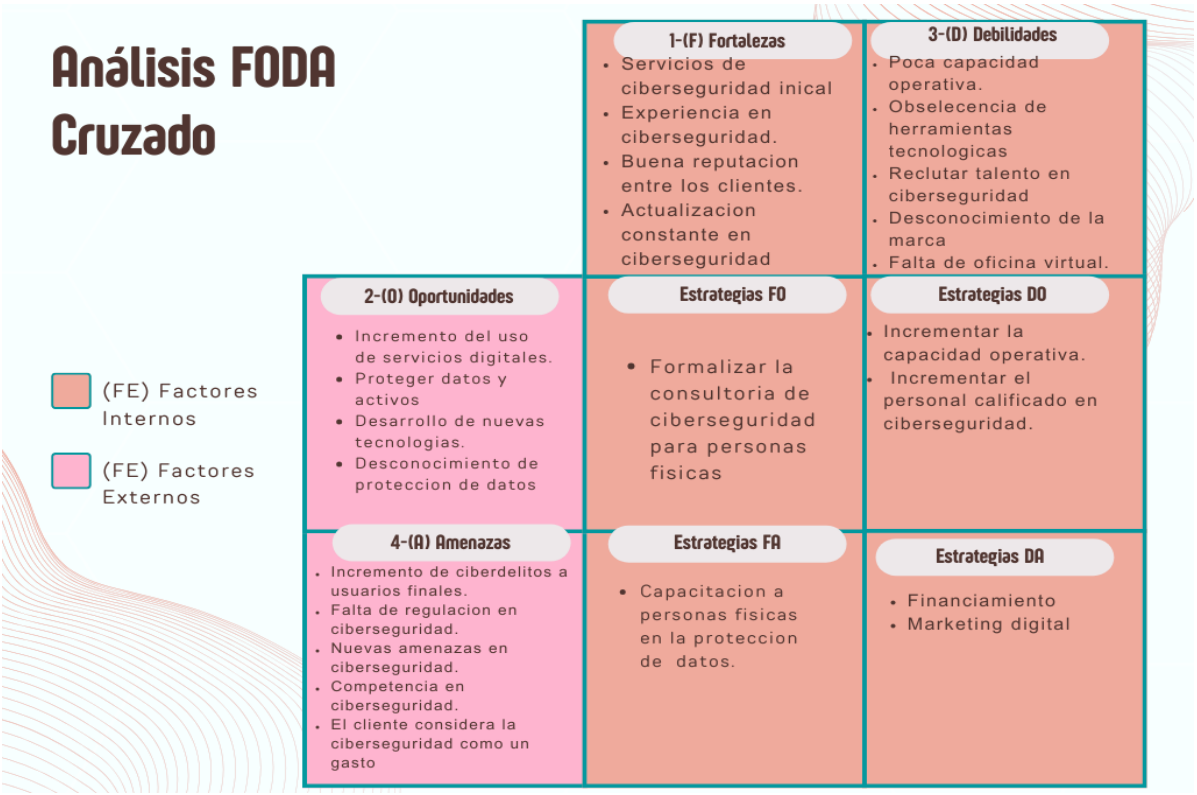
Análisis FODA

Nota. Elaboración propia del autor.

A continuación, en la figura 13 se presenta el análisis FODA cruzado como herramienta para determinar las estrategias a emplear para el emprendimiento de la consultoría de ciberseguridad para personas físicas.

Figura 13

Análisis FODA cruzado



Nota. Elaboración propia del autor.

Las estrategias resultantes del análisis son las siguientes:

- Formalizar la “consultoría de seguridad informática Personal”: permitirá llevar la propuesta de valor a más personas.
- Incrementar la capacidad operativa: permitirá incrementar las ganancias mediante el incremento de oferta de servicios y atención a clientes.
- Incrementar el personal calificado en ciberseguridad: asegura la calidad en los servicios ofrecidos a los clientes establecidos y nuevos clientes en materia de ciberseguridad.

- Financiamiento: presentar la propuesta a futuros inversionistas
- Marketing digital: buscar campañas en redes sociales, para ofertar los servicios de la consultoría “Seguridad Informática Personal”
- Capacitar a personas físicas (profesionales) en la protección de datos, pretende cambiar la forma del consumidor final de que la ciberseguridad es un gasto a la que es una inversión.

4.3.3 Análisis de mercado

4.3.3.1 Mercado América Latina

El tamaño del mercado latinoamericano de ciberseguridad se estima en 8,92 mil millones de dólares en 2024, y se espera que alcance los 12,48 mil millones de dólares en 2029, creciendo a una tasa compuesta anual del 6,95% durante el período previsto (2024-2029). (Mordor Intelligence, 2023).

En América Latina, el cibercrimen se ha manifestado principalmente a través de estrategias de piratería informática como malware, phishing y ataques de denegación de servicio (DoS). Además, el creciente sesgo de los consumidores de la región hacia los pagos móviles está impulsando la necesidad de seguridad en las aplicaciones a medida que los pagos basados en aplicaciones se generalizan y aumenta la inversión en la creación de aplicaciones de pago.

El área necesita más profesionales con habilidades que beneficien al sector de la ciberseguridad. Según una evaluación del Banco Interamericano y la Organización de los Estados Americanos, la zona de América Latina y el Caribe (ALC) necesita estar mejor equipada para hacer frente a los ciberataques.

4.3.3.2 Mercado México

El sector de ciberseguridad en México está mostrando un crecimiento rápido debido al incremento en la penetración de internet, el aumento de los delitos cibernéticos y la adopción de tecnologías avanzadas. El uso en expansión de tecnologías como IoT y la inteligencia artificial está impulsando el desarrollo de este sector. Se espera que la acelerada urbanización y digitalización, junto con el creciente interés en las plataformas de comercio electrónico y la aparición de dispositivos inteligentes, impulsen aún más el mercado de ciberseguridad en México. La tendencia hacia la digitalización y la adopción masiva de sistemas de banca en línea han causado transformaciones significativas en el sector financiero del país. El Gobierno mexicano está aumentando sus inversiones y desarrollando estrategias para combatir la ciberdelincuencia, ya que es una de las regiones de América Latina con más ciberataques. (Mordor Intelligence, 2023).

A través de la “Plataforma CERT-MX”, ubicada en el sitio web https://www.gob.mx/gncertmx, los ciudadanos pueden reportar delitos cibernéticos, y recibir recomendaciones en materia de ciberseguridad; debido a que en este sitio se emiten alertas y boletines de seguridad informática a la ciudadanía.

Con el objeto de atender el incremento de denuncias ciudadanas por diversos fraudes cibernéticos, se implementaron las siguientes campañas de prevención: “Internet seguro para todas y todos” y “Antifraude Cibernético”, ambas con el objeto de difundir las medidas de seguridad, recomendaciones y medios de contacto al ciudadano, para la prevención de fraudes cibernéticos. A través de las 32 unidades de policía cibernética de las entidades federativas, en colaboración con la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros y la Procuraduría Federal del Consumidor, se lograron 171 millones de visualizaciones en redes sociales de contenido de prevención; 57 mil 507 participaciones ciudadanas y 127 eventos transmitidos en línea, con difusión de contenidos preventivos de ciberseguridad. Por su parte, los operativos nacionales denominados “Ciber-Guardián”

“Salvación”, y tienen como propósito combatir el delito de pornografía infantil que es común en las redes sociales. Ambos operativos permitieron la detención de 24 probables responsables del delito de pornografía infantil y el rescate y/o identificación de 26 menores de edad víctimas de este delito. (Guardia Nacional, 2022).

4.3.3.3 Mercado Estado de México

De acuerdo con las incidencias reportadas por la policía cibernética del Estado de México como se puede observar en la tabla 8 Incidencias cibernéticas reportadas semestre Enero - Junio 2023, entre las más altas se encuentran: acoso cibernético con 2556, fraude al comercio electrónico con 1172, robo de contraseñas con 1150, suplantación de identidad 633, extorsión cibernética con 492, entre otras. (Miranda, 2024).

Tabla 8

Incidencias cibernéticas reportadas semestre Enero - Junio 2023

Año	Incidencia cibernética	Número de reportes
2023	Acoso cibernético	2556
2023	Fraude al comercio electrónico	1172
2023	Robo de contraseñas	1150
2023	Suplantación de identidad	633
2023	Extorsión cibernética	492
2023	Orientación	460
2023	Amenazas cibernéticas	343
2023	Fraude al usuario de la banca electrónica	141
2023	Acoso de menores	98
2023	Ciberbullying	93
2023	Spam	86
2023	Amenazas a menores	76
2023	Fraude nigeriano	76
2023	Acceso Lógico no autorizado	71
2023	Acoso sexual	65
2023	Usurpación de Identidad	53
2023	Extorsión a menores	51
2023	Porno venganza	44
2023	Difamación de menores	33
2023	Fraude contra menores	19
2023	Robo	12
2023	Sexting	11
2023	Menor desaparecido	8
2023	Pornografía infantil	4
2023	Persona desaparecida	3
2023	Grooming	2
2023	Virus	1
2023	Pedofilia	1
2023	Corrupción de menores	1
2023	Maltrato animal	1
2023	Delitos contra la salud	1

*Nota***.** Numero de reportes de incidencias de Enero-Junio 2023, fuente: Información estadística generada por la Policía Cibernética del Estado de México

Teniendo en cuenta que los expertos Cisco Systems, Inc, IBM Corporation, Intel Corporation, Cyber Ark Software Ltd, Dell Inc, CrowdStrike, Inc, Sophos Ltd., Palo Alto Networks, Inc, Fortinet, Inc, y Trend Micro Incorporated, entre otras, indican que estas cifras seguirán en aumento.

4.3.3.4 Sector

De acuerdo con el Centro de Habilidades de la OCDE, la dependencia de las tecnologías en la vida diaria hace que las personas sean más vulnerables a ataques cibernéticos, además, con esquemas de trabajo remotos que se aceleraron en la pandemia, la vulnerabilidad ante las amenazas en los espacios digitales también creció; teniendo esto en cuenta la empresa Consultoría de Seguridad Informática Personal se desarrolla en el sector terciario en el segmento de servicios; con el propósito de especializar y capacitar a las personas físicas víctimas del robo de datos, suplantación de identidad o fraude.

4.3.3.5 Competidores

La cantidad de empresas de consultoría en México y en Latinoamérica es alta, sin embargo, en los temas de ciberseguridad recién se están conformando los especialistas. La competencia de consultoría en ciberseguridad a personas físicas se da mayormente por independientes que carecen de la experiencia y conocimientos necesarios y no por empresas de consultoría debidamente organizadas y estructuradas para tal fin, como se confirmó luego de las diversas encuestas realizadas.

Consultoría de Seguridad Informática Personal está enfocada en alcanzar la especialización y el prestigio entre sus clientes, esto marca un camino de éxito para competir adecuadamente con el espacio suficiente para desarrollarse. Para ello Consultoría de Seguridad Informática Personal tiene dentro de su cultura organizacional la continua capacitación de sus colaboradores.

Actualmente en México existen pocos especialistas en temas de ciberseguridad para la cantidad de personas físicas que existen, y los que hay están con sus tiempos completamente ocupados en la, estos están apoyando mayormente a las empresas grandes, quienes inclusive ante la falta de personal especializado contratan especialistas internacionales. Se plantea realizar una alianza estratégica con ellos, a fin de que nos deriven con más usuarios que sean denominados fiscalmente personas físicas o empresas pequeñas y medianas que ellos no cubren.

4.3.3.6 Proveedores

Consultoría de Seguridad Informática Personal tendrá como proveedores a los fabricantes de hardware como son: Cisco, WatchGuard, IBM, DELL, HP y a los fabricantes de software se encuentran: Kaspersky, Sophos, WhatchGuard, Microsoft, Google.

Los proveedores de capacitación existen La Asociación Mexicana de Ciberseguridad, Fortinet, Cisco, Google, Coursera.

Los proveedores de conectividad son: Telmex, TotalPlay, IZZI.

Con la categorización anterior la Consultoría de Seguridad Informática Personal tendrá la capacidad operativa para ofertar soluciones accesibles a los futuros clientes.

4.3.4 Segmento de mercado

El segmento de mercado para la consultoría de “Seguridad Informática Personal” es amplio y diverso, abarcando múltiples profesiones que buscan protegerse contra amenazas cibernéticas.

4.3.4.1 Segmentación demanda

Los canales de distribución utilizados para llegar a los consumidores y entregarles la propuesta de valor es por redes sociales y comunidades digitales relacionadas con ciberseguridad, así también se desarrolla una página web de la consultoría en Seguridad Informática Personal para la consulta de servicios y precios.

De acuerdo al análisis de los resultados de las encuestas realizadas el consumidor que se encuentra con actividades relacionadas a la educación en un 24.7%, seguido del 23.7% relacionado a las ventas y un 12.4% a la administración, así también el 50% de los consumidores utiliza en promedio 4hrs al día las redes sociales mientras que 38% consulta alguna comunidad digital relacionada a tecnología; en donde el 25.8% experimento o fue víctima de robo de identidad seguido de un 16.5 % a fue víctima del robo de datos financieros y un 9.3% relacionado fue víctima de fraude por correo electrónico, para resolver alguna de esta problemáticas de ciberseguridad el 31% busca aun experto en ciberseguridad y el 40% en internet la solución. El 32% cuenta con una computadora, internet o dispositivo móvil, mientras que el 16.8% utiliza el servicio de banca en línea y el 20.8% realiza compras en línea.

El 43% de los consumidores actualmente prefiere recibir una consultoría en línea, reforzado con un 49% debido a que opinan que los servicios en línea resuelven los problemas en menos tiempo y son más económicos, un 37% de los consumidores prefieren a que fuese explicado antes el proceso de la posible solución, también el 22.9% sigue consumiendo software de oficina de dudosa procedencia.

Un 50% de los consumidores se encuentra dispuesto a pagar por un servicio de consultoría entre $500 pesos a $1000 pesos y un 58.8% a pagar $350 pesos por un curso relacionado con tecnologías de la información y ciberseguridad.

La segmentación de la demanda se realiza geográfica y demográficamente, en un primer momento se considera geográficamente, para el municipio de Ixtapaluca cuenta con una población de 542,211 habitantes y para Valle de Chalco cuenta con una

población de 391,731 habitantes, para ambos casos corresponden al 100% de sus poblaciones, la suma de estas dos poblaciones es 933,942 habitantes.

Posterior a la segmentación geográfica se realiza la segmentación demográfica, para el desarrollo de la investigación se observa a la población en edad de 25 a 60 años para cada municipio teniendo que Ixtapaluca cuenta con 347,828.36 habitantes que representa el 64.15% del 100% de la población del municipio; en el caso de Valle de Chalco cuenta con una población de 247,809.03 que representa el 63.26 del 100% de la población del municipio económicamente activa, continuando con la segmentación demográfica se realiza por población económicamente activa se observa que en el municipio de Ixtapaluca tiene 208,001.36 habitantes que representan el 59.8% del 64.15% de la población en edad de 25 a 60 años; para el municipio de Valle de Chalco se observa que tiene 148,189.80 habitantes esto representa el 59.8% del 63.26% de la población en edad de 25 a 60 años. Al sumar esta última segmentación demográfica de la población económicamente activa se obtiene una población de 356,192 habitantes, que se convierte en el mercado objetivo de la investigación, se estima que 7123.84 habitantes equivalente a un 0.02% del mercado objetivo podrían estar interesados en contratar servicios de consultoría, si históricamente se convierten estos este 0.02% de leads en un 10% clientes reales tendríamos 712.38 de ventas reales; en la tabla 9 se puede observar una proyección de ventas a un año de acuerdo por servicio.

Tabla 9

Proyección de ventas

MES	Proyección de ventas en unidades	Asesoría 33%	Capacitación 33%	Licencias de Software 33%
Enero	30	10	10	10
Febrero	30	10	10	10
Marzo	30	10	10	10
Abril	30	10	10	10
Mayo	30	10	10	10
Junio	30	10	10	10
Julio	30	10	10	10
Agosto	30	10	10	10
Septiembre	30	10	10	10
Octubre	30	10	10	10
Noviembre	30	10	10	10
Diciembre	30	10	10	10
Total	360			

Nota: Elaboración propia del autor.

4.3.4.2 Segmentación oferta

Existe una necesidad en la especialización y capacitación de las personas físicas víctimas de los delitos de robo de identidad, robo de datos y fraude por correo electrónico por lo que la propuesta de valor está centrada en solventar este tipo de delitos.

El servicio de consultoría se ofertará en línea utilizando plataformas como Facebook, Mercado Libre, Amazon, una página web y crear una comunidad digital propia donde se explica antes el proceso de solución para obtener la opinión positiva que del cliente sobre los servicios de consultoría en línea en los municipios de Valle de Chalco e Ixtapaluca.

El segmento de los clientes se encuentra dirigido a las personas físicas con actividades relacionadas a educación, ventas y administrativos, la mayor parte de las personas físicas encuestadas cuentan con los recursos mínimos en infraestructura (internet,

dispositivo móvil) necesarios de tal manera que se pueda ofrecer el servicio de consultoría en línea, tienen conocimiento sobre la utilización de algunos servicios como, por ejemplo, manejo de apertura de cuentas bancarias, compras en línea, cursos en línea; las personas físicas necesitan un consultor en ciberseguridad por el tipo de actividades que realizan.

La mayor fuente de ingresos para el presente trabajo de investigación se obtendría de los servicios especializados en ciberseguridad, seguida del ofrecimiento de capacitaciones a los clientes y por último la venta software legal, buscando que se encuentre en el rango de precio de $350 pesos a $1000 pesos.

4.3.5 Estrategia de comercialización y marketing.

Del análisis del FODA cruzado las estrategias que buscan incrementar los factores en que se es fuerte y existe una oportunidad, y, por otro lado, las estrategias que limiten las amenazas mejorando las debilidades, a continuación, se listan las estrategias:

- Formalizar la “consultoría de seguridad informática Personal”: permitirá llevar la propuesta de valor a más personas.
- Incrementar la capacidad operativa: permitirá incrementar las ganancias mediante el incremento de oferta de servicios y atención a clientes.
- Incrementar el personal calificado en ciberseguridad: asegura la calidad en los servicios ofrecidos a los clientes establecidos y nuevos clientes en materia de ciberseguridad.
- Financiamiento: presentar la propuesta a futuros inversionistas
- Marketing digital: buscar campañas en redes sociales, para ofertar los servicios de la consultoría “Seguridad Informática Personal”

4.3.5.1 Mapa de empatía.

El mapa de empatía como se observa en la figura 14 recorre los principales puntos que atraviesa un cliente de la consultoría de Seguridad Informática Personal. Este sirve para mejorar la interactividad con el cliente.

Figura 14

Mapa de empatía para la consultoría Seguridad Informática Personal.

Nota: Elaboración Propia del autor.

4.3.5.2 Buyer

El buyer persona se representan las características específicas de un cliente ideal para la consultoría de Seguridad Informática Personal. Como se observa en la figura 15 Buyer del cliente para “Seguridad Informática Personal”.

Figura 15

Buyer del cliente para Seguridad Informatica Personal.

Nota: Elaboración Propia del autor

4.3.5.3 Ubicación

La ubicación de una empresa se refiere al lugar físico donde se lleva a cabo su actividad comercial o industrial. La elección de esta ubicación es estratégica y puede influir significativamente en el éxito de la empresa.

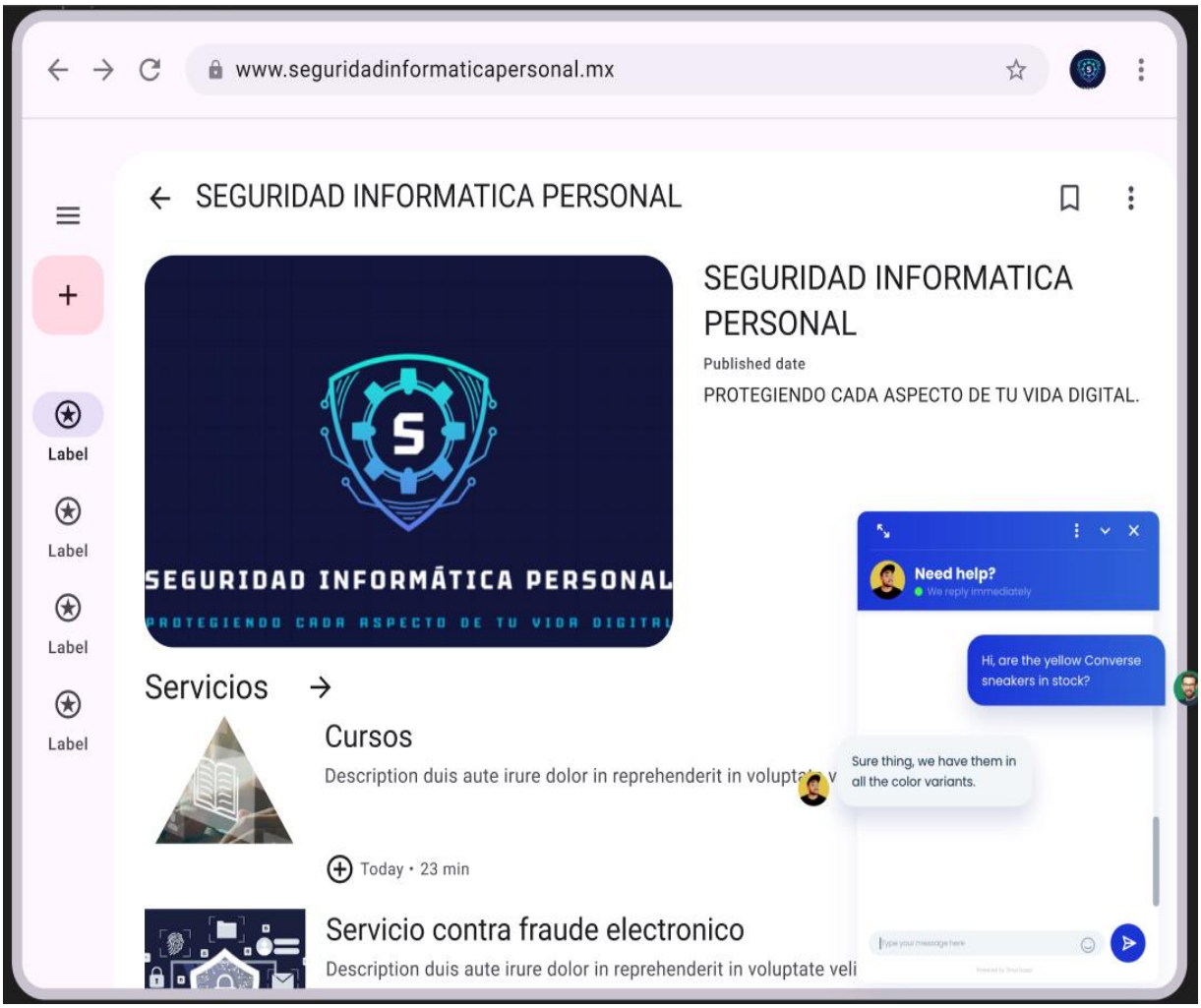
Consultoría en Línea: Seguridad Informática Personal - Especializada en Seguridad Informática a Personas Físicas.

Plataforma y Presencia Digital:

En la figura 16 se observa el Sitio Web: www.seguriinformaticapersonal.mx.

Figura 16

Sitio web de Seguridad Informática Personal



Nota: Elaboración propia del autor.

SEO: Palabras clave como "consultoría de seguridad informática", "ciberseguridad para personas físicas", "auditoría de seguridad digital personal".

Redes Sociales:

- LinkedIn: Publicar artículos sobre ciberseguridad, casos de éxito y novedades del sector.
- Twitter: Compartir noticias de ciberseguridad, tips rápidos y participar en conversaciones relevantes.
- YouTube: Crear videos tutoriales y webinars sobre mejores prácticas de seguridad informática inicial.

Herramientas de Comunicación y Colaboración:

- Videoconferencias: Realizar auditorías y reuniones con clientes mediante plataformas de videoconferencias como los son Google Meet, Zoom.
- Chats en Vivo: Implementar un chat en vivo en el sitio web para consultas inmediatas.
- Emails Profesionales: Usar la dirección de correo profesional (info@seguridadinformaticapersonal.mx) para todas las comunicaciones.
- Marketing Digital:
- Publicidad en Línea: Campañas de WhatsApp dirigidas a empresas que buscan mejorar su seguridad informática.
- Email Marketing: Enviar newsletters mensuales con actualizaciones de seguridad y consejos prácticos.
- Marketing de Contenidos: Blog con artículos sobre temas como protección contra malware, estrategias de ciberseguridad y estudios de caso de clientes.

Recursos y Formación:

- Webinars: Organizar webinars trimestrales sobre las últimas tendencias en ciberseguridad.
- Ebooks y Guías: Ofrecer un ebook gratuito titulado "10 Pasos para Proteger tu información personal digital de Amenazas Cibernéticas" a cambio de suscripciones al boletín informativo.

Esta estrategia integral asegura que la consultoría en línea tenga una presencia fuerte y efectiva, atraiga y retenga a sus clientes, y ofrezca servicios de alta calidad.

4.3.5.4 Marca

La marca es un concepto amplio que abarca diversos elementos y significados en el ámbito empresarial y de marketing. A continuación, se detallan las características y componentes clave de la marca “Seguridad Informática Personal”:

Definición de Marca

Nombre: Seguridad Informática Personal

Logotipo: El símbolo gráfico o diseño que representa visualmente a la marca. Cómo se observa en la figura 17 Logotipo de Seguridad Informática Personal

Figura 17

Logotipo de la marca Seguridad Informática Personal"

Nota: Logotipo de Seguridad Informática Personal, fuente: elaboración propia autor.

Colores y Tipografía: Se utiliza el color azul dado que representa Inteligencia, confianza, seguridad, serenidad, comunicación, eficiencia, lógica, reflexión, calma. La tipografía utilizada es sin serifas dado que se encuentra más ligada a la tecnología e internet representa dinamismo, carácter, modernidad, potencia, seguridad, minimalismo y neutralidad.

Diseño: Las líneas que sobresalen del escudo representan un circuito electrónico, mientras que el escudo representa protección, a las personas que se encuentran unidos que representa un engrane representan procesos, las líneas en curva son las señales wifi que entran o salen las cuales están protegidas por el escudo.
Eslogan: Protegiendo cada aspecto de tu vida digital.

4.3.5.5 Producto.

El producto como estrategia comercial se refiere a la utilización de las características, beneficios y atributos del producto para diferenciarlo en el mercado, atraer y retener clientes y, en última instancia, impulsar las ventas y el crecimiento de la consultoría.

En la consultoría se aplica la estrategia comercial basada en el producto debido a que se obtuvo una comprensión de las necesidades de los clientes, la oferta de alta calidad y el enfoque de marketing y distribución de los clientes de la consultoría. Esto permitirá que la consultoría pueda diferenciarse en el mercado, atraer y retener clientes, y lograr un crecimiento sostenible. A continuación, se detalla de manera general el producto en la figura 18 lienzo de visión del producto.

Figura 18

Lienzo visión del producto

<table>
<tr><td colspan="4">Frase resumen: La propuesta de valor se enfoca en la existente necesidad en la especialización y capacitación de las personas físicas víctimas de los delitos de robo de identidad, robo de datos y fraude por correo electrónico.</td></tr>
<tr><td>Cliente
Personas físicas Ixtapaluca y Valle de Chalco con actividades relacionadas a la educación, ventas y a la administración</td><td>Problema/necesidad
Ciberseguridad individual</td><td>Solución
Ofrecer un servicio de ciberseguridad de alta calidad a las personas físicas</td><td>Valor
El precio bajo.
Servicio de alta calidad.
Servicio de confianza.
Responsabilidad social.</td></tr>
<tr><td colspan="2">Rivales
Empresas con actividades en ciberseguridad
Empresas con actividades similares en ciberseguridad.</td><td colspan="2">Diferenciadores
Oferta precio bajo (accesibles) y de alta calidad, como elementos para generar la confianza en las personas físicas con residencia en Valle de Chalco e Ixtapaluca en servicios de solución de problemas en ciberseguridad.</td></tr>
</table>

Nota: Elaboración propia.

4.3.5.5.1 Costos de producción.

La empresa cuenta con 3 líneas de servicio. En la tabla 10 se observa los costos de la primera línea de servicio que consisten en asesoría en ciberseguridad para prevenir o solventar problemáticas derivadas del robo de identidad, phishing de correo electrónico, secuestro de información.

Tabla 10

Costo de producción del servicio de asesorías

Servicio	Materiales	Total, costo unitario	Personal	Total, de remuneración
Asesorías de ciberseguridad para prevenir ó solventar las problemáticas de robo de identidad, phishing en correo electrónico, secuestro de información	• Laptop. • Sitio web. • Plataforma de conexión remota.	$ 7,598.40	Producción-remuneraciones • Gerente de operaciones. Administración y ventas • Administrativo • Ventas	 $ 2,333.33 $ 1,666.67 $ 1,666.67

Nota: Elaboración propia del autor.

El segundo servicio consiste en capacitación a las personas físicas que así lo requieran en temas de ciberseguridad personal, para prevenir ser víctima de algún ciberdelito; como se observa en la tabla 11 el costo de la capacitación.

Tabla 11

Costo de producción del servicio de capacitación.

Servicio	Materiales	Costo de materiales	Personal	Costo por mano de obra
Capacitación en temas básicos de ciberseguridad personal.	• Laptop. • Sitio web. • Proyector • Plataforma de videoconferencia	$ 5,469.00	• Gerente de operaciones. • Administrativo • Ventas	$ 2,333.33 $ 1,666.67 $ 1,666.67

Nota: Elaboración propia

El tercer servicio es la venta del licenciamiento de software, para comenzar a dar formalidad y legalidad a las personas físicas el software con licencia da la seguridad de contar con las ultimas actualizaciones de seguridad que proporciona el proveedor. A continuación, en la tabla 12 se observa el costo de producción del servicio de licenciamiento de software.

Tabla 12

Costo de producción del servicio de licenciamiento de software

Servicio	Materiales	Costo de materiales	Personal	Costo mano de obra
Venta de licencias de software	• Laptop. • Licencias • Sitio web • Plataforma de comercio electrónico	$15,613.68	• Gerente de operaciones. • Administrativo • Ventas	$ 2333.33 $ 1,666.67 $ 1,666.67

Nota: Elaboración propia del autor.

4.3.6 Análisis de la capacidad operativa

El espacio de trabajo será de 12m^2 desde el cual se darán los servicios ofertados en el sitio web. El local se encontrará ubicado en av. Circuito del Sol núm. 47 casa 3B colonia cuatro vientos municipio de Ixtapaluca.

Los servicios serán ofertados en un principio en los municipios de Valle de Chalco e Ixtapaluca de utilizando el marketing de Facebook.

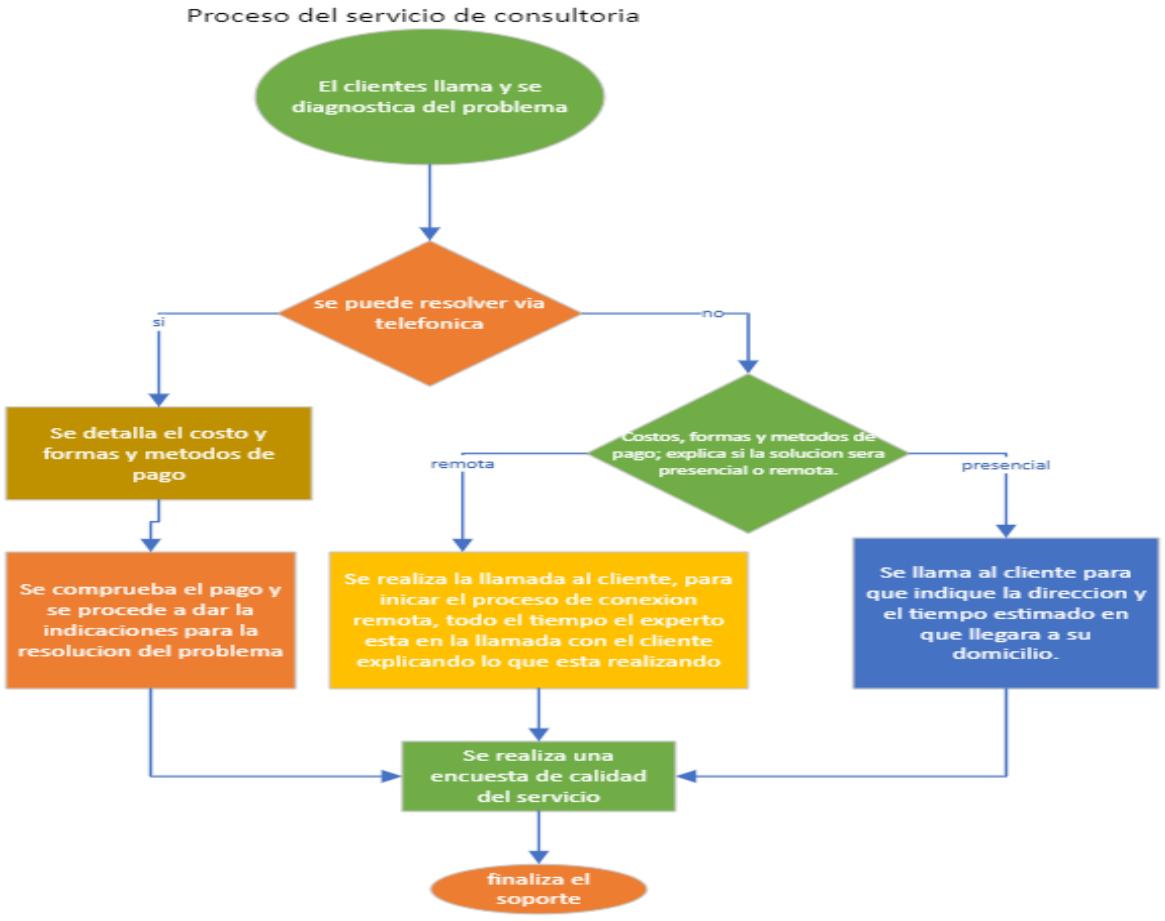
4.3.6.1 Equipos y herramientas.

En el caso de la consultoría “Seguridad Informática Personal”, en lo que tendrá inversión será en lo siguiente:

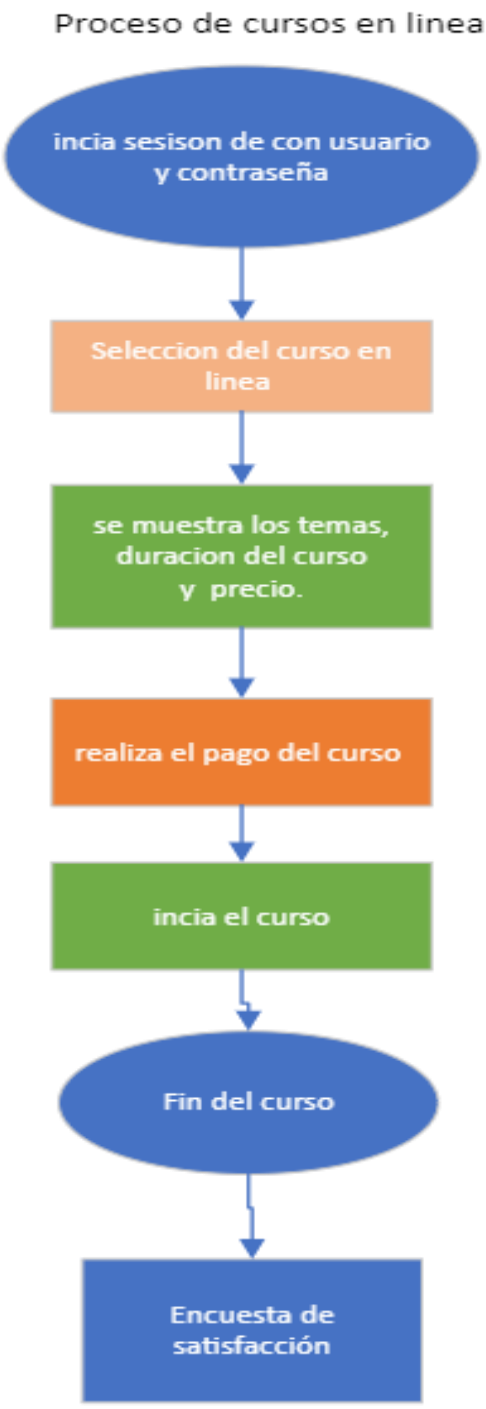
- Computadoras
- Internet
- Software especializado
- Dispositivo móvil

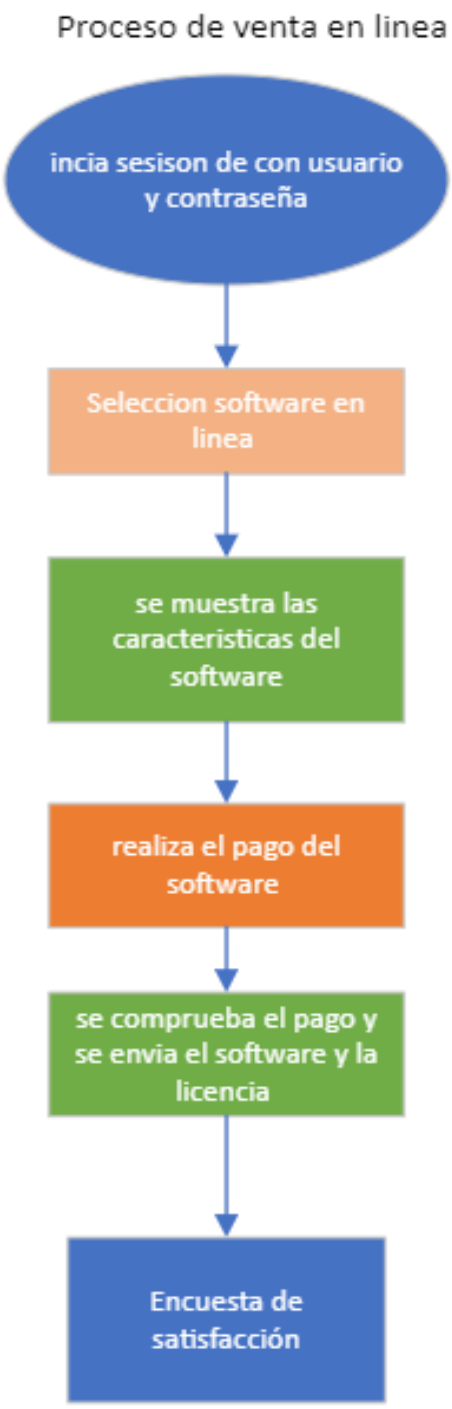
4.3.6.2 Procesos

La consultoría está en un proceso de adaptación y adecuación del producto en función a los clientes. A continuación, se presenta el proceso de obtención del servicio:



Se muestra el proceso de cursos y venta en línea que seguirá la consultoría de Seguridad: Informática.





4.3.6.3 Diferenciación del cliente

A través de la diferenciación del cliente, la consultoría de Seguridad Informática Personal podrá personalizar los productos, servicios y comunicaciones para atender de manera más efectiva a cada grupo de clientes, mejorando así la satisfacción del cliente y fomentando la lealtad, manteniendo una ventaja competitiva en el mercado.

La consultoría en Seguridad Informática Personal atenderá principalmente a 3 segmentos de clientes:

- Segmento 1: Educación (25-60 años) interesados en proteger su información digital personal.
- Segmento 2: Administración (25-60 años) interesados en proteger su información digital personal o de sus clientes.
- Segmento 3: Ventas (25-60 años) interesados en proteger su información digital personal o relacionada a sus actividades.

Los productos y servicios que se ofrecerán son cursos sobre soluciones actualizadas, y promociones para la implementación en las soluciones, venta de software con licencia, asesoría en seguridad informática de acuerdo con sus actividades.

Se realizarán las campañas de marketing en redes sociales. Newsletters con consejos de estilo y promociones exclusivas. Anuncios en blogs y revistas de ciberseguridad, correos electrónicos con promociones y recomendaciones de productos.

Se dará una experiencia al cliente con una navegación rápida y fácil en el sitio web, chat en vivo para resolver dudas de ciberseguridad; así también se ofrecerá una entrega rápida y opciones de devolución, un programa de fidelización para compras recurrentes. Asistencia personalizada en la solución y selección de productos, relacionados a ciberseguridad.

Utilizar herramientas de análisis para recopilar datos sobre el comportamiento de los clientes, sus preferencias y patrones de compra con ello dividir a los clientes en segmentos basados en criterios relevantes. Crear estrategias de marketing, ventas y servicio al cliente adaptadas a las características y necesidades de cada segmento.

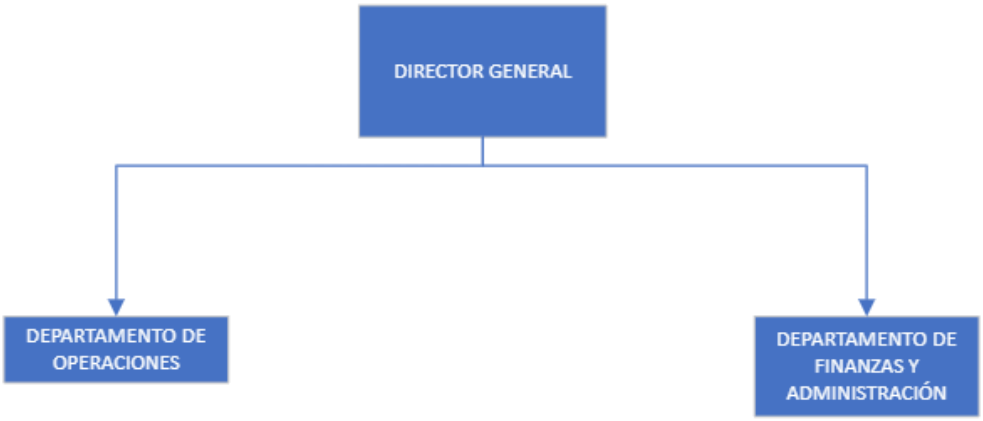
Implementar las estrategias y asegurarse de que todos los equipos de la empresa están alineados con el enfoque de diferenciación del cliente. Monitorear continuamente el rendimiento de las estrategias y ajustar según sea necesario para asegurar la efectividad y la satisfacción del cliente.

4.3.7 Estructura organizacional

La consultoría tendrá una estructura organizacional funcional como se observa en la figura 19 Organigrama de la consultoría de Seguridad Informática Personal.

Figura 19

Organigrama de la consultoría de Seguridad Informática Personal



Nota. Elaboración propia del autor

A continuación, se procede a definir las funciones de los cargos de la consultoría de Seguridad Informática Personal.

1. Director general: Responsable de la visión y dirección estratégica de la consultoría. Supervisa todas las operaciones y departamentos.
2. Departamento de Operaciones: Es el departamento responsable de realizar las evaluaciones de seguridad, análisis de riesgos y pruebas de penetración de forma remota. Proporcionan recomendaciones, cursos y soluciones personalizadas a los clientes.
3. Departamento de Finanzas y Administración: Manejan las cuentas, registros y reportes financieros; apoyar en las ventas y marketing a través de redes sociales.

4.3.8 Análisis de costo

El análisis de costos es un método que permite evaluar si el proceso de “Seguridad Informática Personal” es rentable. Se contemplan 3 servicios los cuales se mencionan a continuación: Asesoría, Capacitación y Venta de licenciamiento de software.

En la tabla 13 Costos de materiales e insumos de producción del servicio de asesoría se observa que ascienden a un total de $7598.40 pesos, se espera ofrecer 10 servicios al mes, resultando en un costo por unidad de $759.84.

Tabla 13

Costos de materiales e insumos directos

Material	**Cantidad requerida**	**Precio unitario ($)**	**Total, costo ($)**
Laptop	1	$ 5,999.00	$ 5,999.00
Sitio web	1	$ 219.00	$ 219.00
Plataforma para conexión remota	1	$ 1,380.40	$ 1,380.40
Total, costo unitario por concepto materiales e insumos directos			$ 7598.40

Nota: Elaboración propia del autor

Como se observa en la tabla 14 Costos de materiales e insumos de producción del servicio de capacitación con un total de $5751.33 pesos, se espera ofrecer 10 servicios al mes, resultando en un costo por unidad de $575.13.

Tabla 14

Costos de materiales e insumos del servicio de capacitación

Material	**Cantidad requerida**	**Precio unitario ($)**	**Total, costo ($)**
Laptop	1	$ 4,276.00	$ 4,276.00
Proyector	1	$ 974.00	$ 974.00
Sitio web	1	$ 219.00	$ 219.00
Plataforma de videoconferencia	1	$ 282.33	$ 282.33
Total, costo unitario por concepto materiales e insumos directos			$ 5,751.33

Nota: Elaboración propia del autor

Como se observa en la tabla 15 Costos de materiales e insumos de producción del servicio de venta de licenciamiento de software, con un total de $15,613.68 pesos, se espera vender 10 licencias al mes, resultando en un costo por unidad de $1,561.36.

Tabla 15

Costos de producción de venta de licenciamiento de software.

Material	**Cantidad requerida**	**Precio unitario ($)**	**Total, costo ($)**
Licencias de software	10	$ 1,136.80	$ 11,368.00
Laptop	1	$ 3,727.00	$ 3,727.00
Sitio web	1	$ 219.00	$ 219.00
Plataforma de comercio electrónico	1	$ 299.68	$ 299.68
Total costo unitario por concepto materiales directos			**$ 15,613.68**

Nota: Elaboración propia del autor

En la tabla 16 Remuneración mensual del personal de producción, cabe mencionar que se encuentra prorrateado entre los 3 servicios el sueldo mensual del personal mano de obra directa, el costo total de remuneraciones producción, concepto de mano de obra directa es de $ 7,000.00, se espera ofrecer 10 unidades por cada servicio al mes, resultando en un costo por unidad de $700.00.

Tabla 16

Remuneración mensual del personal de producción

(III) Personal de producción-Remuneraciones (cv-directa) mensuales:				
Puesto	**Servicio**	**Cantidad**	**Sueldo mensual**	**Sueldo mensual total**
Gerente de operaciones	Asesorías	1	$ 2,333.33	$ 2,333.33
Gerente de operaciones	Capacitación	1	$ 2,333.33	$ 2,333.33
Gerente de operaciones	Licenciamiento	1	$ 2,333.34	$ 2,333.34
Total remuneraciones producción, concepto de mano de obra directa:				$ 7,000.00

Nota: Elaboración propia del autor

En la tabla 17 Remuneración mensual del personal de administración, cabe mencionar que se encuentra prorrateado entre los 3 servicios el sueldo mensual del personal administración y ventas, el costo total de remuneraciones administrativa y ventas, es de $ 10,000.00, se espera ofrecer 10 servicios al mes, resultando en un costo por unidad de $1,000.00.

Tabla 17

Remuneración mensual del personal de administración y ventas.

(IV) Personal Administración y ventas (cf-indirecta)-Remuneraciones mensuales				
Puesto	**Servicio**	**cantidad**	**Sueldo mensual**	**Sueldo mensual total**
Administrativo				$ 5,000.00
Director general	Asesoría	1	$ 1,666.67	$ 1,666.67
Director general	Capacitación	1	$ 1,666.67	$ 1,666.67
Director general	Licenciamiento	1	$ 1,666.66	$ 1,666.66
Ventas				$ 5,000.00
Gerente de ventas	Asesoría	1	$ 1,666.67	$ 1,666.67
Gerente de ventas	Capacitación	1	$ 1,666.67	$ 1,666.67
Gerente de ventas	Licenciamiento	1	$ 1,666.66	$ 1,666.67
Total, remuneraciones administrativa y ventas:				$ 10,000.00

Nota: Elaboración propia

En la tabla 18 Gastos de operación, son los mismos para los 3 servicios, el total del concepto de gasto de operación es de $10,857.39, se espera ofrecer un total de 30 servicios al mes, resultando en un costo por unidad de $361.91.

Tabla 18

Gastos de operación

(**V) Gastos generales mensuales (cf-costo indirectos)**			
Concepto	**Fijos y sufijos**	**Variables**	**Total**
gastos generales			$ 1,996.95
agua	$ 552.00		$ 552.00
luz (electricidad)	$ 600.00		$ 600.00
telefonía móvil	$ 360.00		$ 360.00
internet	$ 484.95		$ 484.95
gastos administrativos			$ 8,428.02
alquile oficina o bodega (renta)	$ 3,000.00		$ 3,000.00
mobiliario e instalaciones	$ 4,401.00		$ 4,401.00
suministro de oficina y papelería	$ 847.02		$ 847.02
artículos de limpieza	$ 180.00		$ 180.00
gastos de ventas			$ 432.42
Publicidad Facebook		$ 432.42	$ 432.42
Total	$10,424.97	$ 432.42	$ 10,857.39
Total, gastos generales mensuales			$ 10,857.39

Nota: Elaboración propia.

En la tabla 19 se encuentra los gastos preoperatorios que suman $6,458.00 en el caso de la constitución de la empresa se iniciara como persona física con actividad empresarial el trámite es gratuito

Tabla 19

Gastos Preoperatorios

Descripción	**Cantidad requerida**	**Precio unitario ($)**	**Total, costo ($)**
Gastos de constitución empresa			$ -
Personas físicas con actividad empresarial	1	$ -	$ -
Gastos de servicios			$ 4,362.00
contrato de internet, cable, teléfono	1	$ 519.00	$ 519.00
contrato de agua	1	$ 3,190.00	$ 3,190.00
contrato de luz	1	$ 653.00	$ 653.00
Gastos de capacitación			**$ 2,096.00**
Certificación en ciberseguridad	1	$ 2,096.00	$ 2,096.00
Total, de preoperatorios intangibles			**$ 6,458.00**

Nota: Elaboración Propia

En la tabla 20 se observa el cálculo de la depreciación y amortización a 5 años con un total en su valor residual por $2,786.50.

Tabla 20

Depreciación y Amortización

DEPRECIACION								
Concepto	**%**	**Monto**	**Año 1**	**Año 2**	**Año 3**	**Año 4**	**Año 5**	**Valor residual**
Equipo de computo	30 %	$ 14,975.99	$ 4,492.80	$ 4,492.80	$ 4,492.80	$ 1,497.60	$ -	$ -
Mobiliario para oficina	10 %	$ 4,401.00	$ 440.10	$ 440.10	$ 440.10	$ 440.10	$ 440.10	$ 2,200.50
Total, de depreciación		$ 19,376.99	$ 4,932.90	$ 4,932.90	$ 4,932.90	$ 1,937.70	$ 440.10	$ 2,200.50
	AMORTIZACION (intangibles)							
Concepto	**%**	**Monto**	**Año 1**	**Año 2**	**Año 3**	**Año 4**	**Año 5**	**Valor residual**
Contrato de internet telefónico	10 %	$ 519.00	$ 51.90	$ 51.90	$ 51.90	$ 51.90	$ 51.90	$ 259.50
Contrato de luz	10 %	$ 653.00	$ 65.30	$ 65.30	$ 65.30	$ 65.30	$ 65.30	$ 326.50
Total, de amortización		$ 1,172.00	$ 117.20	$ 117.20	$ 117.20	$ 117.20	$ 117.20	$ 586.00
Total, de Depreciación y Amortización		$ 20,548.99	$ 5,050.10	$ 5,050.10	$ 5,050.10	$ 2,054.90	$ 557.30	$ 2,786.50

Nota: Elaboración propia

Una vez recabados los costos se procede a calcular el precio de venta unitario de cada uno de los servicios utilizando la siguiente formula

$$P = \frac{CT}{1 - U}$$

$P = Precio\ unitario\ de\ venta$

$CT = Costos\ totales$

$U = Utilidad\ esperada$

Cómo se observa en la tabla 21 que el coste total de producción es $ 993.17 y con una utilidad del 30% con lo cual el precio unitario es de $ 1,418.82, suma el IVA del 16% el precio de venta unitario del servicio de asesoría es de $1,645.83.

Tabla 21

Costo y Precio Unitario del servicio de asesoría

Costo por concepto de consumo de materiales por		$	621.80
Costo por concepto de mano de obra por		$	233.33
Costo por concepto de otros insumos por		$	138.04
Total, costo unitario de fabricación		**$**	**993.17**
TOTAL, DE COSTO Y GASTOS (producción)		**$**	**993.17**
Margen de utilidad	30.00%	$	425.65
PRECIO UNITARIO DEL …		**$**	**1,418.82**
IVA incluido del …	16.0%	$	227.01
PRECIO UNITARIO DEL … (venta)		**$**	**1,645.83**

Nota: Elaboración propia del autor

En la tabla 22 Costo y Precio Unitario del servicio de capacitación se observa que el coste total de producción es $ 808.47 y con una utilidad del 30% con lo cual el precio unitario es de $ 1,154.95, suma el IVA del 16% el precio de venta unitario del servicio de asesoría es de $1,339.74.

Tabla 22

Costo y Precio Unitario del servicio de capacitación

Costo unitario de fabricación (Costos Variables Directos)			
Costo por concepto de consumo de materiales por …		$	546.90
Costo por concepto de mano de obra por …		$	233.33
Costo por concepto de otros insumos por …		$	28.23
Total, costo unitario de fabricación		$	808.47
TOTAL, DE COSTO Y GASTOS (producción)		$	808.47
Margen de utilidad	30.00%	$	346.49
PRECIO UNITARIO DEL …		$	1,154.95
IVA incluido del …	16.0%	$	184.79
PRECIO UNITARIO DEL … (venta)		$	1,339.74

Nota: Elaboración propia del autor.

En la tabla 23 Costo y Precio Unitario del servicio de licenciamiento de software se observa que el coste total de producción es $ 808.47 y con una utilidad del 30% con lo cual el precio unitario es de $ 1,154.95, suma el IVA del 16% el precio de venta unitario del servicio de asesoría es de $1,339.74.

Tabla 23

Costo y Precio Unitario del servicio de licenciamiento de software

Costo unitario de fabricación (Costos Variables Directos)			
Costo por concepto de consumo de materiales por		$	1,531.40
Costo por concepto de mano de obra por …		$	233.33
Costo por concepto de otros insumos por …		$	29.97
Total, costo unitario de fabricación		$	1,794.70
Total, de costo y gasto (producción)		$	1,794.70
Margen de utilidad	20.00%	$	448.68
Precio unitario del …		$	2,243.38
IVA incluido del …	16.0%	$	358.94
Precio unitario del … (venta)		$	2,602.32

Nota. Elaboración propia del autor.

Una vez calculado el precio unitario de venta de cada uno de los servicios ofertados, se realiza la proyección de las ventas a un año, como se observa en la tabla 24 que vender 360 servicios, el total del costo de producción promedio es $ 3,596.34, mientras que el precio promedio de venta es de $ 4,817.15.

Tabla 24

Concentrado de precio de costo y venta a un año

Concepto	**Cantidad**	**Porcentaje capacidad producción**	**Costo producción**	**Precio venta**
Asesoría especialidad de ciberseguridad	120	33%	$ 993.17	$ 1,418.82
Actualización y manejo de nuevas tecnologías en ciberseguridad	120	33%	$ 808.47	$ 1,154.95
Legalidad del software	120	33%	$ 1,794.70	$ 2,243.38
Productos totales	**360**	**100%**		
	Costo producción promedio		**$3,596.34**	
			precio promedio venta	**$ 4,817.15**

Nota. Elaboración propia del autor

En la tabla 25 se observa el concentrado de costos y precios unitarios el cual tiene un costo total de producción es por la cantidad de $ 3,596.00, se calcula un margen del 30.78% equivalente a la cantidad de $ 1,599.26 este importe sumado al costo total de producción nos indica que el precio unitario es por $ 5, 915.60 sumando la cantidad de $ 831.30 por concepto del IVA, se obtiene el precio unitario de venta por la cantidad de $6,026.90.

Tabla 25

Concentrado de costo y precio unitario

Costo unitario de fabricación (Costos Variables Directos)			
Costo por concepto de consumo de materiales		$	2,700.10
Costo por concepto de mano de obra		$	700.00
Costo por concepto de otros insumos por …		$	196.24
Total, costo unitario de fabricación		**$**	**3,596.34**
TOTAL, DE COSTO Y GASTOS (producción)		**$**	**3,596.34**
Margen de utilidad	30.78%	$	1,599.26
PRECIO UNITARIO DEL		**$**	**5,195.60**
IVA incluido del …	16.0%	$	831.30
PRECIO UNITARIO DEL (venta)		**$**	**6,026.90**

Nota. Elaboración propia del autor

Los datos que se observan en la tabla 25, sirven para realizar el cálculo del punto de equilibro, se utiliza la siguiente formula:

$$PE = \frac{Costos\ Fijos}{Precio\ de\ Venta\ Unitario - Costo\ Variable\ Unitario}$$

se debe de tener en cuenta que los costos fijos están compuestos por el total de la suma del costo materiales e insumos, la cual representa $ 2,896.34 y mano de obra directa que tiene la cantidad de $700; ambas cantidades multiplicadas por el volumen

de producción a un año equivalente a 360; se obtiene como costo fijo la cantidad de $ 1,294,682.76. Sustituyendo los valores en la ecuación anterior:

$$PE = \frac{1{,}294{,}682.76}{5195.60 - 0} = 249\ servicios$$

se requiere vender 249 servicios para que la empresa se mantenga su operación y cubrir sus gastos.

En la tabla 26 se presenta el plan de inversión con la asignación de activo fijo, gastos preoperatorios y capital de trabajo, todo en su conjunto da un total de $ 205,206.81, esta cantidad será prorrateada con los inversionistas.

Tabla 26

Plan de inversión

Rubro	**Valor Unitario**	**Unidad Req.**	**Inversión Total**
1. Activo Fijo			
Muebles y enseres	$ 19,376.99	1	$ 19,376.99
Total, Activos Fijos			**$ 19,376.99**
2. Gastos Preoperatorios (diferida)			
preoperatorio	$ 6,458.00	1	$ 6,458.00
Total, de gastos preoperatorios			**$ 6,458.00**
3. Capital de trabajo			
Materia prima e insumos	$ 86,890.23	1	$ 86,890.23
Mano de Obra	$ 51,000.00	1	$ 51,000.00
gastos de fabricación (operación)	$ 32,572.17	1	$ 32,572.17
Total, de Capital de Trabajo			**$ 170,462.40**
Total, Inversión			**$ 196,297.39**

Nota. Elaboración propia del autor

En la tabla 27 se presenta la inversión necesaria debe ser al menos de $196,297.39, para esto en el financiamiento se consideran a tres, el Socio A con un monto de $100,000.00 equivalente a una participación del 47.6%, el Socio B con un monto de $100,000.00 equivalente a una participación del 47.6%, el Socio C con un monto de $10,000.00 equivalente a una participación del 4.8%, dando un total de $210,000.00, con esta estrategia se financia el proyecto con dinero propio evitando los intereses que generaría un préstamo de alguna institución financiera.

Tabla 27

Financiamiento

Socios	**Monto**		**%participación**
Socio A	$	100,000.00	47.6%
Socio B	$	100,000.00	47.6%
Socio C	$	10,000.00	4.8%
Total, aportación de capital	**$**	**210,000.00**	**100.0%**
Total, financiamiento	**$**	**210,000.00**	**100.0%**

Nota: Elaboración propia del autor

En la tabla 28 es la proyección de ventas en unidades - ingresos por ventas, estimando las ventas con una inflación del 10% en un periodo de 5 años la estimación es de $8,629,869.97. Esta proyección permite a la empresa utilizar la información de ventas pasadas para identificar tendencias y patrones; para la toma de decisiones de las estrategias a ejecutar, para el logro de los objetivos planteados a un mediano plazo.

Tabla 28

Proyección de ventas

			Precio de Venta Proyecto					
Determinar la proyección de ventas en unidades- ingresos por ventas-P.E			$ 5,195.60	$ 5,715.16	$ 6,286.68	$ 6,915.35	$ 7,606.88	
Producto	**Incremento/Inflación**	**Cant.prod año/precio**			**periodos**			**Total**
			1	**2**	**3**	**4**	**5**	
Seguridad Informática Personal	10%	$ 249.19	$ 249.19	$ 259.21	$ 269.93	$ 280.46	$ 291.74	$ 1350.22
			$1,294,682.76	$1,481,401.91	$1,695,049.69	$1,939,509.76	$2,219,225.85	$8,629,869.97
Ingresos por venta anual			$1,294,682.76	$1,481,401.91	$1,695,049.69	$1,939,509.76	$2,219,225.85	$8,629,869.97

Nota: Elaboración propia del autor

La proyección de costos permitirá a la empresa “Sistemas de Seguridad Personal” prever los recursos necesarios y realizar los ajustes de manera pertinente. Como se observa en la tabla 29 Proyección de costos.

Tabla 29

Proyección de costos

Precio de Costo Producción Proyectado								
			$ 3,596.34	$ 3,955.98	$ 4,351.57	$ 4,786.73	$ 5,264.40	
Producto	**Incremento/Inflación**	**Cant prod año/precio**	**periodos**					**Total**
			1	**2**	**3**	**4**	**5**	
Seguridad Informática Personal	10%	$ 249.19	$ 249.19	$ 274.11	$ 301.52	$ 331.67	$ 364.84	$ 1,521.32
			$896,165.56	$1,084,360.33	$1,312,075.99	$1,587,611.95	$1,921,010.46	$6,801,224.29
Costos de producción por venta anual			$896,165.56	$1,084,360.33	$1,312,075.99	$1,587,611.95	$1,921,010.46	$6,801,224.29

Nota: *Elaboración propia del autor.*

En la proyección de gastos se consideran los gastos administrativos, gastos de venta y gastos financieros, como se puede observar en la tabla 30, una proyección de gastos en un periodo de 5 años con un total de $1,332,373.87.

Tabla 30

Proyección de Gastos

Producto	**incremento/ inflacion**	**cant prod año/Precio**	**Periodos**					**Total**
			1	2	3	4	5	
SEGURIDAD INFORMÁTICA PERSONAL	10%	$256,747	$257,003	$257,260	$257,518	$257,775	$258,033	**$1,287,590**
Gasto anual			$ 257,775.21	$ 258,032.98	$ 1,287,589.74	$ 257,775.21	$ 258,032.98	$ 1,287,589.74

Nota: Elaboración propia del autor.

A continuación, se presenta el desarrollo del flujo de efectivo el cual está determinado en un periodo de 5 años que permite evaluar la liquidez de la empresa “Sistemas de Seguridad Personal” para cubrir sus obligaciones a corto plazo, gastos de operación, gastos de venta. Como se observa en la tabla 31 el efectivo al final del periodo es un total de $ 45,6687.49.

Tabla 31

Flujo de Efectivo

Concepto		Periodos por 5 años						Total
		0	1	2	3	4	5	
Ingresos (A)			$ 1,294,682.76	$ 1,481,401.91	$ 1,695,049.69	$ 1,939,509.76	$ 2,219,225.85	$ 8,629,869.97
Egresos (B)		-$ 196,297.39	$ 1,153,168.98	$ 1,341,620.76	$ 1,569,593.68	$ 1,845,387.16	$ 2,179,043.45	$ 8,088,814.03
Muebles y enseres (oficina, limpieza)		$ 19,376.99						$ 0
Gastos preoperatorios		$ 6,458.00						$ 0
Materia Prima/Insumos		$ 86,890.23						$ 0
Mano de obra		$ 51,000.00						$ 0
gastos de fabricación (operación)		$ 32,572.17						$ 0
Saldo antes de impuestos (A-B)		-$ 196,297.39	$ 141,513.78	$ 139,781.15	$ 125,456.01	$ 94,122.60	$ 40,182.41	$ 541,055.94
Impuestos	16%		$ 22,642.20	$ 22,364.98	$ 20,072.96	$ 15,059.62	$ 6,429.19	$ 86,568.95
Saldo económico (C)		-$ 196,297.39	$ 118,871.57	$ 117,416.17	$ 105,383.05	$ 79,062.98	$ 33,753.22	$ 454,486.99
FLUJO NETO (+ Depreciación)			$ 123,804.47	$ 122,349.06	$ 110,315.94	$ 81,000.68	$ 34,193.32	$ 456,687.49
Incremento Neto de efectivo (C+D)		-$ 196,297.39	$ 123,804.47	$ 122,349.06	$ 110,315.94	$ 81,000.68	$ 34,193.32	$ 456,687.49
Efectivo al final del periodo			$123,804.47	$122,349.06	$110,315.94	$81,000.68	$34,193.32	$456,687.49

Nota: Elaboración propia

En la tabla 32 se encuentra calculada el porcentaje de la Tasa Interna de Retorno (TIR) que es la tasa de descuento que tiene un porcentaje del 48% lo que significa que el proyecto es viable económicamente, también que en el momento inicial, iguala los cobros futuros con los pagos, resultando en un Valor Actual Neto (VAN) positivo. El Beneficio-costo es mayor a los costos debido a que el valor 2.63 es mayor a uno indicando que el proyecto es rentable y el periodo de la recuperación de la inversión será en 2 años 1 mes.

Tabla 32

Indicadores

Inversión Inicial	**VAN**	**TIR**	**Tasa 20%**		
-$196,297	$108,482.23	48%	0.20		
VAN COSTOS	**VAN INGRESOS**	**B/C**	**INDICE DE RENTABILIDAD**	**PERIODO DE RECUPERACION INVERSION (PRI)**	
-$159,591.37	$420,224.00	2.63	2.63	-5	2 AÑOS 1 MESES

Nota: Elaboración propia del autor.

Conclusiones

El desarrollo de un modelo de negocio CANVAS de una consultoría en ciberseguridad para personas físicas de los municipios de Ixtapaluca y Valle de Chalco del Estado de México establece en la propuesta de valor satisfacer la creciente demanda de especialización y capacitación para las personas físicas que han sido víctimas de delitos como el robo de identidad, el robo de datos y el fraude por correo electrónico.

Esto implica ofrecer servicios de ciberseguridad, capacitación y venta de software que se ajusten a las necesidades específicas de cada tipo de profesional, y que sean de calidad con sustento científico y tecnológico para garantizar su seguridad. Este tipo de servicios deben ser certificados y de fácil acceso, permitiendo a las personas con físicas llevar a cabo sus actividades diarias de manera independiente y segura. Se entiende la importancia de proporcionar herramientas y conocimientos específicos que permitan a estas personas protegerse y recuperarse de manera efectiva.

Los consumidores potenciales beneficiado del servicio de la consultoría de acuerdo con el estudio de mercado son los relacionados a las áreas de: la educación, ventas y administración. Los servicios de la consultoría se ofrecerán en línea, con asistencia telefónica.

Los canales ideales con los cuales se llegarán a los clientes son el sitio web de la consultoría que tendrá información pertinente a temas de ciberseguridad, las redes sociales como Facebook, TikTok, y WhatsApp.

Un cuarto de la población de entre Ixtapaluca y Valle de Chalco ha sido víctima de robo de identidad, seguido del robo de datos financieros y de fraude por correo electrónico, requieren o buscan un servicio experto en ciberseguridad el mercado es potencial y exponencial la creación de una consultoría en ciberseguridad tendrá una aceptación favorable en el mercado.

La evaluación de la Tasa Interna de Retorno (TIR) indica que el proyecto es viable económicamente, también que, en el momento inicial, iguala los cobros futuros con los pagos.

La propuesta de emprendimiento es rentable derivado del resultado del Valor Actual Neto (VAN) que fue positivo. El Beneficio es mayor a los costos debido a que se obtuvo como valor 2.63, al ser mayor que 1 el proyecto es rentable y el periodo de la recuperación de la inversión será en 2 años 1 mes.

Por último, la existencia de un mercado potencial y expansión para el servicio de ciberseguridad a personas físicas es un apoyo para salvaguardar los activos de estas, considerando los posibles beneficios económicos, tecnológicos y capacitación para las personas físicas de los municipios de Ixtapaluca y Valle de Chalco.

Recomendaciones

Basado en los resultados obtenidos, se sugieren las siguientes líneas de trabajo futuras para continuar con el proyecto, proponiendo lo siguiente:

- La ejecución del modelo de negocio CANVAS.
- Desarrollo del Plan de Negocios para la Consultoría de Ciberseguridad para Personas Físicas de los Municipios de Ixtapaluca y Valle de Chalco
- Investigar la adopción de inteligencia artificial para mejorar la capacidad de análisis y la toma de decisiones, además de completar los datos y mejorar la experiencia del usuario.
- Investigar y evaluar la formación bajo estándares de competencia del CONOCER.
- Realizar nuevamente las entrevistas, para ahondar en el establecimiento de precios originario de las respuestas resultantes durante las entrevistas, con el propósito de mejorar los precios.
- Realizar múltiples entrevistas con clientes potenciales para una muestra más grande.
- Evaluación y valoración de la ampliación del catálogo de servicios a partir de la información recibida de entrevistas a expertos del sector.
- Considerar una situación en la que el capital de los socios se combina con una cuenta bancaria para obtener deducciones fiscales.
- Evaluar una situación en la que se incluya un socio externo para reducir el riesgo que presenta la inversión.
- Se recomienda realizar nuevamente el análisis FODA luego del establecimiento y funcionamiento de la empresa para poder actualizar y adaptar la estrategia en caso de ser necesario en base a la información obtenida.
- Dirigirse a los competidores existentes para obtener una comprensión más profunda de sus ofertas y ampliar su panorama competitivo.

Referencias.

Aguilera Díaz, A. (16 de septiembre de 2017). *El costo-beneficio como herramienta de decisión en la inversión en actividades científicas.* Obtenido de Cofin Habana: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2073-60612017000200022&lng=es&tlng=es.

Aldeco-Perez, R. &.-A.-G. (2020). *Introducción a la Ciberseguridad y sus aplicaciones en México.* México: Academia Mexicana de Computación, A. C.

Alexandra, R. C. (2021). *Diseño de un modelo de negocio para ofrecer servicios de seguridad de la información a Pymes del sector salud en Bogotá.* Bogotá: Doctoral dissertation, UNIVERSIDAD EAFIT.

Amazon Web Services Inc. (Enero de 2023). *¿Que es la ciberseguridad?* Obtenido de aws.amazon.com: https://aws.amazon.com/es/what-is/cybersecurity/

Baca Urbina, G. (2013). Costo de capital o tasa mínima aceptable de rendimiento. En G. Baca Urbina, *Evaluación de proyectos. Septima edición* (págs. 182-199). Mexico: McGRAW-HILL/INTERAMERICANA EDITORES, S.A. DE C.V.

Baca Urbina, G. (2013). Valor presente neto (VPN). Ventajas y desventajas. En G. Baca Urbina, *Evaluación de proyectos. Septima edición.* (págs. 221-222). México: McGRAW-HILL/INTERAMERICANA EDITORES, S.A. DE C.V.

Celina Oviedo, H., & Campo Arias, A. (2005). Aproximación al uso del coeficiente alfa de Cronbach. *Revista Colombiana de Psiquiatría, vol. XXXIV, núm. 4*, 572-580.

Cohen, W. A. (2003). Cómo ser un consultor exitoso. En W. A. Cohen, *Cómo ser un consultor exitoso* (pág. 360). Bogotá: Editorial Norma.

Coll Morales, F. (05 de Agosto de 2021). *Viabilidad económica*. Obtenido de Economipedia.com: https://economipedia.com/definiciones/viabilidad-economica.html

Coll Morales, F., & Westreicher, G. (1 de julio de 2021). *economipedia.com/definiciones-diccionario*. Obtenido de Economipedia.com: https://economipedia.com/definiciones/viabilidad-economica.html

Debate Escolar. (01 de ENERO de 2015). *Fundacionactivate.* Obtenido de Fundacionactivate.org: https://fundacionactivate.org/wp-content/uploads/2015/01/BUSINESS-MODEL-CANVAS.pdf

Economia, S. d. (15 de Febreo de 2023). *Tasa Interna de Retorno*. Obtenido de Glosario : https://e.economia.gob.mx/glosario/tasa-interna-de-retorno-tir/#:~:text=La%20Tasa%20Interna%20de%20Retorno,de%20una%20empresa%20o%20negocio.

Fernández de la Cigoña, J. R. (25 de Agosto de 2023). *Tasa interna de retorno (TIR): ¿Qué es y cómo se calcula?* Obtenido de sage.com: https://www.sage.com/es-es/blog/tasa-interna-de-retorno-tir-que-es-y-como-se-calcula/

García Prado, E. (2015). *Proyecto y viabilidad del negocio o microempresa.* España: Ediciones Paraninfo S.A.

Gobireno Mexicano. (2017). *Estrategia Nacional de Ciberseguridad (2017) (Spanish).* México: Gobierno de México.

González, I. (16 de junio de 2021). *Revista: Economia y Negocios*. Obtenido de https://mexico.unir.net: https://mexico.unir.net/economia/noticias/que-es-tir-como-calcular/

Guardia Nacional. (2022). *Informe anual de actividades 2021.* México: Guardia Nacional.

Guevara Jurado, L. A. (2022). *El hacking ético como servicio conexo de consultoría en seguridad por parte de las empresas de seguridad privada.* Bogotá D.C.: FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD Programa ADMINISTRACIÓN DE LA SEGURIDAD. Obtenido de http://hdl.handle.net/10654/40525.

Investor. (14 de Abril de 2023). *TIR: ¿Qué es la Tasa Interna de Retorno y para qué sirve?* Obtenido de theinvestoru.com: https://theinvestoru.com/blog/que-es-la-tir/

KUBR, M. (1997). *La consultoría de empresas: guía para la profesión.* Ginebra: Oficina Internacional del Trabajo, tercera edición (revisada).

León, J. Á. (25 de 03 de 2021). Ciberseguridad y protección de datos personales en el Perú. (A. R. Lima, Entrevistador) doi:https://doi.org/10.26439/advocatus2021.n39.5114

Lourdes, M. (2010). *Administración. Gestión organizacional, enfoques y proceso administrativo.* México: Pearson Educación.

Martínez Valencia, D. M. (01 de septiembre de 2012). *Implementación de una nueva metodología para el modelado de procesos de negocio aplicada en una casa consultora enfocada a las tecnologias de la información.* Obtenido de Ptolomeo UNAM: http://webcache.googleusercontent.com/search?q=cache:7BKHC3NGfwwJ:www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/2157/Informe%2520de%2520Actividades.pdf%3Fsequence%3D1&cd=3&hl=es-419&ct=clnk&gl=mx

Miranda, R. (25 de Enero de 2024). ¿Cuáles son los delitos cibernéticos con más incidencia en Edomex? *El Sol de Toluca*.

Mordor Intelligence. (2023). *Latin America Cyber Security Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029)*. Obtenido de Industry-reports: https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market

Osterwalder, A. (2011). *Modelo Canvas.* Barcelona: Deusto S.A. Ediciones.

Osterwalder, A., & Pigneur, Y. (2009). *Strategyzer Series Books.* Obtenido de strategyzer.com: https://www.strategyzer.com/books/business-model-generation

Pérez, A. (22 de Abril de 2021). *Blog Estudio de viabilidad de un proyecto: ¿qué es y cómo hacerlo?* Obtenido de OBS Business School: https://www.obsbusiness.school/blog/estudio-de-viabilidad-de-un-proyecto-estructura-e-importancia#:~:text=Hace%20referencia%20a%20la%20posibilidad,hacerlo%20un%20profesor%20de%20matem%C3%A1ticas

Perspectiva. (2007). Origen y Desarrollo de la Administración. *Perspectivas*, 45-54.

Reyes Gómez Israel, D. E. (1 de Febrero de 2023). Cuatro de los ciberataques más grandes de 2022. *Forbes México*. Obtenido de https://www.forbes.com.mx/ad-cuatro-ciberataques-grandes-ciberseguridad-uber-sedena-conti-optus/

Riquelme, R. (28 de Agosto de 2022). México reprueba en ciberseguridad, según reporte de IQSec. *EL ECONOMISTA*. Obtenido de https://www.eleconomista.com.mx/tecnologia/Mexico-reprueba-en-ciberseguridad-segun-reporte--de-IQSec-20220828-0002.html

Sabino, C. (1992). *Proceso de investigación.* Caracas: Panapo.

Servín, A. (23 de Marzo de 2023). Se debe trabajar en un plan preventivo para proteger a los usuarios de un ciberataque: Especialistas. *EL ECONOMISTA*. Obtenido de https://www.eleconomista.com.mx/los-especiales/Se-debe-trabajar-en-un-plan-preventivo-para-proteger-a-los-usuarios-de-un-ciberataque-Especialistas-20230323-0050.html

Sevilla Arias, A. (15 de Julio de 2014). *Tasa interna de retorno (TIR): Qué es fórmula y ejemplos.* Obtenido de Economipedia.com: https://economipedia.com/definiciones/tasa-interna-de-retorno-tir.html

Tamayo, M. T. (2003). *El proceso de la investigación cientifica.* Ciudad de México: Limusa.

Anexos

Anexo 1

Encuesta

1 ¿Cuál es su profesión u oficio?

2 ¿Indique en que área se encuentra ejerciendo (RH, contabilidad, logística, finanzas, educación, ventas, etc)?

a) Recursos Humanos(RH)
b) Finanzas
c) Educación
d) Logistica
e) Ventas
f) Compras
g) Administración

3 ¿Cuales son los recursos tecnológicos con los que cuentas en tu hogar u oficina? (Selecciona mas de una opción)

a) Internet
b) Computadora
c) Móvil
d) asistentes virtuales (alexa, google)
e) electrodomésticos inteligentes
f) camaras de vigilancia con acceso remoto (camaras wifi)

4 ¿Con que frecuencia utiliza las redes sociales (Facebook, whatssap, Instagram, tiktok)?

a) Todo el día.
b) De 1:00 - a 4:00 horas
c) menos de 1:00 hora

5 En términos de tecnológia ¿Con que frecuencia consultas comunidades digitales?

a) Siempre
b) Casi siempre
c) Poco
d) No participo, de ninguna forma

6 ¿Utilizas algunos de los siguientes servicios en línea especializado?

a) Apertura de cuenta (inversiones, bancarias u alguna otra)
b) Servicio de entretenimiento
c) Compras en linea
d) Banca en linea
e) Consulta de correo electronico

7 Los servicios de consultoría ¿Cómo le gusta recibirlos?

a) En linea.
b) Presencial.
c) Telefónica.
d) Remota y telefónica.
e) Remota y presencial.
f) Presencial y telefónica.

8 ¿Cuál es la opinion que le generan los servicios en linea?

a) Resuelve el problema en el menor tiempo posible y es económico.
b) Ahorra tiempo y dinero al contratar.
c) Me generan desconfianza.
d) Nunca utilizo un servicio en linea.

9 Si usted contrata un servicio de ciberseguridad ¿En que momento gustaria que fuese explicado el proceso de la solución del problema.? (Puede seleccionar mas de una opción)

a) Antes.
b) Durante.
c) Final.

10 ¿Ha utilizado algun de los siguientes servicios de consultoría en tecnología?

a) Capacitación en tecnológia.
b) Compra de productos tecnologicos.
c) Solucion de problemas relacionados a tecnologia.
d) Ciberseguridad.

11 Cuando tiene un problema relacionado a ciberseguridad ¿Como lo resuelve?

a) Busco a un experto en ciberseguridad.

b) Busco en internet la solucion.
c) Consulto con un conocido o familiar.
d) No he tenido ningun problema relacionado a seguridad de mis datos

12 ¿Cuánto estaría dispuesto a pagar por los servicios de una consultoría especializada en ciberseguridad?

a) $500 a $1000.
b) $1,000 - $5,000.
c) Mas de $5,000.

13 ¿Cuanto es lo que ha pagado por un curso relacionado a tecnología?

a) 350
b) 450
c) 500 o más

14 ¿Usted o algun conocido experimentado alguno de los siguientes delitos ciberneticos? (puede seleccionar mas de una opción)

a) robo de identidad.
b) secuestro de información.
c) espionaje cibernetico.
d) fraude por correo electrónico.
e) Robo de datos financieros.
f) Ninguna.

15. De los siguientes productos ¿Selecciona cuales utilizas de manera pirata relacionadas con sus actividades cotidianas dentro y fuera del trabajo?

a) Software de oficina (Word, Excel, Power Point, Outlook).
b) Software contable o administrativo.
c) Software de diseño.
d) Juegos.
e) Películas.
f) Antivirus.
g) Windows.