Universidad Iberoamericana

Estudios con Reconocimiento de Validez Oficial por Decreto Presidencial del 3 abril de 1981

“CASO DE NEGOCIO DE EMPRENDIMIENTO DE CIBERSEGURIDAD PARA PYMES DE MÉXICO”

ESTUDIO DE CASO

Que para obtener el grado de

MAESTRO EN GESTIÓN DE LA INNOVACIÓN TECNOLÓGICA

Presenta

VICTOR ANDRES MENDOZA OROZCO

Directora: Dra. Alejandra Herrera Mendoza

Lectores: Mtro. Joshua Gerardo Henderson Villalpando

ÍNDICE

1. Introducción

Las organizaciones están viviendo una época de intensos cambios y readaptación con la nueva realidad que ha dejado la pandemia de COVID 19, con una aceleración en la transformación digital que ha cambiado de forma parcial o total los procesos de negocio manuales por digitales, sin embargo, esta transformación digital trae consigo la amenaza de posibles intentos de ciberataques, es por eso que es importante tomar en cuenta la ciberseguridad para lograr dicha transformación con éxito.

En el presente escrito se identifica como el principal problema la baja adopción e incluso el desconocimiento de prácticas de ciberseguridad y reconocimiento oportuno de engaños e ingeniería social dentro de las organizaciones en un contexto de creciente número de intentos de ciberataques a sistemas computacionales y robo de información digital de pequeñas y medianas empresas de México. En los últimos cinco años los 100 ciberataques más importantes representaron un impacto económico de $18 mil millones de dólares en pérdidas a nivel global, lo cual tan solo es un reflejo de lo que se conoce oficialmente. (Endeavor & Paypal, 2020, pág. 10.).

El impacto de no contar con una estrategia de ciberseguridad podría resultar más costoso que la propia inversión en ella, ya que ser víctima de ciberseguridad puede representar pérdidas económicas, penalizaciones, reputación deteriorada, desconfianza de los clientes, pérdida de información valiosa, interrupciones al negocio y en algunos casos hasta el cierre total de la empresa. Cuando con una inversión de $26,000.00 podría ayudar drásticamente a proteger la organización de ciberataques. Con esta inversión se cubrirá una capacitación para 1 a 7 personas ($7, 500.00), 25 implementaciones de antivirus ($500.00 c/u) y un diagnóstico de madurez de ciberseguridad de la organización ($6,000.00). Esta podría ser una primera etapa en ese camino hacia la ciberseguridad.

Para el estudio de caso, se siguieron las 11 principales secciones de la metodología propuesta por la coordinación de la maestría en Gestión de la Innovación tecnológica (Herrera, 2022, pág. 2.), donde se emplean modelos teóricos que permitieron generar información valiosa para llegar a un caso de negocio final, en el cual se identificó un problema a una situación actual, se establecieron objetivos del trabajo, se desarrolló un caso de negocio que permitió evaluar aspectos importantes como propuesta de valor, entorno de mercado, barreras de entrada, entorno competitivo, identificación de tipo de cliente, análisis financiero, proceso de validación de alternativas de solución entre otros. Este proceso dio como resultado un caso de negocio para un emprendimiento de una empresa de servicios de ciberseguridad con una oferta inicial de 5 servicios que están orientados a mitigar o aliviar algunos de los principales *pains* de las organizaciones al momento de proteger sus sistemas y activos digitales. Algunos de ellos son; Ransomware, Ingeniería Social, Phishing y Spyware los cuales en muchas de las ocasiones actúan en conjunto, por ejemplo, un ataque puede iniciar como un caso de phishing y terminar con un ransomware.

Como parte de la solución, se propone crear una empresa enfocada en ayudar a Pymes con procesos digitales a implementar y configurar sistemas de ciberseguridad y antivirus, así como ofrecerles capacitaciones sobre ciberseguridad y gestión de la información que las ayuden a minimizar el riesgo de ser víctima de un ciberataque y ser su socio de ciberseguridad para que no tengan que preocuparse por este tema y se enfoquen en su negocio y así evitar ser parte de las estadísticas de mortandad de Pymes, al menos por un tema de seguridad cibernética. Todo esto con un precio orientado a Pymes. La propuesta de oferta de servicios es la siguiente:

- Diagnóstico de nivel de madurez en ciberseguridad
- Implementación de consola de antivirus y endpoint
- Gestión de consola de antivirus y endpoint
- Capacitación en ciberseguridad
- Consultoría en implementación y cumplimiento de estándares de seguridad

En el proceso de validación de la propuesta de solución final se entrevistó a expertos en la industria de ciberseguridad para conocer su perspectiva con respecto a la propuesta de servicios y oportunidad de negocio en ciberseguridad para Pymes con procesos digitales de México. De la misma forma participaron prospectos de clientes para conocer su perspectiva y familiarización con la materia desde una posición clave dentro de sus organizaciones.

El análisis financiero está basado en un escenario intermedio, especialmente el pronóstico de ventas del primer semestre. Con base en esta consideración y los supuestos definidos en el proyecto tiene una TIR de 44% para los primeros 3 años de operación y un VPN de $ 1,955,178.80 con una utilidad neta de -$880,890.22 el primer año, $939,697.71 el segundo año y $1,180,491.64 el tercer año de operación.

Robert Muller ex agente del FBI dice (Endeavor & Paypal, 2020, pág. 10.): "*Hace un par de años las empresas se dividían entre aquellas que ya fueron atacadas y las que van a ser atacadas. Hoy se divide entre las que ya fueron atacadas y lo saben y las que no lo saben.*" Es por ello que hoy es el mejor momento para considerar la ciberseguridad como elemento clave dentro de la estrategia general de las organizaciones, donde debe ser tarea de todos y no solo de un área o del departamento de TI, cada miembro de la organización con acceso a sistemas e información de la empresa podría representar un punto de acceso para ciberdelincuentes.

2. Antecedentes

Las organizaciones están viviendo una época de intensos cambios y readaptación en varios sentidos con la nueva realidad que ha dejado la pandemia de COVID 19, con una aceleración en la transformación digital y rápida adopción de las principales tendencias digitales según la revista Logistec son:

- Inteligencia artificial
- Internet de las Cosas (IoT)
- Block chain
- Ciberseguridad
- Computación cuántica

Algunas tendencias adicionales a la que menciona la revista se encuentran:

- Transformación Digital
- Nube
- Redes sociales
- Banca en línea
- Big data
- Comercio electrónico

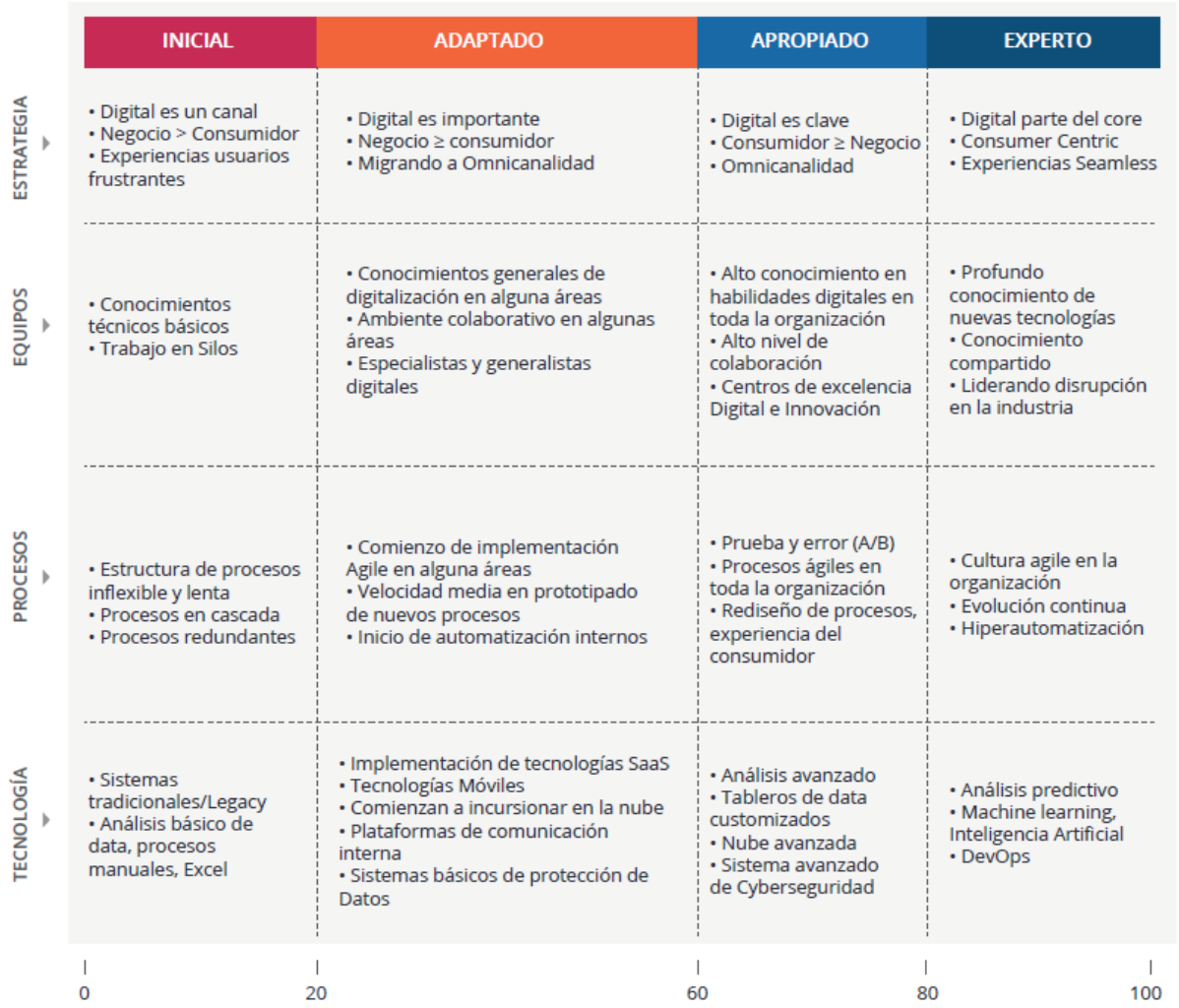
La propia ciberseguridad también se considera una tendencia digital debido a la creciente superficie cibernética que se tendrá que resguardar de los atacantes..

Debido a que estas tendencias no tienen marcha atrás ni hay forma de frenarlas, pues son parte importante del desarrollo y avance tecnológico para las sociedades, toma relevancia el concepto de ciberseguridad, que surge por la necesidad de contrarrestar, neutralizar y, en el ideal, evitar posibles ciberataques, es decir, para proteger los activos digitales que se están generando como parte de estas actividades en el ciberespacio. Estos activos digitales pueden tomar diferentes formas como son: archivos, imágenes, videos, cuentas bancarias, sistemas, configuraciones, credenciales de sitios y cualquier otro dato que pueda estar almacenado digitalmente en un disco duro, sin importar si está conectado a la red o de manera local.

Precisamente esta transformación digital que ha permitido impulsar el potencial de negocio de las empresas que han adoptado y se han subido a este proceso de sustituir de forma parcial o total los procesos manuales o análogos en digitales que son importantes o clave para el negocio, han logrado competir y sobrevivir a los distintos factores globales que hemos vivido recientemente, sin embargo, esta transformación digital trae consigo la amenaza de posibles intentos de ataques cibernéticos, es por eso que es importante tomar en cuenta la ciberseguridad para lograr dicha transformación. De

acuerdo con un informe del 2021 realizado en conjunto por Kio Networks, EY y needed education, acerca de la madurez digital de las empresas proponen los siguientes aspectos para medir el nivel de madurez digital en el que se encuentran. Con ayuda de esta clasificación las empresas pueden hacer conciencia de su nivel de madurez digital y por ende reflexionar que tan protegida se encuentra para hacer frente al número creciente de intentos de ciberataques.

Figura 1. Niveles de madurez digital



(Kio Networks, EY, needed, 2021)

Según una definición de IBM sobre **ciberseguridad** es la práctica de proteger los sistemas importantes y la información confidencial de los ataques digitales. También conocida como seguridad de la tecnología de la información (TI), las medidas de ciberseguridad o seguridad cibernética están diseñadas para combatir las amenazas contra sistemas en red y aplicaciones, ya sea que esas amenazas se originen dentro o fuera de una organización (IBM, 2022). Por otro lado, es importante entender qué es un **ciberataque,** son intentos no deseados de robar, exponer, alterar, deshabilitar o destruir información mediante el acceso no autorizado a los sistemas informáticos (IBM, 2022).
En este contexto de un mundo cada vez más digital y conectado viene consigo un efecto colateral y convertido en un problema severo en materia de seguridad cibernética, el cual afecta a personas, organizaciones, instituciones y empresas, ya que cada vez es mayor la información que se almacena en las nubes y en medios digitales. Es por ello que, la **situación actual de muchas organizaciones públicas y privadas** es que se ven con la obligación de cumplir cada vez con mayor frecuencia con estándares de seguridad en el manejo y protección de datos personales, ya sea por medio de leyes o bien por estándares de seguridad internacionales que puedan aplicar a cada industria; por ejemplo, PCI (Payment Card Industry) para la industria bancaria.

Las grandes empresas destinan mayores recursos (tiempo, económicos y esfuerzos) a concientizar a su personal y darle cierta prioridad a la ciberseguridad de su organización por distintos motivos, sin embargo, esto no resulta tan usual para las pequeñas y medianas empresas que comúnmente su día a día es absorbido por la operación, las urgencias por entregar, diseñar estrategias para continuar compitiendo y siendo rentables en su entorno, básicamente sobrevivir en el mercado cada vez más competido y en el escenario ideal crecer. Es por ello, que es muy común ver que este tipo de empresas asignen una menor o en algunos casos nula prioridad a la ciberseguridad de su organización, de igual forma tendrán sus motivos para dejarlo de lado que van desde la escasez de recursos, que pudieran ser, económicos, conocimiento y tiempo, así como tener una percepción de poca importancia del tema y principalmente desconocimiento en materia de ciberseguridad. Estas mismas empresas hoy en día sufren más de lo necesario por cumplir con normas ya que, en muchas ocasiones sus operaciones no les permiten abordar estos temas de la forma más eficiente posible o bien enfocarse en entender dichas normas y tratar de implementarlas sin descuidar sus operaciones, es por ello que en ocasiones las organizaciones ven el cumplimiento y certificación de estándares de seguridad como algo burocrático y doloroso, que incluso pierden de vista que el obtener este tipo de certificaciones podría representar una ventaja competitiva sobre su competencia, también al tener a su personal capacitado ayuda a prevenir la exposición al robo de información y ser víctima de la ciberdelincuencia que podría resultar más costoso que tomar las medidas necesarias de forma preventiva.

Los principales motivos que buscan los atacantes son; beneficiarse económicamente robando dinero, información estratégica e interrumpir el negocio dejando fuera los sistemas de alguna organización, ya sea pública o privada. Un claro ejemplo de ataques organizados y deliberados, son los múltiples ataques que sufrieron las instituciones gubernamentales rusas derivado de la decisión de invadir Ucrania en febrero del 2022; grupos organizados advirtieron que atacarían sus sistemas y páginas web con el objetivo de demostrar su descontento con la guerra.

Ahora que entendemos dichos conceptos es momento de identificar algunos de los factores y elementos que interactúan en esta disputa entre ciberseguridad y ciberataques. Detrás de un ciberataque existen personas comúnmente llamadas ciberdelincuentes y organizaciones criminales que desean beneficiarse del robo de información o algún activo digital. Podemos clasificar estas amenazas para la ciberseguridad como internas y externas.

Amenazas cibernéticas externas:

- Hackers profesionales
- Hackers aficionados
- Delincuentes organizados

Amenazas internas (usuarios autorizados):

- Empleados no apegados a las políticas de seguridad
- Empleados actuales o ex empleados descontentos
- Socios de negocio, clientes o proveedores con accesos autorizados al sistema

Los ciberataques pueden afectar a personas, organizaciones gubernamentales, empresas privadas y prácticamente a cualquiera que tenga algún dispositivo que consuma o almacene información de forma digital. Es por lo que me gustaría responder un par de preguntas que probablemente muchos se harían ¿Qué tiene que ver la ciberseguridad conmigo? o ¿Por qué es importante la ciberseguridad? El mundo actual es más globalizado y conectado que nunca, prácticamente todos estamos conectados a la red y probablemente algunos podrían decir que no tienen nada que esconder o que su información no es importante para alguien más, sin embargo, esta postura sería un error, ya que la ciberseguridad tiene que ver con confidencialidad y privacidad, es decir, parte de su propósito es tratar de garantizar eso y aunque se considere, por ejemplo, que algunas imágenes de nuestras mascotas no son importantes, debemos tratar cualquier dato como un dato confidencial o público, ya que existen muchas formas de ciberataques y sumado a eso, tenemos **Vigilancia Permanente** que gobiernos y empresas privadas han implementado para conocer nuestros gustos, hábitos, preferencias y opiniones que usarán para vendernos más productos o servicios, o bien, predecir por cuál candidato podríamos votar en las próximas elecciones. Edward Snowden (2019, p.282, en su libro Vigilancia permanente, menciona que:

> "D*ecir que no te importa la privacidad porque no tienes nada que esconder no es diferente a afirmar que no te importa la libertad de expresión porque no tienes nada que decir; o que no te importa la libertad de prensa porque no te gusta leer; o que no te importa la libertad de religión porque no crees en Dios".*

Es probable que la información que hoy tienes almacenada o publicada no sean de suma relevancia, sin embargo, eso no significa que esté bien y que no importe que sea sustraída o usada para otros fines a los que tú deseas, es por eso que es importante la ciberseguridad para personas, organizaciones y gobiernos.
A manera de integrar las ideas vistas hasta el momento nos hemos situado en un contexto de una superficie cibernética más extensa con algunas tendencias sociales y tecnológicas que empujarán a estar aún más conectados con personas y dispositivos donde existen datos que buscamos proteger de algunas actividades deliberadas que buscan vulnerar la ciberseguridad para extraer información o bien cualquier otro tipo de crimen cibernético que iremos analizando.

2.1 Tipos de ciberseguridad

Hoy en día la información digital es uno de los activos más valiosos para las personas y las organizaciones y para que esta información cumpla con su objetivo de ser de valor debe cumplir con las siguientes características:

- Confidencialidad (solo personas autorizadas pueden acceder a ella)
- Integridad (solo personas autorizadas pueden modificarla y alterarla)
- Disponibilidad (la información debe estar disponible cuando sea necesario)

De acuerdo con lo que hemos definido (Infosecurity México, s.f.) acerca de ciberseguridad, ciberataque y amenazas, se puede realizar la siguiente clasificación, basada en los elementos que protegen, de tipos de ciberseguridad que toda persona y principalmente organizaciones deben tomar en cuenta en la gestión de su información y sistemas informáticos:

- Seguridad de hardware (protección a elementos y espacio físicos)
- Seguridad de software (protección a aplicaciones y programas)
- Seguridad de red (protección a la conexión y medios de comunicación entre sistemas)

2.2 Tipos de ataques y posibles soluciones

Por la forma en que se comportan y logran su cometido, podemos agrupar y clasificar a los ciberataques de la siguiente forma:

Ransomware. Es un software malicioso que bloquea el acceso a la información o al equipo completo, es una especie de secuestro de la información donde los cibercriminales son dueños de la clave para acceder a la información y la víctima para obtener esa clave debe pagar por el rescate sin ninguna garantía de recuperar la información o de que no lo vuelvan a chantajear.

Algunas recomendaciones para protegerse de un ataque de tipo ransomware son:

- Realizar respaldos periódicos de la información, a disco o a la nube
- Habilitar el explorador de archivos del sistema operativo para que muestre la extensión de los archivos e identificar más fácilmente los .EXE
- Filtrar los archivos .EXE del correo electrónico
- Deshabilitar el escritorio remoto (RDP) del sistema operativo si no es necesario usar este protocolo
- Mantener actualizadas las versiones de los programas y sistema operativo para evitar que los cibercriminales exploten vulnerabilidades conocidas
- Contar con un buen antimalware y un firewall activo
- Desconectar inmediatamente el equipo de la red (wifi o ethernet) si el ataque se encuentra en curso, actuar rápido puede minimizar el daño
- Formatear el sistema operativo, lo que significa, volver a la configuración de fábrica y restaurar la información de los respaldos previamente realizados

Suplantación de identidad (phishing). Este tipo de ataque tiene la finalidad de robar información, comúnmente bancaria o credenciales de acceso y consiste en enviar correos electrónicos fraudulentos que se asemejan a correos electrónicos de fuentes de buena reputación. Es uno de los ataques más exitosos por su naturaleza de asemejar un sitio verdadero y engañar a su víctima.

Algunas recomendaciones para protegerse de un ataque de tipo phishing son:

- Identificar correos sospechosos. Comúnmente utilizan nombres y logos de empresas reales, incluyen links a sitios falsos con la identidad del verdadero o muy parecidas a las originales, se basan en promociones, regalos o problemas con la cuenta como anzuelos
- Verificar muy bien la fuente de los correos, el dominio o cuenta completa del emisor
- No dar clic en links dentro del correo electrónico. Ya que redireccionan a una página fraudulenta para obtener la información que desean, como podría ser el inicio de sesión del banco o algún otro portal
- Contar con antivirus, actualizar el sistema operativo y navegadores.

Spyware. Es un tipo de programa maligno (malware) que se instala o se ejecuta sin que el usuario se dé cuenta, tiene la finalidad de espiar y acceder a su información; se ejecutan en segundo plano y suelen ser instaladas por una segunda aplicación posiblemente legítima.
Algunas recomendaciones para protegerse de un ataque de tipo spyware:

- No abrir correos electrónicos de desconocidos o sospechosos.
- No descargar archivos a menos que provengan de una fuente fiable.
- Colocar el cursor sin dar clic sobre enlaces antes de abrirlos y asegurarse de acceder al sitio correcto.

Finalmente, tenemos la **ingeniería social**, la cual, de forma general son tácticas que utilizan los criminales para engañar a sus víctimas o simplemente podría ser, asomarse a la pantalla de algún usuario para obtener información que lo lleve a algún dato relevante (pueden ser descuidos o revelar contraseñas incluso en un post-it sobre el escritorio). Este tipo de ataque comúnmente es utilizado en combinación con alguno de los anteriores.

Esta es una forma muy general de clasificar los ciberataques en cuatro categorías, los cuales consideraremos como los principales *pains* (dolores de las organizaciones en materia de ciberseguridad) ya que su estos se presentan cada vez más frecuentemente y estos son más sofisticados y con un impacto mayor en las organizaciones, que en el caso de una pequeña o mediana empresa podría representar el cierre total. Incluso el impacto de no contar con una estrategia de ciberseguridad pudiera resultar más costoso que la propia inversión en ella, ya que ser víctima de un ciberataque puede representar pérdidas económicas, penalizaciones, reputación deteriorada, desconfianza de los clientes, pérdida de información crítica del negocio y/o clientes, interrupciones al negocio y en algunos casos hasta el cierre total de la empresa, tal como ya se mencionó.

3. Problema

El principal problema que se identifica es el desconocimiento de prácticas de ciberseguridad y reconocimiento oportuno de engaños e ingeniería social dentro de las organizaciones en un contexto de creciente número de intentos de ciberataques a sistemas computacionales y robo de información digital a pequeñas y medianas empresas de México. Existe aún, una brecha grande en cuanto a capacitación e información sobre el manejo y protección de activos digitales dentro de las organizaciones, ya que gran parte de los ciberataques son permitidos por negligencias, descuidos y desconocimiento del personal interno.

De acuerdo con el estudio Panorama del ecosistema de ciberseguridad (Endeavor & Paypal, 2020, pág. 11.): "*La principal barrera de adopción de la ciberseguridad dentro de los emprendimientos es la falta de presupuesto (34%), seguida de la ausencia de integración en la estrategia (18%) y la dificultad técnica de implementación (14%)*."

Adicional a la información presentada acerca de las barreras de adopción de la ciberseguridad, se identifican como los principales retos para hacer que las empresas adopten dichos servicios los siguientes:

- **Encontrar espacio para abordar el tema de ciberseguridad con las Pymes**. Al ser un tema nuevo y considerado ajeno a su operación representará un reto encontrar ese espacio de atención para hablar del tema y persuadirlo del riesgo en el que se encuentran si no se realizan algunas acciones para proteger activos digitales.
- **Falta de presupuesto para ciberseguridad**. Una vez encontrado el espacio y teniendo una noción de los riesgos existentes, las empresas deberán generar un presupuesto para ciberseguridad que probablemente lo vean como un gasto y no como una inversión y esto es parte de lo que se debe trabajar para crear un entendimiento de la materia.
- **Crear conciencia de los riesgos de los ciberataques**. Al encontrar espacio en las agendas de las empresas se deberá ser muy efectivo para comunicar los riesgos, impactos y probabilidades de los ciberataques.
- **Demostrar que los ciberataques no son ajenos a ellos.** Una opción es una demostración consensuada de vulnerabilidades existentes al momento de presentar servicios de ciberseguridad.
- **Crear conciencia de la importancia de sus procesos, sistemas e información digital para su negocio.** En ocasiones no se tiene claro lo importante que es un proceso, herramienta o acceso a información digital. En otras palabras, saber cómo se podría continuar la operación del negocio sin el correo electrónico, acceso a la información digital, sin acceso al sistema de facturación, etc. ¿Cuánto tiempo tomaría recuperar el sistema y qué impacto tendría para la operación no contar con ello?

Dentro del mismo estudio se hace referencia a un reporte de Cyentia Institute publicado en 2020, indica que en los últimos cinco años los 100 ciberataques más importantes representaron un impacto económico de $18 mil millones de dólares en pérdidas con 10 mil millones de registros comprometidos, lo cual tan solo es un reflejo de lo que se conoce oficialmente, debido a que no todos los ciberataques y sus impactos son denunciados y publicados.
Con este problema viene también una oportunidad de mejora y por supuesto, de negocio, para atender y solventar o minimizar posibles vulnerabilidades y ayudar a las pequeñas y medianas empresas a capacitar y sensibilizar a sus equipos de trabajo en temas de ciberseguridad, ciberdelincuencia y ciberhigiene para tratar de evitar ser víctimas de alguna de las formas de ciberataques existentes, así como disminuir el impacto que se pudiera tener en caso de verse en una situación de ciberataque en curso y conocer cómo actuar ante ello, si bien esto es un primer paso en el largo camino de la ciberseguridad, esta disciplina es mucho más extensa que solo conocer las distintas formas que puede tomar un ciberataque o implementar sistemas de seguridad perimetral robustos para evitar ataques, también este tipo de empresas (pequeñas y medianas) requieren acompañamiento en su proceso de certificación en estándares de seguridad y en el cumplimiento de leyes de protección de datos donde requieren diagnósticos de madurez de ciberseguridad, capacitación continua y asesoría en el tema. Es verdad que cada vez surgen más consultoras en materia de ciberseguridad, manejo y protección de datos personales aún es una oportunidad grande debido a que es más frecuente que las empresas grandes tomen la iniciativa en capacitar y sensibilizar a su personal, sin embargo, las Pymes podrían verse limitadas en tiempo y esfuerzo para aspectos de ciberseguridad y es ahí donde existe un mercado amplio para nuevas o actuales consultoras para acompañar a estas Pymes en ese camino hacia la ciberseguridad y ciberhigiene que deben tener. Es importante tomar en cuenta que la tecnología está en constante evolución y de forma muy acelerada, tanto así, que va más rápido que los procesos, normas y leyes, dejando muy pronto obsoleto los conocimientos y cumplimiento de ciertas prácticas que se pudieran ser efectivas en cierto momento.

4. Objetivo

Desarrollar y diseñar un caso de negocio sobre una empresa nueva de servicios de ciberseguridad orientada a Pymes de la zona metropolitana de México que permita analizar aspectos de mercado, evaluación financiera, entorno e industria, así como oferta de servicios y se pueda ejecutar en el transcurso de un año..

Objetivos específicos del estudio:

1. Describir cada uno de los servicios a ofrecer, así como su alcance y responsabilidades del cliente y proveedor.
2. Identificar el perfil y tipo de Pyme, así como sus características y tamaño de mercado objetivo.
3. Evaluar viabilidad financiera como proyecto de inversión para la creación de una empresa de ciberseguridad enfocada en Pymes.

5. Contexto externo

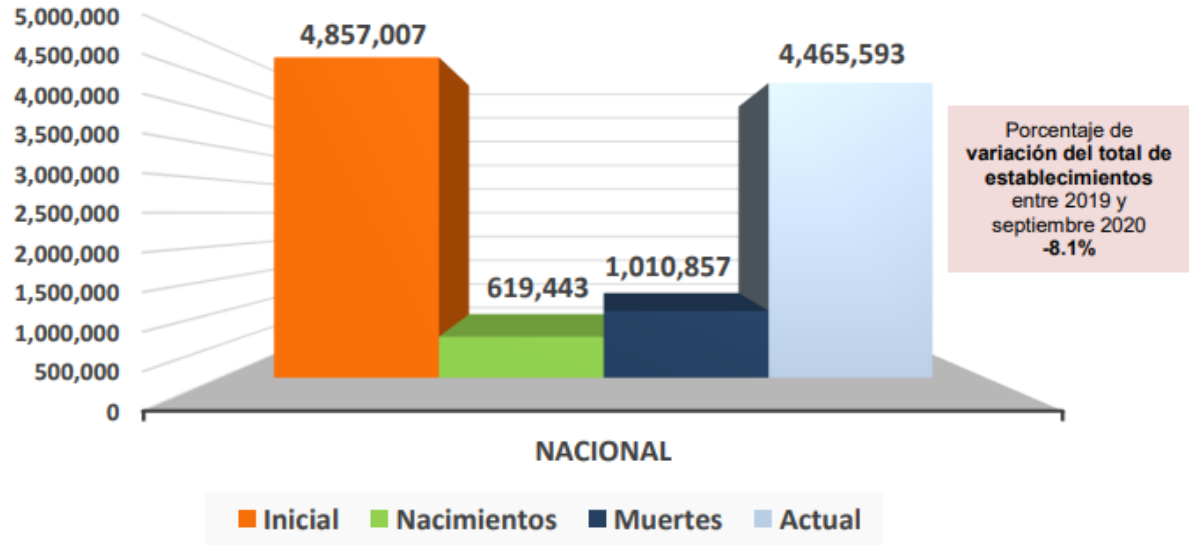
A partir del año 2020, un año de gran avance para la transformación digital, ya que la pandemia de COVID 19 obligó a las empresas a enfocar sus esfuerzos en el bienestar de sus colaboradores, asegurar la continuidad de sus negocios y a reinventar su estrategia de transformación digital, soportado en gran medida por el trabajo a distancia. Las empresas con procesos digitales tuvieron un crecimiento exponencial, por ejemplo, Amazon y Zoom, las empresas que no son nativas digitalmente hablando, tuvieron que acelerar su transformación para seguir en el mercado adoptando nuevas tecnologías y adaptarse a los nuevos hábitos de los consumidores. La transformación digital solo es un ejemplo de las tendencias digitales que se listaron anteriormente y con esto busco poner en contexto hacia dónde va la tendencia del espacio digital, es decir, cada vez con mayor superficie digital y con esto se convierte en un terreno inmenso para los ciberdelincuentes, al igual que estas tendencias los ciberataques van en aumento y las organizaciones más vulnerables son las micro, pequeñas y medianas empresas por distintos motivos que van desde sistemas de seguridad, antivirus, información sobre ciberseguridad, hábitos de consumo y resguardo de datos digitales, presupuestos para implementación de sistemas de seguridad física y digital, presupuesto para adquirir software original, etc. Para Dmitry Bestuzhev, (Forbes. 2021), director del Equipo de Investigación y Análisis de Kaspersky para América Latina, el alto índice de programas piratas en la región es un factor de impulso importante para el cibercrimen. Brasil lidera la región con más de 1,390 intentos de infección por minuto, seguido de México (299 por minuto); Perú (96 por minuto), Ecuador (89 por minuto) y Colombia (87 por minuto).

Por otro lado, México se encuentra dentro de los países con mayores intentos de ciberataques de Latinoamérica, según un estudio realizado por Fortinet (Empresa de tecnología y fabricante de dispositivos de seguridad), México ocupó el primer lugar de Latinoamérica con 67% de intentos de ataque, seguido por Brasil con 17% y Perú con 5% en tercer lugar, de un total de 289 000 millones de intentos en 2021, (Fortinet, 2022).

5.1 Entorno de mercado

De acuerdo con el INEGI (Instituto Nacional de Estadística, Geografía e Informática) en un estudio del 2021, tal como se muestra en la siguiente figura en México existen 4.9 millones de establecimientos privados y paraestatales de los cuales el 99.8 % pertenecen al conjunto de micro, pequeños y medianos establecimientos los cuales mantienen ocupadas a 27 millones de personas y este grupo de empresas es el más vulnerable a ser víctimas de ciberataques, uno de los principales ataques a las cuales están expuestos son tácticas de ingeniería social, las cuales muchas veces se originan por descuidos y/o desconocimiento de personal interno de las organizaciones en prácticas de ciberseguridad.

Figura 2. Número de establecimientos CE 2019 y EDN 2020



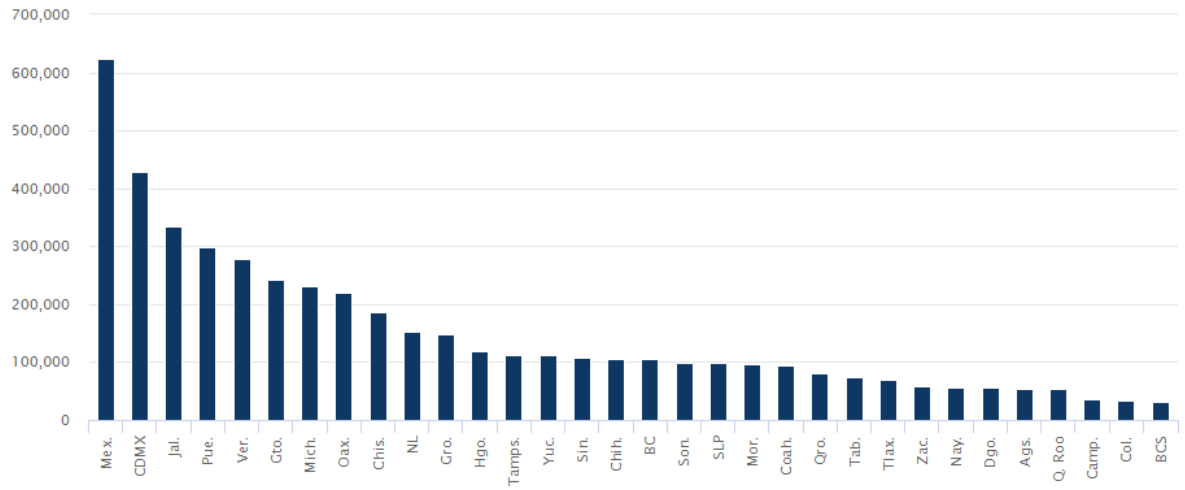
(INEGI, 2021)

Al igual que los ciberataques que van en crecimiento cada año, también la **ciberseguridad es un mercado en crecimiento** en distintos servicios, probablemente no al mismo ritmo que los ciberataques, sin embargo, sí es un tema que va tomando relevancia dentro de los procesos internos de las organizaciones y se está tomando cada vez mayor seriedad. Algunos de los servicios que actualmente se ofrecen con mayor frecuencia en el mercado son:

- Capacitación en ciberseguridad
- Implementación, instalación y administración de Antivirus
- Implementación, instalación y administración de sistemas de seguridad perimetral
- Correlación de eventos de seguridad
- Escaneo de redes y dispositivos para identificar vulnerabilidades
- Diagnósticos de nivel de seguridad

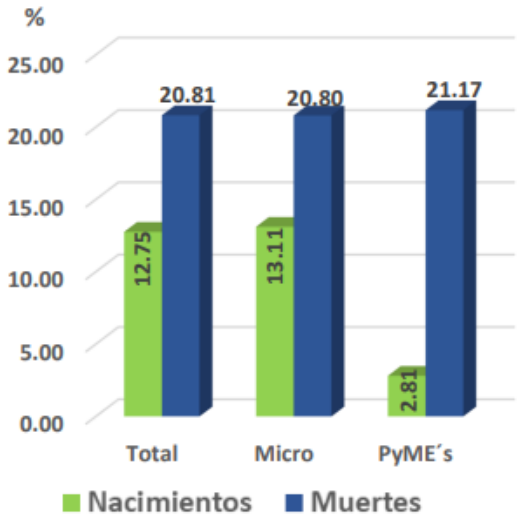
A pesar de que la tasa de mortalidad de Pymes es alta, tal como lo muestra la figura anterior, cuando nacen nuevas empresas es muy común que lo hagan con alguno de procesos de forma digital, y es ahí donde será relevante para ellos contar con buenas prácticas de ciberseguridad, al menos en un nivel elemental, la cual podrían lograr con asesoría de expertos en la materia. El mercado meta en un inicio se considera a las Pymes de la zona metropolitana que contempla la CDMX y estado de México los cuales son los estados con mayor densidad de este tipo de empresas dando un total de 1,052,431 establecimientos.

Figura 3. Establecimientos por entidad federativa



(INEGI, 2019)

Figura 4. Proporción de nacimientos y muertes de establecimientos a nivel nacional



(INEGI, 2021)

Como primera fase y con base en la plantilla de tamaño de mercado de Dynamic se podría definir el tamaño de mercado meta para los servicios de ciberseguridad enfocados a Pymes con procesos digitales de la zona metropolitana de México.

Figura 5. Plantilla de tamaño de mercado de Dynamic empresa Ciberseguridad

(Elaboración propia, 2022)

Con base en el mercado y la necesidad que existe de contar con medidas de protección de datos y ciberseguridad actuales se determina que será *market pull* la modalidad en la cual se busca entrar en el mercado para la nueva empresa de servicios de ciberseguridad.

5.2 Barreras de entrada

Algunas de las barreras de entrada que se identifican para el mercado que se busca atacar son las siguientes:

- Conocimiento especializado en materia de ciberseguridad
- Conocimiento en materia de regulaciones, normas y leyes de protección de datos
- Jugadores existentes bien posicionados
- Se requiere personal especializado con certificaciones y/o acreditaciones en la materia
- Conocimiento profundo en tecnologías de información y comunicaciones
- El segmento de mercado meta no está completamente consciente de la necesidad de esta solución
- Para el segmento de mercado meta aún no percibe la ciberseguridad como una prioridad

Con base en el modelo de cuadrícula de expansión Producto – Mercado la nueva empresa de ciberseguridad se encontraría en el cuadrante de "**Desarrollo de producto**" debido a que es un mercado ya existente en cuestión de soluciones y consultoría en ciberseguridad, sin embargo, existen segmentos de mercado poco atendidos y necesidades de estos segmentos poco exploradas, que probablemente ni las mismas Pymes tengan claro que las necesitan hasta que se ven afectadas por un ataque.

Figura 6. Empresa de ciberseguridad en modelo cuadrícula de expansión Producto - Mercado

	Productos existentes	Nuevos productos
Mercados existentes	Penetración de mercado	Desarrollo de nuevo producto
Nuevos mercados	Desarrollo de mercado	Diversificación

(Elaboración propia, 2022)

5.3 Entorno competitivo

Actualmente en la industria de tecnologías de información y en particular en ciberseguridad ya existen algunos jugadores bien posicionados como son:

- Kio Cyber Security
- T Systems Cyber Security
- Scitum
- GLAC
- ProtektNet
- ARAME
- BMobile Grupo Scanda
- Lightech
- HD Latinoamérica
- Zero Uno
- IQsec
- Netrix
- Eyesec
- 2Secure
- N3XAsec
- HackingMexico
- Alestra
- Bestel

En esta sección se presentará información de los principales competidores de la industria.

Kio Networks. Empresa fundada en 2002 con capital 100% mexicano conformada por un gran equipo de expertos, que ofrecen un amplio portafolio de infraestructuras y servicios de tecnologías de información de misión crítica, con altos niveles de calidad y procesos internacionales.
Cuentan con 40 Centros de Datos de alta densidad y disponibilidad en México, Centroamérica, El Caribe y Europa.
Específicamente en su unidad de negocios de Ciberseguridad cuentan con más de 200 especialistas en seguridad informática, más de 70 especialistas en dimensionamiento y más de 50 profesionales técnicos en cumplimiento de ciberseguridad y riesgos.

Algunos de los servicios en ciberseguridad que ofrecen son:

- End detection and response
- Next Generation Antivirus
- Next Generation Secure Gateway
- Cloud Access Security Broker
- Security Information and Event Management
- Web Application Firewall
- Data Loss Prevention
- Unified Threat Management

Scitum. Es la empresa líder en ciberseguridad en México, con presencia en Latinoamérica, Estados Unidos y algunos países de Europa. Su enfoque es cubrir las necesidades de sus clientes con servicios que abarcan de manera completa el ciclo de ciberseguridad, entre los cuales destacan los servicios de

consultoría y servicios administrados. Scitum forma parte de Telmex y Grupo Carso, lo cual representa un gran respaldo y capacidad financiera. Cuenta con 755 colaboradores

Algunos de los servicios en ciberseguridad que ofrecen son:

- Gestión de riesgos y gobierno de ciberseguridad
- Ciberinteligencia
- Gestión del factor humano
- Gestión end to end de la seguridad aplicativa
- Protección de infraestructuras digitales
- Detección y respuesta a ciberamenazas

5.4 Análisis de factores de entorno e impacto

Tabla 1. Análisis de factores de entorno e impacto

Aspectos Demográficos	
Factor	**Impacto**
Educación y capacitación	La ciberseguridad requiere de cierto conocimiento especializado para desarrollar una cultura de seguridad para proteger la información que poseen las empresas
Bancarización	Es un aspecto importante para el comercio electrónico y entretenimiento digital cuyos usuarios tengan acceso a servicios bancarios, a pesar de existir tarjetas de prepago, la banca es un importante potencializador para seguir desarrollando dichas tendencias digitales que deben contar con medidas de seguridad digital
Evolución de la pirámide poblacional	Puede llegar a ser común que a las personas de mayor edad se les dificulte más entender y dominar la tecnología y por ende sus implicaciones, así como su seguridad digital
Fuerzas Sociales	
Factor	**Impacto**
Empleo y desempleo	Mayor gente buscando autoemplearse por medio de ventas en línea debido a limitadas oportunidades de empleo en muchas industrias y una creciente demanda de empleo. Empleados o exempleados con conocimiento de accesos lógicos molestos con la empresa
Seguridad social	Con índices de informalidad y desocupación altos se incrementa el índice en actividades delictivas como fraude, robo de activos digitales, extorsiones, etc.
Costumbres y hábitos de seguridad cibernética	Baja prioridad a proteger activos digitales y escasa cultura de la seguridad cibernética. Percepción de poca importancia a información digital y falta de conciencia en la importancia de la seguridad

Factores Políticos, Legales, Regulatorios	
Factor	**Impacto**
Regulación y leyes en protección de datos	Los gobiernos e iniciativa privada cada vez toman más en serio el manejo y protección de datos personales por lo cual da lugar a nuevas leyes
Estándares de seguridad	Es muy frecuente que algunas industrias como la bancaria deban cumplir estrictos estándares de seguridad y protección de datos
Imposición de nuevas sanciones económicas por violación de leyes de protección de datos	Creación de nuevos impuestos o sanciones por incumplir con leyes en materia de protección de datos personales por parte de empresas poseedoras de información de sus clientes
Ambiente Natural	
Factor	**Impacto**
Cambio climático	Las empresas que se preocupan por el medio ambiente, aquellas "Socialmente responsable" cuentan con mejor reputación y buscan promover el teletrabajo que su vez se vuelve un punto de riesgo que se debe gestionar y proteger como si fuera la oficina
Contaminación	Mayores esfuerzos en evitar traslados a oficinas o escuelas haciendo remoto el trabajo y educación
Factores Tecnológicos	
Factor	**Impacto**
Inteligencia Artificial	Algoritmos para correlacionar eventos en bitácoras de logs y dispositivos de seguridad
Automatización	Automatización de procesos y eficiencia operativa para evitar intervención humana en sistemas y así exponer accesos lógicos e información que pueda comprometer la seguridad
Nube	Es una tendencia tecnológica para muchas de las industrias, lo que implica contar con medidas de ciberseguridad
Transformación digital	Los comercios encuentran una ventaja competitiva cuando se cuentan con comercio electrónico y procesos digitalizados
Infraestructura y acceso a internet	Zonas de difícil acceso a internet e infraestructura en algunas zonas de países en vías de desarrollo.
Fuerzas Globales	
Factor	**Impacto**

Pandemia	El efecto de la pandemia por COVID 19 ha acelerado la adopción de tendencias digitales y por consiguiente la necesidad de redoblar esfuerzos en ciberseguridad
Conflictos armados entre países	Guerras armadas entre países afectan no solo vida cotidiana de los países involucrados, sino que también han extendido el conflicto al espacio digital con ciberataques dirigidos
Globalización	Un mundo digital más conectado da lugar a posibles ciberataques no solo del país de origen, sino de cualquier lugar del planeta

(Elaboración propia, 2022)

6. Contexto interno

Actualmente me encuentro trabajando para una empresa mexicana de tecnología en la cual a lo largo de 8 años de experiencia como administrador de infraestructura y sistemas operativos he visto de primera mano el aumento en el número de eventos e incidentes por ciberataques, la necesidad de los clientes por certificarse en normas internacionales en el manejo y protección de datos cada vez más frecuente, así como el aumento en la demanda de servicios de ciberseguridad. La empresa en la cual me desempeño actualmente identificó esta necesidad y dentro de su estrategia de crecimiento la llevó a crear una unidad de negocio dedicada para brindar servicios de ciberseguridad.

Realizando un análisis comparativo con experiencia laboral previa para una empresa de centro telefónico (*Call center*) que contaba con más de 250 posiciones de trabajo, es decir, equipos de cómputo con extensión telefónica pude identificar que realmente no siempre se cuentan con las medidas de ciberseguridad para proteger los sistemas informáticos e información digital, es por eso que la conexión de ambas experiencias me lleva a pensar en un emprendimiento de una empresa de ciberseguridad enfocada en Pymes de la zona metropolitana de México con procesos digitales que cuenten y/o con más de 25 estaciones de trabajo, esto es, equipos de cómputo o dispositivos móviles con acceso al sistema e información de la organización.

La idea y el proyecto se realizará en un esfuerzo en conjunto con un colega laboral y compañero de carrera en sistemas computacionales en la Universidad de las Américas, esto significa que, la creación de la empresa de ciberseguridad constará de dos socios y como implementadores podrían sumarse colegas del medio, un poco más abajo en esta misma sección se describirán con más detalle la estructura organizacional.

A partir del entendimiento de que una de las características de las Pymes es tener personal limitado y este personal está enfocado en los procesos y operación propios del negocio se plantea tomar la figura de CISO (Chief Information Security Officer) para estas y así no descuiden sus operaciones y negocio por invertir demasiado tiempo en ciberseguridad, o sea, dejar este tema para algún especialista en la materia.

El CISO Algunas de las funciones que realiza un CISO son las siguientes:

- Diseñar y alinear la estrategia de ciberseguridad con la estratégica general de la organización.
- Analizar vulnerabilidades de ciberseguridad para mitigarlas.
- Responder antes cualquier incidente de ciberseguridad.
- Ser responsable de la administración de ciberseguridad.
- Reportar cualquier incidente de ciberseguridad.
- Salvaguardar y proteger la información y activos digitales de la organización.
- Concientizar y sensibilizar a los miembros de la organización sobre la seguridad de la información.

Estas son algunas de las principales funciones del CISO, sin embargo, derivado del cambio de hábitos de trabajo, compras y entretenimiento de los consumidores derivado de la pandemia de COVID 19

planteado en el estudio Panorama del ecosistema de ciberseguridad (Endeavor & Paypal, 2020, pág. 4.): "*Este hecho ha transformado el papel de los CISO en las organizaciones, pues ya no solo se dedican a proteger y resguardar la información de la empresa: ahora son elementos indispensables para la entrega de valor comercial para muchas de las organizaciones.*" Esto nos deja ver que el papel de la ciberseguridad y la figura del CISO toma más relevancia en estos tiempos, se considera un papel clave en entrega de valor y estrategia de negocio, en este mismo estudio el apartado es titulado "Ciberseguridad: el gran diferenciador para el emprendimiento" lo cual refleja un poco de lo que se propone en el presente proyecto acerca de crear una empresa de ciberseguridad que ayude a la Pymes en esta materia.

La ciberseguridad puede ser tan compleja, amplia y profunda como se pueda imaginar, sin embargo, para situarnos en un marco de referencia en cuanto niveles y alcance de los servicios que se desean ofrecer se plantea el siguiente modelo:

Tabla 2. Nivel de madurez de ciberseguridad

Nivel	Tipo	Descripción
1	Preventivo	Actuar antes de que las ciberamenazas se materialicen y se conviertan en un problema
2	Activo	Monitoreo y vigilancia activa para contener posibles ciberataques
3	Proactivo	Anticipar e identificar ciberamenazas para estar protegido en caso ciberataque por medio de correlación de eventos e inteligencia artificial

(Elaboración propia, 2022)

La oferta de servicios de la nueva empresa de ciberseguridad está enfocada en ayudar a las Pymes con procesos digitales en alcanzar al menos el nivel 1 y preferentemente el nivel 2 de madurez de ciberseguridad para diseñar una estrategia de ciberseguridad para cada organización.

6.1 Misión, Visión y Valores

Se establece una misión, visión y valores que ayudarán a la organización a conducirse y tomar decisiones dentro de este marco y ayudarán a diseñar una estrategia bajo estos conceptos.

Misión: Ser un socio clave en ciberseguridad para nuestros clientes para ayudarlos a alcanzar sus objetivos tecnológicos y de seguridad.

Visión: Ser el socio más confiable y experimentado en ciberseguridad para nuestros clientes para que solo se tengan que preocupar por su negocio y no por la ciberseguridad y tecnología.

Valores:

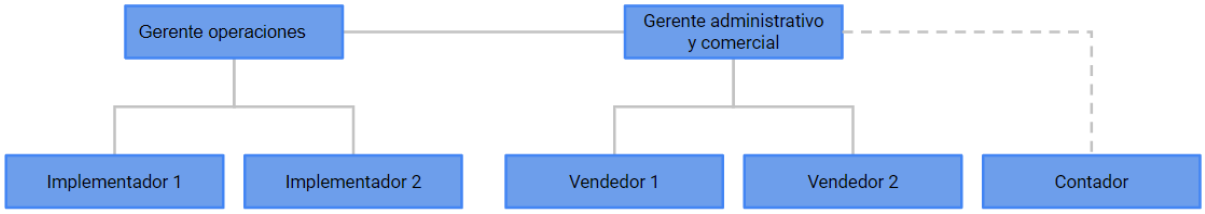
- **Flexibilidad**: Saber adaptarnos a las necesidades y exigencias de nuestros clientes para ayudarlos a que logren sus objetivos tecnológicos y de ciberseguridad.
- **Agilidad**: Priorizar la urgencia y criticidad de las necesidades de nuestros clientes para atenderlos en el mejor tiempo posible.
- **Servicio al cliente**: Todos nuestros procesos y estructura están orientadas en honrar nuestra promesa de ser el socio más confiable para nuestros clientes, así como cumplir con nuestros valores de flexibilidad y agilidad.

6.2 Estructura organizacional

En este caso al tratarse de la creación de una Pyme que ofrecerá servicios de ciberseguridad a otras Pymes, no sería una excepción en cuanto a algunas de las características de estas, o sea, normalmente cuentan con recursos limitados, lo cual no es exclusivo de solo de las Pymes, poco reconocimiento de marca al poco tiempo de su creación, limitada fuerza de trabajo, es por eso que en este último punto se propone iniciar la Pyme de servicios de seguridad con el siguiente personal para cumplir con los compromisos comerciales:

- Vendedor 1
- Vendedor 2
- Implementador/Capacitador 1
- Implementador/Capacitador 2
- Implementador/Capacitador 3 (contratación al segundo año de operación)
- Gerente operaciones (Socio 1)
- Gerente administrativo y comercial (Socio 2)

Figura 7. Organigrama empresa de ciberseguridad año 1



(Elaboración propia, 202

7. Marco teórico y conceptual

7.1 Caso de negocio

Entendamos un caso de negocio como un análisis de una oportunidad de negocio, donde se evalúan las condiciones de mercado y se realiza un análisis financiero para buscar la aprobación de un presupuesto y obtener recursos para ese proyecto, en poca palabras el resultado de un caso de negocio es solicitar que se invierta en una oportunidad de negocio. Comúnmente un caso de negocio contiene los siguientes rubros:

- Resumen ejecutivo
- Problema y oportunidad
- Entorno de mercado
- Entorno competitivo
- Impacto y análisis financiero
- Análisis de riesgos
- Supuestos
- Conclusiones y recomendaciones

Resumen ejecutivo normalmente se realiza al final del documento y en una sola hoja se explica el por qué, qué, dónde, quién y cuándo de la oportunidad de negocio.

Problema y oportunidad describe con la mayor claridad posible el problema, deseo, necesidad o frustración que motivará al cliente a comprar el producto o servicio en cuestión, o sea, ¿Cómo es la situación actual del cliente sin este producto o servicio?. También se plantean alternativas de solución.

Entorno de mercado proporciona una visión general del mercado, en otras palabras, ¿Se trata de un mercado en crecimiento? ¿Quiénes son los líderes del mercado? ¿Qué tamaño de mercado es? y considera algunos factores como políticos, tecnológicos, ambientales y sociales.

Entorno competitivo describe la situación de la empresa en el mercado, ¿Con quien se competirá? ¿En qué ámbitos se va a competir (ciertos productos o todos)? Análisis FODA (Fortalezas, Oportunidades, debilidades y amenazas).

Impacto y análisis financiero explica proyecciones de ventas, costos, presupuestos de salarios y mercadotecnia, etc. normalmente proyectados a 3 o 5 años. También describe cómo podría verse afectados los recursos por dicha inversión, así como disponibilidad de recursos.

Análisis de riesgos identifica y analiza los principales obstáculos que podrían impedir el servicio proporcionado por el proyecto ¿Cómo superar estos obstáculos?, ¿Cómo pueden afectar esos obstáculos a la empresa? ¿Qué probabilidad de materializarse existe?.
Supuestos como el caso de negocio se trata de predecir el futuro se tendrán que listar supuestos que den justificación al análisis.

Conclusiones y recomendaciones justifican los pros y contras de la oportunidad de negocio, así como los impactos de llevar o no a cabo dicho proyecto.

7.2 Business Model Canvas

Un modelo de negocio es en realidad una serie de suposiciones e hipótesis y para entender mejor el modelo de negocio del presente trabajo se propone utilizar el *Business Model Canvas* de Alexander Osterwalder, quien propone la plantilla más completa sobre la cual construir esas suposiciones e hipótesis. Dicha plantilla consta de 9 bloques muy bien organizados para exponer la racionalidad detrás de cómo se pretende generar, entregar y capturar valor por la nueva empresa de servicios de ciberseguridad. Los nueve bloques que se describirán son:

1. Segmentos de clientes
2. Propuesta de valor
3. Canales de distribución
4. Relaciones con clientes
5. Flujos de ingresos
6. Recursos clave
7. Actividades clave
8. Relaciones clave
9. Estructura de costos

La propuesta de valor para el segmento de mercado que se pretende atender es el acompañamiento, asesoría y consultoría en forma de un CISO externo para las Pymes orientado a un precio accesible para estas y atención personalizada y directa que muchas veces las grandes empresas que se orientan a cuentas grandes no atienden. Es por lo que, se considera el siguiente modelo Canvas:

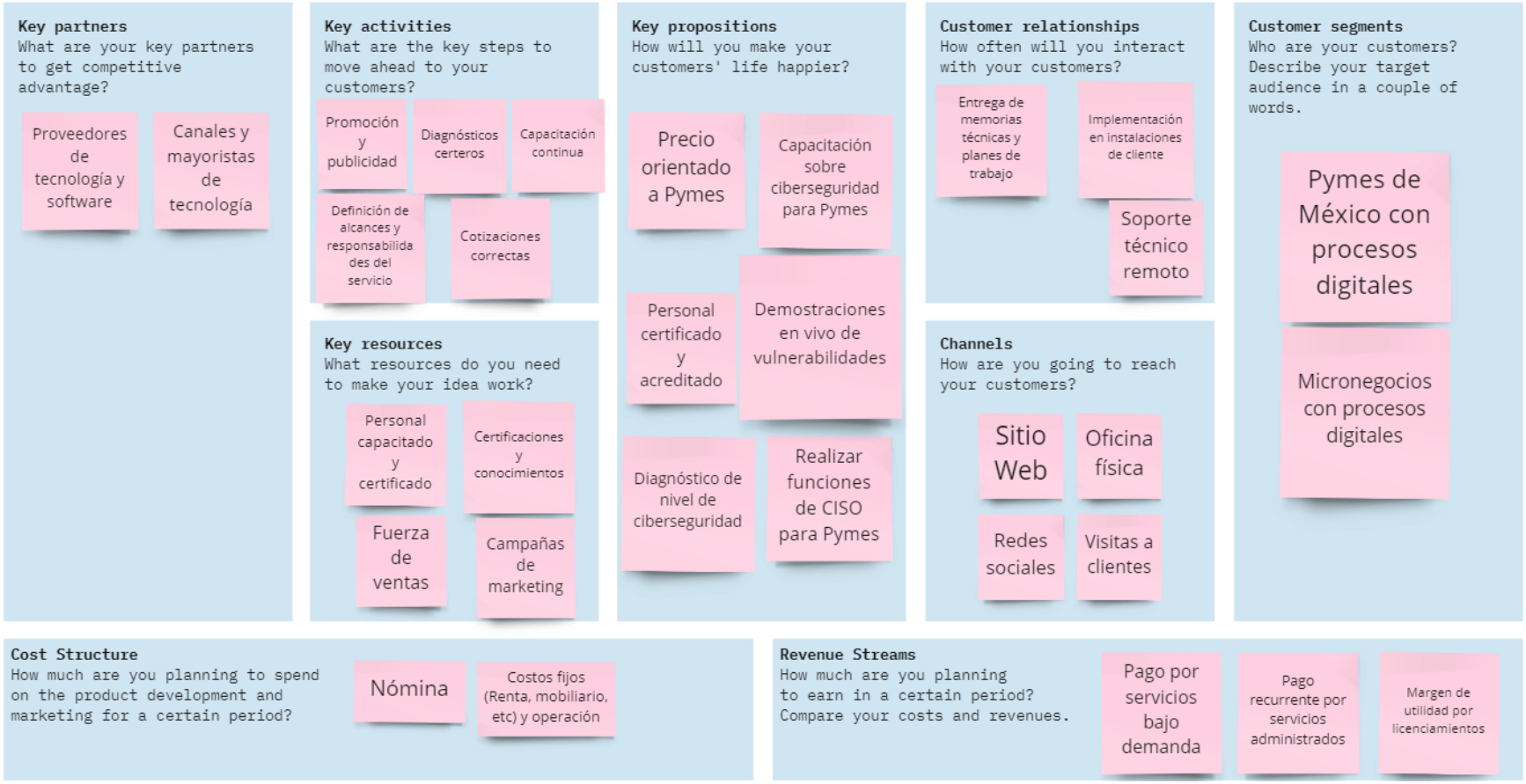
Tabla 3. Business Model Canvas empresa de ciberseguridad acotado

Valor		
Propuesta de valor: - Precio orientado a Pymes - Personal calificado y certificado - Diagnóstico de nivel de ciberseguridad - Realizar funciones de CISO para Pymes	**Relación con el cliente:** - Entrega de memorias técnicas y planes de trabajo - Implementación en instalaciones de cliente - Cotizaciones en 3 días hábiles - Soporte técnico remoto	**Segmento de cliente:** - Pymes de México con procesos digitales - Pymes con al menos 25 equipos de cómputo (Servidores, desktops, dispositivos móviles, etc.)

- Capacitación de ciberseguridad orientada a Pymes - Acompañamiento y asesoría en su camino a certificación en estándares de seguridad	**Canales:** - Sitio Web - Oficina física - Redes sociales - Visitas a clientes	
Fuentes de ingreso: - Pago por servicios bajo demanda - Pago recurrente por servicios administrados - Margen de utilidad por licenciamientos		

(Elaboración propia, 2022)

Figura 8. Business Model Canvas empresa de ciberseguridad completo



(Elaboración propia, 2022

7.3 Análisis FODA proyectado

Si bien, el análisis FODA se realiza sobre una organización o ente existente, la intención de realizarlo en el presente proyecto en donde la empresa aún no existe es, identificar y prever el entorno y capacidades con las cuales la empresa de ciberseguridad nacerá, es decir de antemano ya se conocen y se esperan algunas condiciones como contar con personal limitado, se conocen algunos aspectos de la competencia y de la industria que seguirán vigentes al momento de ejecutar el plan de negocios.

Tabla 4. Análisis FODA proyectado de empresa de ciberseguridad

FODA EMPRESA DE CIBERSEGURIDAD		
	INTERNO	EXTERNO
POSITIVO	**Fortalezas**: ● Agilidad y flexibilidad para entregar el servicio ● Precio accesible para Pymes ● Dominio y conocimiento en ciberseguridad ● Personal certificado en tecnologías y estándares de seguridad	**Oportunidades**: ● Incremento de ventas en línea y transformación digital ● Nacimiento de nuevas Pymes en México ● Ciberseguridad como un tema de novedad y permanente ● Mayores regulaciones en protección de datos y cumplimiento de estándares de ciberseguridad
NEGATIVO	**Debilidades**: ● Limitada fuerza laboral ● Marca nueva con poco reconocimiento ● Cartera de clientes limitada	**Amenazas**: ● Creación de nuevos competidores en ciberseguridad ● Incursión de fabricantes de tecnología en consultoría en ciberseguridad para Pymes ● Nuevas modalidades de ciberataques y fraudes en línea

(Elaboración propia, 2022)

Fortalezas

Agilidad y flexibilidad para entregar el servicio. El ser una empresa emergente permitirá ofrecer servicios al cliente más flexibles y ágiles, a diferencia de empresas grandes existentes que cuentan con estructuras organizacionales complejas que implican largos procesos de autorización.
Precio accesible para Pymes. Se puede ofrecer un precio más accesible a los clientes, ya que no se destinan grandes costos (o costos fijos) a numerosas oficinas, nóminas de un amplio personal, etc.
Dominio y conocimiento en ciberseguridad. El personal pudiera ser tan amplio, pero sí calificado con amplia experiencia en temas de ciberseguridad.
Personal certificado en tecnologías y estándares de seguridad. Es importante amparar experiencia y dominio del conocimiento con acreditaciones de cursos y certificaciones en tecnologías y estándares de seguridad.

Debilidades

Limitada fuerza laboral. Al ser una empresa emergente es muy probable que no se pueda contar con una amplia plantilla de colaboradores y se deberá tener un perfil más amplio para desempeñar varios roles.
Marca nueva con poco reconocimiento. El mundo de los negocios con frecuencia prefiere no tratar con empresas que están empezando y que se conoce poco de su trabajo.
Cartera de clientes limitada. Con en muchas ocasiones sucede para los nuevos negocios que se ven limitados en su cartera de clientes y conforme van ganando experiencia y reputación esta también puede incrementar.

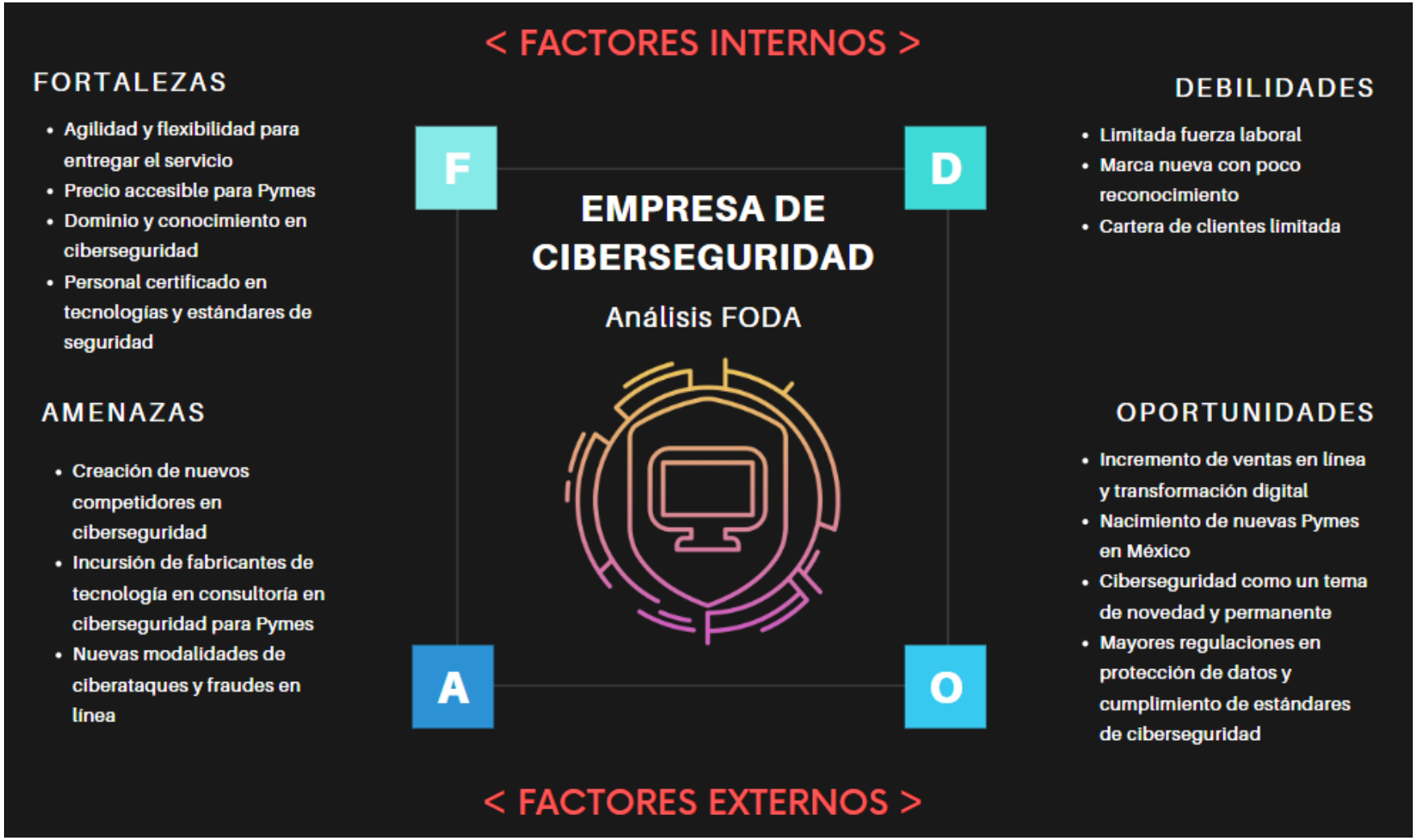
Amenazas

Creación de nuevos competidores en ciberseguridad. La ciberseguridad al ser una tendencia digital y un mercado en crecimiento es normal que muchos se sientan atraídos por incursionar y obtener beneficios en etapas tempranas de un mercado con estas características.
Incursión de fabricantes de tecnología en consultoría en ciberseguridad para Pymes. Los grandes fabricantes y proveedores de tecnología ya cuentan con recursos, reconcomiendo y posicionamiento de marca que representan ventajas para ellos en comparación con nuevos competidores que aún no son conocidos.
Nuevas modalidades de ciberataques y fraudes en línea. Al igual que la tecnología que avanza más rápido que las regulaciones, procesos y normas también las modalidades de ciberdelincuencia están en constante evolución y resulta más lento tratar de entenderlos y generar mecanismo de defensa que el surgimiento de nuevas modalidades.

Oportunidades

Incremento de ventas en línea y transformación digital. Estas tendencias digitales crearán un ciberespacio más extenso y cada vez más conectado que necesitará ser protegido y gestionado con prácticas de seguridad, en otras palabras, la ciberseguridad seguirá siendo demandada en los próximos años a medida que el ciberespacio siga creciendo.
Nacimiento de nuevas Pymes en México. Es verdad que la tasa de mortalidad de Pymes aún es muy alta, sin embargo, también se tiene gran potencial con el nacimiento de nuevas Pymes que requerirán servicios de ciberseguridad para ayudarse a sobrevivir en un ciberespacio en constante riesgo.
Ciberseguridad como un tema de novedad y permanente. El resto de las tendencias digitales que ya hemos mencionado difícilmente podrían seguir existiendo sin la ciberseguridad.
Mayores regulaciones en protección de datos y cumplimiento de estándares de ciberseguridad. El endurecimiento y creación de nuevas normas dará más materia para adoptar una cultura y prácticas de seguridad para las Pymes y grandes empresas.

Figura 9. Análisis FODA proyectado de empresa de ciberseguridad



(Elaboración propia, 2022)

7.4 Análisis de industria de ciberseguridad en México con el modelo de las 5 fuerzas competitivas de Porter

Con ayuda del modelo de las 5 fuerzas competitivas de Porter analizaremos los siguientes rubros:

1. Poder de negociación de los proveedores
2. Poder de negociación de los clientes
3. Productos sustitutos
4. Rivalidad dentro del sector
5. Nuevos competidores

Tabla 5. Análisis 5 Fuerzas de Porter de empresa de ciberseguridad

<table>
<tr><th colspan="3">Modelo de 5 Fuerzas de Porter de empresa de ciberseguridad</th></tr>
<tr><td rowspan="2">Proveedores poder de negociación:
El conocimiento especializado de proveedores debe ser superior al del cliente
Intensa competencia en precios de los fabricantes por ganar cuentas
Alianzas con fabricantes para dar servicio al cliente final
Fabricantes de tecnología y ciberseguridad son proveedores y competencia al mismo tiempo</td><td colspan="2">Posibles nuevos competidores:
Competidores extranjeros como Fortinet, Cisco, Kaspersky, etc.
Fabricantes de tecnología incursionando en servicios de ciberseguridad como IBM, Microsoft, Cisco, etc.
Nuevos competidores iniciando una curva de aprendizaje y madurez
Departamentos de ciberseguridad internos de cada empresa</td></tr>
<tr><td>Rivalidad dentro del sector:
Número amplio de competidores bien posicionados con buena reputación
Mercado en crecimiento y cada vez más competidores
Nuevos competidores con mínima experiencia pero con precios menores
Jugadores compiten por ganar cuentas grandes como gobierno
Estrictos requisitos para competir por licitaciones</td><td rowspan="2">Clientes poder de negociación
Bajo/medio nivel de conocimiento de cliente para tomar decisiones tecnológicas y seguridad
Muchas alternativas para elegir proveedor
Reputación para consultora por tener su cuenta
Clientes grandes pueden realizar concursos y licitaciones para elegir proveedor de ciberseguridad</td></tr>
<tr><td colspan="2">Productos sustitutos:
Oferta de cursos de ciberseguridad en línea
Auto capacitación y desarrollo de material interno por parte de Pymes
Nube pública bajo ciertos criterios de regulación
Departamentos de TI internos de cada empresa</td></tr>
</table>

(Elaboración propia, 2022)

Poder de Negociación de los proveedores:

- **El conocimiento especializado de proveedores debe ser superior al del cliente**: Cuando el cliente no entiende mucho de sistemas informáticos y ciberseguridad (lo cual no necesariamente está mal), recurre a proveedores que sean expertos en esta materia y los asesore, aquí es cuando los proveedores pueden tomar ventaja para proponer soluciones que más convengan a intereses del mismo proveedor.
- **Intensa competencia en precios de los fabricantes por ganar cuentas***:* Muchos clientes grandes lanzan RFPs (Request for proposal) donde se pone a competir a varios proveedores para proponer una solución bajo ciertos lineamientos como presupuesto, necesidades, exigencias de alta disponibilidad, rendimiento, etc. Y frecuentemente gana el proveedor con el mejor precio y solución tecnológica.
- **Alianzas con fabricantes para dar servicio al cliente final***:* En ocasiones los fabricantes de tecnología buscan algún partner en específico para competir por ganar un proyecto nuevo de algún cliente final, la elección de estos partners va en función de su capacidad de financiamiento, conocimiento técnico para implementar, relacionamiento con la cuenta, crédito disponible, certificaciones requeridas, etc.
- **Fabricantes de tecnología y ciberseguridad son proveedores y competencia al mismo tiempo***:* Hay fabricantes de tecnología que son proveedores de infraestructura de otros consultores de ciberseguridad, sin embargo, en ocasiones deciden ir a ofertar directamente al cliente alguna solución, quitando del medio a canales, centros de datos, partners, mayoristas, etc. Volviéndose su competencia.

Poder Negociación de los clientes:

- **Bajo/medio nivel de conocimiento***:* En ocasiones los clientes tienen un buen nivel técnico por lo cual saben muy bien qué es lo que necesitan y comparan opciones antes de elegir un proveedor, esto es muy común cuando el cliente inicialmente administraba sus sistemas y posteriormente delegó la administración a un tercero. En estos casos no solo es importante el precio antes de elegir un proveedor de tecnología y seguridad.
- **Muchas alternativas para elegir proveedor***:* A pesar de que en México no sobran los proveedores de ciberseguridad, los clientes tienen distintas alternativas para elegir proveedor (nacionales, extranjeros, reconocidos, nuevos, pequeños, grandes, etc.). Esto le brinda al cliente poder de negociación principalmente en servicios adicionales como valor agregado a la oferta y en ocasiones sobre el precio.
- **Reputación para consultora por tener su cuenta***:* Existen clientes grandes o importantes que con el hecho de tenerlos como clientes genera cierto prestigio para el proveedor de ciberseguridad y a su vez, da confianza para otros clientes al saber que el mismo proveedor atiende clientes de prestigio e importantes.
- **Clientes grandes realizan concursos y licitaciones para elegir proveedor de ciberseguridad***:* Los clientes suelen realizar concursos e invitar a varios proveedores para competir entre ellos y proponer la mejor solución al mejor precio posible.

Productos Sustitutos:

- **Oferta de cursos de ciberseguridad en línea***:* Cada vez existe más contenido en línea sobre distintos temas de interés como en este caso ciberseguridad que pudieran ofrecer información básica para cumplimiento de algún estándar de seguridad, ejemplos de este tipo de sitios pudieran ser Udemy, Coursera, etc.
- **Auto capacitación y desarrollo de material interno por parte de Pymes***:* Las Pymes a falta de presupuesto anual asignado a rubro de ciberseguridad podrían desarrollar material interno como videos, cuestionarios y documentos para la capacitación de su personal, sin embargo, esto no resolvería por completo este aspecto, ya que la ciberseguridad es un conjunto de prácticas y elementos como son cultura de ciberseguridad, sistemas de ciberseguridad y conocimiento y prácticas de seguridad.
- **Nube pública bajo ciertos criterios de regulación:** Una tendencia es migrar a la nube pública como Google, Azure y AWS de Amazon, etc. Así los clientes ya no se preocupan por la tecnología y seguridad detrás de sus sistemas, ni las condiciones del centro de datos, ya que estos proveedores de nube se encargan de todas esas complejidades y el cliente solo se

preocupa por el cargo recurrente. Cabe mencionar que la mayoría de estas nubes se encuentran fuera del país y por algunas regulaciones las empresas no pueden almacenar su información fuera del país, por ello no en todos los casos es viable esta estrategia.

- **Departamento de TI interno de cada empresa***:* A pesar de que el departamento de TI de cada empresa se encarga más de la operación y mantenimiento de los sistemas se decide asignarle una labor más estratégica para la empresa como es la ciberseguridad y la gestión de riesgos, esto por desconocimiento sobre el tema, falta de presupuesto o bien baja prioridad al tema.

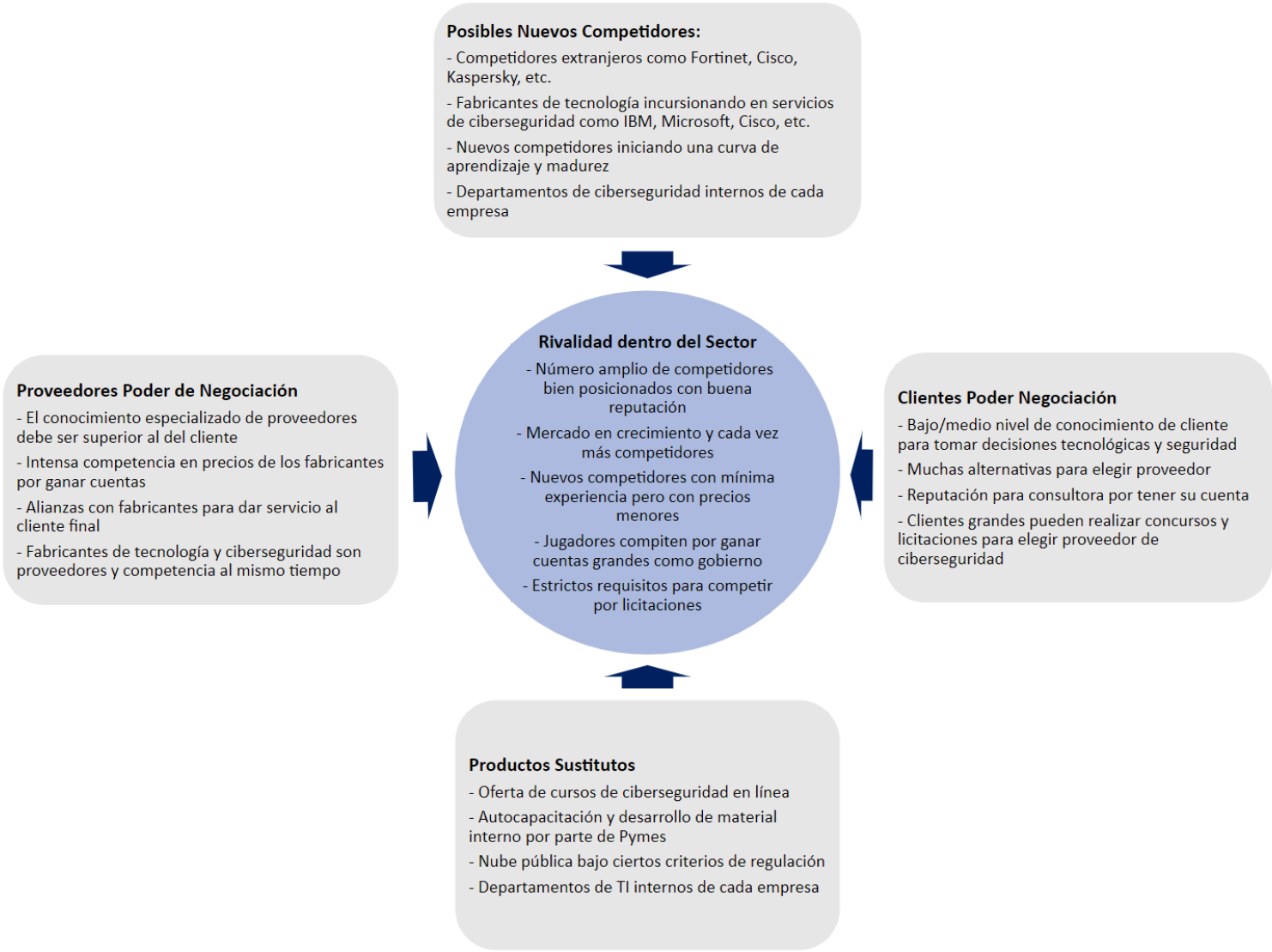
Rivalidad dentro del Sector:

- **Número amplio de competidores bien posicionados con buena reputación***:* Existen diversas opciones de proveedores de infraestructura y servicios de ciberseguridad en México por lo cual la rivalidad se vuelve intensa por ganar las cuentas grandes, sin embargo, aún existe un terreno no tan saturado en las Pymes que inician su recorrido en temas de ciberseguridad.
- **Mercado en crecimiento y cada vez más competidores***:* La ciberseguridad al ser una tendencia digital es normal que se surjan cada vez más competidores para ofrecer este tipo de consultorías y servicios hasta que se sature este mercado como ha ocurrido con otros mercados.
- **Nuevos competidores con mínima experiencia, pero con precios menores***:* Al ser un mercado en crecimiento también es usual que nuevos jugadores con el afán de incursionar en mercado atractivo ingresen sin los conocimientos, herramientas y experiencia suficientes y en el camino ir puliendo estas carencias, y para lograrlo es común que sus precios sean inferiores a competidores mejor posicionados pero que para las Pymes pudiera ser un buen trato.
- **Jugadores compiten por ganar cuentas grandes como gobierno***:* Comúnmente los proveedores buscan ganar las cuentas grandes de privados y gobierno ya que representan ciertas garantías como remuneración, prestigio por tener la cuenta de una empresa grande, cierta certidumbre de cumplimiento de contratos, entre otros.
- **Estrictos requisitos para competir por licitaciones***:* Las empresas grandes y gobiernos al tener operaciones críticas demandan requisitos y exigencias mayores que probablemente no todos los proveedores pudieran cumplir.

Posibles Nuevos Competidores:

- **Competidores extranjeros como Fortinet, Cisco, Kaspersky, etc.***:* La llegada de competidores extranjeros siempre es una amenaza para las empresas locales, ya que en la mayoría de las ocasiones también son empresas de renombre y buena reputación.
- **Fabricantes de tecnología incursionando en servicios de ciberseguridad como IBM, Microsoft, Cisco, etc.***:* Existen fabricantes de tecnología incursionando en ciberseguridad, quienes en cierto momento pudieran convertirse en proveedor y competencia al mismo tiempo.
- **Nuevos competidores iniciando una curva de aprendizaje y madurez***:* Surgimiento de nuevos competidores que inician de cero a diferencia de los fabricantes que llevan años en un mercado e incursionan en la ciberseguridad ya cuentan con experiencia y posicionamiento de marca
- **Departamentos de ciberseguridad internos de cada empresa***:* Es una buena práctica, sin embargo, en muchas ocasiones no es suficiente solo contar con personal interno para el cumplimiento de todo lo que implica la ciberseguridad. El departamento o área debe estar asesorado y acompañado de expertos externos para lograr los objetivos de seguridad de la empresa.

Figura 10. Análisis 5 Fuerzas de Porter de empresa de ciberseguridad



(Elaboración propia, 2022)

7.5 Casos de estudio

7.5.1 4 Cybersecurity Strategies for Small and Midsize Businesses (HBR)

Descripción:

En marzo del 2021, la IA (Inteligencia Artificial) detectó un ciberataque sofisticado que explotó una vulnerabilidad de día cero en varias empresas. La IA detectó, investigó y contuvo el ataque, y descubrió que se trataba de una amenaza completamente nueva. Semanas después, esta acometida se atribuyó públicamente a un ente del estado chino conocido como APT41. Las organizaciones afectadas por el ataque incluían gobiernos, entidades públicas, infraestructura crítica, empresas grandes y sorprendentemente, también empresas medianas, (Gustafsson , 2021.).

Anteriormente, se ha mencionado que vivimos en un mundo cada vez más digital y conectado, sin embargo, los ciberataques también han evolucionado y cada vez son más sofisticados y recurrentes por lo cual las grandes empresas e instituciones públicas ya no son los únicos objetivos de ciberataques, es decir, los ciberdelincuentes han identificado que estas son quienes más esfuerzos ponen en prácticas de ciberseguridad, mientras que, las pequeñas y medianas empresas son quienes menos esfuerzos realizan para proteger sus activos digitales, es por eso que bajo este contexto se rescata este caso "4 Cybersecurity Strategies for Small and Midsize Businesses" de *Harvard Business Review.*

Más adelante en el mismo caso cito textualmente lo siguiente:

"*Hemos entrado en una nueva era de ciberamenazas. Si se midiera como un país, el ciberdelito sería la tercera economía más grande del mundo después de Estados Unidos y China. Las empresas medianas a menudo se consideran un punto débil para los ciberdelincuentes.*"

Es alarmante el impacto en términos económicos que ha alcanzado la ciberdelincuencia, al grado de estar al nivel de las primeras 3 economías mundiales, es por eso que cada vez serán más recurrentes los intentos de ciberataques, y los ciberdelincuentes han identificado que existen más probabilidades de que sus ataques sean exitosos en las pequeñas y medianas empresas por su falta de medidas de ciberseguridad y que en muchas ocasiones podrían tener accesos legítimo a sistemas de empresas grandes por la naturaleza de sus operaciones o bien poseer información digital importante y crítica de empresas grandes, por lo que sería más fácil obtenerla por medio de los negocios medianos, o sea, encontrar la puerta más vulnerable o desprotegida.

7.5.2 NIST to Provide Cyber-Security Advice to SMBs Under New Federal Law

Descripción:

El Ex Presidente de los Estados Unidos Donald Trump promulgó durante su mandato la ley del NIST Ciberseguridad para pequeñas empresas, la cual solicita al instituto que proporcione recursos de ciberseguridad (guías, herramientas, mejores prácticas, estándares, metodologías, entre otros) a las pequeñas y medianas empresas de Estados Unidos, (W.Rash & J. Maguire, 2018.).

Continuando con la idea del caso anterior, donde deja en claro que las pequeñas y medianas empresas se han vuelto un objetivo atractivo para los ciberdelincuentes y estos ataques son cada vez más frecuentes y sofisticados que en muchas ocasiones estas empresas no cuentan con los recursos y el talento humano para hacerles frente. Resulta importante reconocer que en algún momento serán atacadas y muy probablemente esto será inevitable, sin embargo, lo que sí se puede hacer es tomar conciencia y seriedad a la ciberseguridad para identificar oportunamente los ciberataques y tener protocolos y conocimientos para contener un ciberataque.

Con este caso lo que se intenta demostrar es lo serio que se está tomando la ciberseguridad en pequeñas y medianas empresas, las cuales como ya se mencionó tienen mayores dificultades para poner en práctica medidas de ciberseguridad, se ha vuelto un problema tan grande que el Ex

Presidente Donald Trump promovió y firmó una ley para equilibrar y promover de alguna forma las prácticas de ciberseguridad abarcando a los pequeños y medianos negocios, esto significa, no dejar toda la responsabilidad a los gobiernos y grandes empresas, ya que como se describe en el caso anterior están son un blanco atractivo por su desinterés o bien escasos recursos para protegerse de la ciberdelincuencia.

7.5.3 Computadora portátil robada en el hospital causa acidez estomacal

Descripción:

Un ejecutivo del sistema de atención médica dejó su computadora portátil del trabajo con acceso a más de 40,000 consultas médicas y registros en su auto cerrado mientras atendía un asunto. El auto fue asaltado y robaron la computadora portátil que no contaba con ningún mecanismo de encriptado. A pesar de que el empleado denunció inmediatamente el robo a la policía y al departamento de TI del sistema de salud, quienes deshabilitaron el acceso remoto de la computadora portátil y comenzaron a monitorear la actividad. Los datos almacenados en el disco duro no estaban encriptados, los cuales eran datos confidenciales y personales de los pacientes. El hospital gastó más de $200,000 en remediación, monitoreo y mejoras operativas, (National Cybersecurity Alliance, 2020.).

Con este caso lo que se intenta demostrar es que, existe una combinación de factores que intervienen en prácticas de ciberseguridad, o sea, intervinieron factores humanos, tecnológicos y de procesos o protocolos. El factor humano debido a que un empleado dejó fuera de su vista un equipo de cómputo que pertenece a la organización y almacena información valiosa. El factor tecnológico fue clave al no contar con mecanismo de encriptado del disco duro, con esto se hubiera minimizado el problema dejándolo solo en una pérdida de activo físico, ya que la información habría sido ilegible para el ladrón. Los protocolos de la organización funcionaron y se atendieron oportunamente, sin embargo, no sirvió de mucho debido al descuido humano y la carencia tecnológica de herramienta de encriptación. Por esto es importante abordar la ciberseguridad desde los 3 factores de forma adecuada, ya que si uno de ellos falla puede anular la efectividad de los otros y genera un impacto severo para la organización como en este caso. Existen otros factores que el caso no menciona, sin embargo, en este tipo de ataques también deja secuelas a la reputación del negocio y desconfianza de los clientes hacia el hospital en este caso.

8. Alternativas de solución

Con el problema identificado y reconociendo la relevancia que tiene la ciberseguridad desde hoy y hacia el futuro en un mundo más digital y conectado, la visión de solución al grave problema y cada vez más recurrente y sofisticado ciberataque es crear una empresa enfocada en ayudar a Pymes con procesos digitales con su implementación y configuración de sistemas de seguridad cibernética y antivirus, así como oferta de capacitaciones sobre ciberseguridad y gestión de la información que las ayuden a minimizar el riesgo de ser víctima de dicho mal, contar con conocimientos sobre cómo actuar en caso de encontrarse bajo ataque y finalmente en el mejor de los casos evitar ser víctima de ciberataques gracias al seguimiento y cumplimiento de mejores prácticas de seguridad cibernética. El enfoque de las capacitaciones tiene como objetivo, brindar al personal que labora en Pymes conocimiento sobre ciberseguridad y generar conciencia y cultura de ciberseguridad. Con esto lo que se busca es ser su socio confiable de ciberseguridad para que tengan que preocuparse lo menos posible por este tema y se enfoquen en su negocio y tratar de evitar ser parte de las estadísticas de mortandad de Pymes, al menos por un tema de ciberataques.

8.1 Propuesta de catálogo de servicios de ciberseguridad

Recuperando **Tabla 2. Nivel de madurez de ciberseguridad** en la sección 6, es posible catalogar y ubicar cada servicio que se ofrecerá de acuerdo con el nivel de madurez en ciberseguridad que irán alcanzando los clientes en su camino hacia la protección de sus activos digitales y de sus clientes. Estos servicios están pensados principalmente en alcanzar los dos primeros niveles que son preventivo y activo, ya que la ciberseguridad es una disciplina que debe adaptarse constantemente a la situación

tan cambiante que exigen los nuevos ciberataques, que como ya se ha mencionado cada vez son más sofisticados y recurrentes, ya no solo son originados por aficionados, sino que ahora existen grupos organizados con intereses muy ambiciosos de estos. Anteriormente se mencionaba que si fueran una economía sería en este momento la tercera economía más grande del planeta de acuerdo con las pérdidas económicas generadas. En la siguiente tabla podemos ver cómo se clasifica el catálogo de servicios propuesto de acuerdo con el nivel de madurez de ciberseguridad que pueden alcanzar los clientes:

Tabla 6. Catálogo de servicios y nivel de madurez de ciberseguridad

Servicio a ofrecer	Nivel de madurez de ciberseguridad cubierto		
	Preventivo	**Activo**	**Proactivo**
Diagnóstico de nivel de madurez en ciberseguridad	●		
Implementación de consola de antivirus y endpoint	●	●	
Gestión de consola de antivirus y *endpoint*	●	●	
Capacitación en ciberseguridad	●		
Consultoría en implementación y cumplimiento de estándares de seguridad	●	●	●

(Elaboración propia, 2022)

Por supuesto que los servicios se adecuan con la necesidad y presupuesto de cada cliente, sin embargo, la solución ideal es una combinación o conjunto de algunos de ellos, ejemplo: La capacitación en ciberseguridad debería ser la base y primer paso para generar conciencia y sensibilidad de la seriedad del tema, así como reconocer la importancia de implementar el resto de los servicios. La ciberseguridad es una práctica constante, para ejecutarla se requiere una vigilancia permanente y reforzamiento en varias vías, procesos, tecnologías y humanos, en otras palabras, los procesos deben alinearse con las prácticas de ciberseguridad. Las tecnologías deben ser administradas y tener un mantenimiento constante, no basta con solo adquirirlas y tenerlas, requieren de constante revisión y atención de eventos y alertas que puedan surgir para actuar oportunamente ante vulnerabilidades o eventos de seguridad. Cuando se menciona el aspecto humano se refiere a que el personal debe contar con nociones sobre ciberseguridad, ya que aunque se cuente con la tecnología más avanzada y robusta, los descuidos humanos podrían vulnerar los sistemas de ciberseguridad, ejemplo: Un administrador de infraestructura que no se resguarda correctamente las credenciales de administrador de los sistemas, esto podría dejar accesible los sistemas a personas no autorizadas para el robo de información, alteración y/o interrupción de ellos.

Diagnóstico de nivel de madurez en ciberseguridad

Descripción: Reporte y análisis realizado por especialistas para identificar áreas de oportunidad y vulnerabilidades presentes en la red, sistemas y gestión humana que puedan representar un riesgo para la continuidad del negocio como un primer paso para el diseño de estrategia de ciberseguridad.

Alcance:

- Entrega de reporte con análisis de áreas de oportunidad en configuración tecnológica y humana
- Presentar y explicar hallazgos en una sesión al cliente
- El reporte es elaborado a partir de entrevistas y revisión de infraestructura de cliente

- El reporte se entrega dentro de los primeros 5 días laborables posterior al levantamiento de la información
- El análisis está basado en información proporcionada por el cliente y el acceso a su configuración

Beneficios: Ayuda a contrarrestar el tipo de ciberataque ingeniería social

Implementación de consola de antivirus y *endpoint*

Descripción: Implementación y configuración de antivirus como consola o bien *endpoint* dentro de la red del cliente.

Alcance:

- La implementación incluye licenciamiento de antivirus TrendMicro (ver gráfica de Gartner en anexos)
- Incluye software de instalación
- La implementación y costo es por equipo de cómputo, servidor o dispositivo móvil
- La infraestructura provista por cliente debe cumplir con prerrequisitos de implementación
- Actualización de base de datos de antivirus a últimos niveles disponibles
- Escaneo inicial de los endpoints configurados
- Configuración de actualizaciones automáticas
- Entrega de memoria técnica y especificaciones de la configuración realizada
- Entrega de plan de trabajo de implementación y configuración
- Entrega de cronograma con base en necesidades del cliente

Beneficios: Ayuda a contrarrestar el tipo de ciberataque *spyware, phishing y ransomware*.

Gestión de consola de antivirus y *endpoint*

Descripción: Administración y configuración de antivirus como consola o bien *endpoint* dentro de la red del cliente.

Alcance:

- La administración incluye licenciamiento de antivirus TrendMicro (ver gráfica de Gartner en anexos)
- Se proporcionará software de instalación
- La administración y costo es equipo de cómputo, servidor o dispositivo móvil
- La infraestructura provista por cliente debe cumplir con prerrequisitos de implementación

Beneficios: Ayuda a contrarrestar el tipo de ciberataque *spyware, phishing y ransomware*.

Capacitación en ciberseguridad

Descripción:

- Diseño de programas de conciencia y cultura de la ciberseguridad en todos los niveles y perfiles de la organización
- Ejercicios de simulación de crisis durante un ciberataque
- Creación y formación de equipos de ciberseguridad con conocimiento especializado.
- Diseño de programas de gestión de amenazas internas para reconocer cuando algún empleado representa un riesgo para la seguridad de la información de la organización

Alcance:

- Entrega de planes de comunicación y difusión
- Asistencia en el diseño de campañas de concientización

- Asistencia en la definición de una estructura para crear un área de ciberseguridad con roles, funciones y responsabilidades

Beneficios: Ayuda a contrarrestar el tipo de ciberataque ingeniería social, *spyware, phishing y ransomware.*

Consultoría en implementación y cumplimiento de estándares de seguridad

Descripción: Asesoría especializada para Pymes en estándares de seguridad como ISO 27001 o PCI para su implementación y cumplimiento en la organización.

Alcance:

- Ser un guía en el entendimiento del estándar de seguridad
- Ser un guía en la implementación de cada control de seguridad
- Facilitador de información para la exitosa implementación de estándares de seguridad
- Ejercicio de simulación de auditoría de estándares de seguridad

Limitaciones de los servicios

- La infraestructura debe ser proporcionada por el cliente en ambiente virtual o físico según sus posibilidades
- Se podría cotizar el aprovisionamiento e implementación de la infraestructura requerida para los servicios arriba mencionados
- El precio de implementaciones y administración es por dispositivo
- El análisis y diagnósticos requieren de accesos a infraestructura e información proporcionada por el cliente

Beneficios: Ayuda a contrarrestar el tipo de ciberataque ingeniería social, *spyware, phishing y ransomware*.

Roles y responsabilidades

Cliente:

- Cubrir el 50% del costo del servicio por adelantado y el otro 50% al finalizar el servicio
- Asignar un facilitador para la realización de actividades del servicio
- Autorización de cambios a la configuración de los equipos, cambios de versiones e instalación de parches
- Proporcionar la información necesaria y verídica para una configuración correcta
- Aprovisionar infraestructura virtual o física para alojar antivirus
- Proporcionar matriz de contactos y escalación e interesados en cada proyecto
- Informar sobre cambios en la infraestructura que puedan afectar al buen funcionamiento del servicio
- Definición y aprobación de ventanas de tiempo para implementación
- Proveer espacio adecuado para capacitaciones presenciales en oficinas del cliente
- El cliente es propietario de las configuraciones realizadas en sus plataformas y sistemas de seguridad

Empresa de Ciberseguridad:

- Proveer el licenciamiento durante la vigencia del servicio
- Ejecutar las acciones pertinentes para la solución a violaciones de seguridad detectadas por la herramienta durante la vigencia del servicio
- Procesar solicitudes de servicio aprobadas por el Cliente
- Proporcionar planes de trabajo para ventanas de implementación y configuración
- Entrega de reportes mensuales de servicio al cliente
- Entrega de reporte de disponibilidad de la consola de antivirus
- Entrega de reporte de accesos lógicos a la consola de antivirus

Beneficios generales de todos los servicios:

- Prevención de ataques cibernéticos
- Protección de dispositivos críticos
- Reducción de las vulnerabilidades de la red interna
- Identificación de vulnerabilidades para su tratamiento

Con el catálogo de servicios propuesto aquí se busca ayudar a los clientes a atacar y mitigar algunos de los principales *pains* y sus impactos que ya hemos revisado en el presente trabajo. Ahora sabemos que existen algunos *pains* y barreras de adopción de la ciberseguridad, sin embargo, seguir ignorando el tema y no hacer nada al respecto ya no es opción, ya que hemos visto casos reales de ciberataques a este tipo de negocios y conocemos los impactos que pueden provocar. En la siguiente tabla podemos ver como cada uno de los servicios de ciberseguridad ofrecidos ayuda a mitigar y contrarrestar los principales ataques que ya hemos clasificado.

Tabla 7. Ciberataques atendidos por propuesta de servicios en ciberseguridad

Servicio a ofrecer	Tipos de ciberataque			
	Ransomware	**Phishing**	**Spyware**	**Ingeniería social**
Diagnóstico de nivel de madurez en ciberseguridad				●
Implementación de consola de antivirus y *endpoint*	●	●	●	
Gestión de consola de antivirus y *endpoint*	●	●	●	
Capacitación en ciberseguridad	●	●	●	●
Consultoría en implementación y cumplimiento de estándares de seguridad	●	●	●	●

(Elaboración propia, 2022)

Diagnóstico de nivel de madurez en ciberseguridad. Este servicio se enfoca en ayudar a las organizaciones y a su personal a evitar ser víctimas de ciberataques mayores iniciados o provocados por ingeniería social, el cual ya hemos visto que se trata de tácticas de engaño para hacer que la víctima revele información crucial para un posterior ataque mayor, ya que con el diagnóstico de nivel de ciberseguridad se tendrá una radiografía actual de la organización en cuanto procesos, tecnología y factor humano. El primer paso es reconocer e identificar áreas de oportunidad y así poder diseñar una estrategia de ciberseguridad. Una posible traducción de este servicio es ayudar a nuestros clientes a **integrar en su estrategia de negocio la ciberseguridad**, hoy en día la ciberseguridad es un gran diferenciador para los emprendimientos como ya hemos citado en estudios anteriormente.

Implementación de consola de antivirus y *endpoint*. Este servicio se enfoca en ayudar a las organizaciones y a su personal a evitar ser víctimas de ciberataques por la mayoría de los virus conocidos y nuevos cuando se mantiene una base de datos actualizada con el fabricante del antivirus. Estos antivirus pueden ayudar a identificar software malicioso o dañino que normalmente ingresan a los equipos o sistemas por medio de correo electrónico, medios extraíbles, *software* ilegítimo, etc. Este *software* malicioso es crucial para completar los ciberataques de tipo *ransomware*, *phishing* y *spyware.* En pocas palabras este servicio consiste en **venderle a nuestros clientes la tecnología** con la cual podrán avanzar en su camino hacia la ciberseguridad.

La propuesta tecnológica en herramientas de antivirus es TrendMicro por su posicionamiento en el mercado, ya que se encuentra en el cuadrante superior derecho, es decir líderes del mercado, en una escala de Líderes, Visionarios, Retadores y Buenos jugadores. Esto quiere decir que cuenta con experiencia, confianza de los clientes y madurez tecnológica.

Figura 11. Cuadrante Mágico de plataformas de protección Endpoint

(Microsoft, 2021, como se citó en Gartner 2021)

Gestión de consola de antivirus y *endpoint*. Este servicio se enfoca en ayudar a las organizaciones y a su personal a evitar ser víctimas de ciberataques por la mayoría de los virus conocidos y nuevos cuando se mantiene una base de datos actualizada con el fabricante del antivirus. Estos antivirus pueden ayudar a identificar *software* malicioso o dañino que normalmente ingresan a los equipos o sistemas por medio de correo electrónico, medios extraíbles, *software* ilegítimo, etc. Este *software* malicioso es crucial para completar los ciberataques de tipo *ransomware*, *phishing* y *spyware.* En pocas palabras este servicio consiste en **gestionar la tecnología de nuestros clientes** con la cual podrán contrarrestar los ciberataques antes listados.

Capacitación en ciberseguridad. Este servicio en conjunto con el diagnóstico de nivel de madurez en ciberseguridad deberían ser la base para iniciar el camino hacia la ciberseguridad de cualquier organización, ya que la sensibilización y concientización es el paso número 1, esto es, reconocer que la ciberseguridad es importante, es una inversión y no un gasto, ya que al igual que en el mundo físico ¿Quién hoy en día decide no poner candados y seguros a la ventanas de la casa? Esto parece una acción natural y normal que no necesita gran análisis para realizar, sin embargo, como ya hemos visto,

actualmente aún no se toma con la misma seriedad el ciberespacio a pesar de que en muchas ocasiones los activos e información digitales pueden ser más valiosos que el mobiliario de una empresa, por ejemplo una base de datos o el sistema de cobranza puede poseer información crítica con la cual no podría seguir operando el negocio, en cambio sí podría seguir operando sin los escritorios o bien las pantallas de las salas de juntas. Es por ello que este servicio se considera un servicio impulsor para el resto de ellos ya que a medida que se tenga conciencia de la ciberseguridad se buscará proteger con mayor seriedad el ciberespacio de la organización y el principal problema que trata de contrarrestar es el de ingeniería social.

Consultoría en implementación y cumplimiento de estándares de seguridad. Este servicio se podría considerar el servicio más avanzado y robusto del catálogo, debido a lo sofisticado que son los estándares de seguridad, sin embargo, una vez digeridos y aplicados de acuerdo con su cumplimiento, las organizaciones en automático deberían contar con un nivel **proactivo** de nivel de madurez en ciberseguridad, ya que los controles que marcan las normas consisten en implementar muchas de estas prácticas que se ofrecen como; antivirus activo, correlacionador de eventos, procesos de protección de datos, mecanismos de seguridad perimetral, controles de accesos físicos y lógicos, etc. Es por ello que este servicio ayuda a contrarrestar los 4 tipos de amenazas que hemos visto y se podría considerar como transferencia de conocimiento para nuestros clientes.

8.2 Propuesta de solución “No hacer nada”

Una alternativa como en muchos casos sucede, no solo en materia de ciberseguridad, es no hacer nada, debido a que hacer algo representa una inversión de recursos, los cuales pueden ser humanos, económicos, tiempo, etc. Sin embargo, esta alternativa podría llegar a ser más costosa que la propia inversión en prácticas de ciberseguridad. Pensemos en un paradigma muy similar, que es de los seguros, los cuales resulta no deseable pagar hasta que se llegan a necesitar y se podría lamentar no haberlos pagado, ya que los costos por un siniestro pueden ascender a cantidades mucho mayores que al pago por la prima del seguro, algo similar sucede con la ciberseguridad, actualmente aún no se toma con seriedad que debería y comúnmente se tienen ideas como; nadie querría mi información o no tengo nada que esconder o proteger ¿Para qué querría alguien atacarme?, entre otras ideas, seguro existen empresas y objetivos más grandes o atractivos para los ciberdelincuentes, sin embargo, este es el primer error, ya que los objetivos más atractivos no son los más grandes y protegidos, sino los más vulnerables, es decir siempre será atractivo un objetivo que no represente un reto vulnerar.

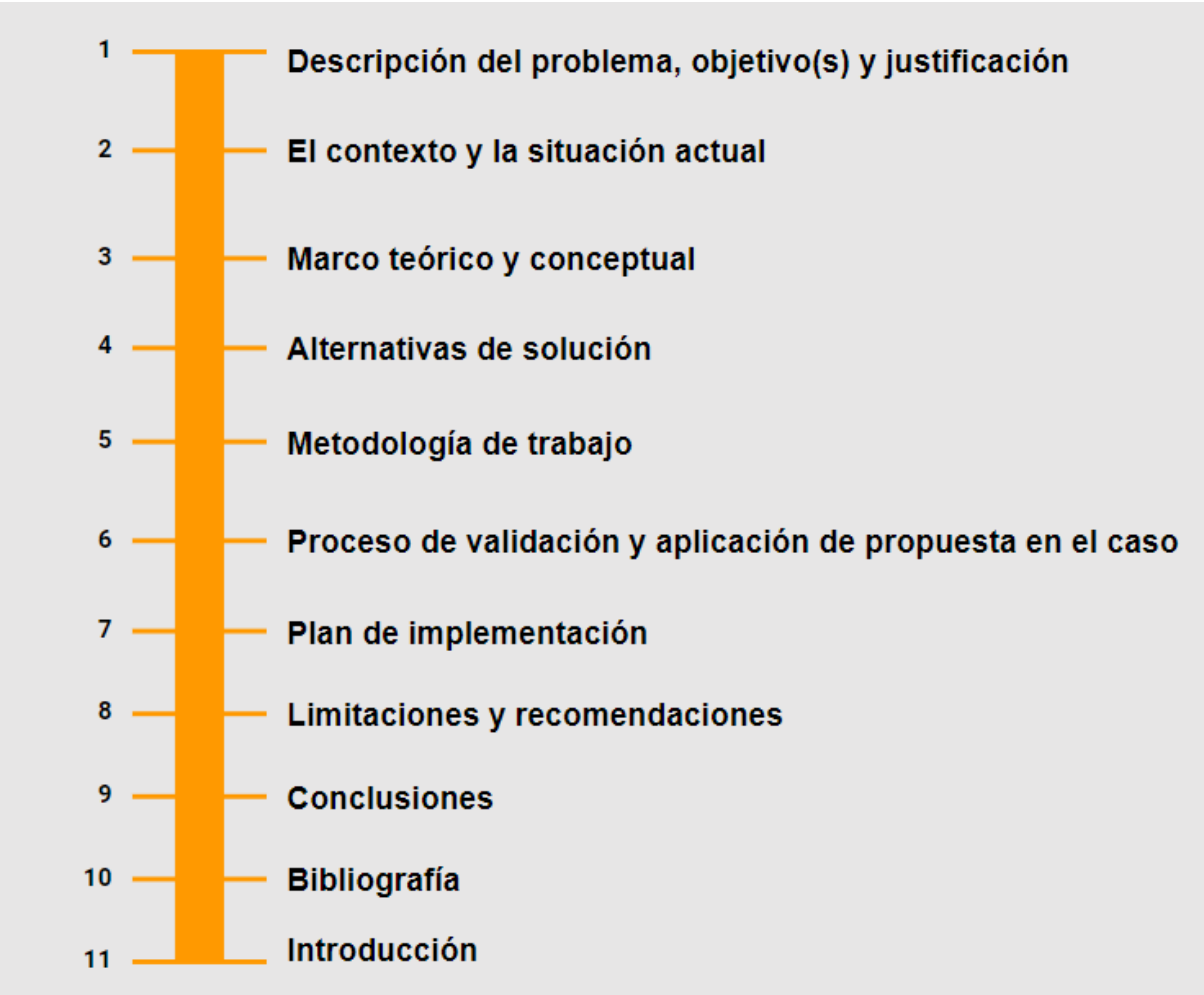
Las organizaciones por varios motivos que ya hemos visto no deberán darse el lujo de ver a la ciberseguridad como un gasto o algo innecesario, ya que conocemos los impactos y repercusiones de un ciberataque. Por lo cual las organizaciones tienen la decisión de elegir entre protegerse o seguir ignorando y relegando la ciberseguridad, pero ambas decisiones que se tomen el día de hoy tendrán consecuencias para el negocio y su futuro que es más próximo de lo que se piensa.

Son por estas razones que no debería optarse más por esta alternativa de **no hacer nada**, debido a que hoy vivimos en una situación en la cual, solo es cuestión de tiempo para ser víctimas de algún intento de ciberataque, tanto personas físicas como morales. Robert Muller ex agente del FBI dice lo siguiente (Endeavor & Paypal, 2020, pág. 10.): “*Hace un par de años las empresas se dividían entre aquellas que ya fueron atacadas y las que van a ser atacadas. Hoy se divide entre las que ya fueron atacadas y lo saben y las que no lo saben.*” Es alarmante esta afirmación debido a que la ciberdelincuencia es una práctica perpetua y es una carrera contra la ciberseguridad por estar un paso adelante.

9. Metodología de trabajo

La metodología que se utilizó para desarrollar el presente trabajo fue diseñada por las autoridades de la universidad Iberoamericana, específicamente por la coordinación de la maestría Gestión de la Innovación Tecnológica con el fin de estructurar el contenido y desarrollo de los trabajos de los alumnos de la materia de Proyecto de Vinculación Industrial y servir como guía de cumplimiento del contenido y aplicación del conocimiento adquirido a lo largo del maestría. Dicha metodología busca hacer que el conocimiento adquirido quede plasmado en forma de un trabajo completo que sea desarrollado usando esta guía (Herrera. 2022).
Dicha metodología consta de 11 pasos o secciones que llevan una secuencia lógica para desarrollar el trabajo respetando ese orden, por ejemplo; no se debería desarrollar las conclusiones antes de la descripción del problema y objetivos. En la siguiente tabla podemos ver el paso a paso de dicha metodología.

Figura 12. Metodología de trabajo



(Elaboración propia, 2022)

Para cada paso o sección del trabajo se le asigna un tiempo específico para desarrollar su contenido y así seguir avanzando con el resto de las secciones, adicionalmente se tienen 2 presentaciones de

revisión de avances que se encuentran entre el paso 3 y 4 y posteriormente entre el paso 5 y 6, o sea, posterior a la sección situación actual y la segunda presentación posterior a la metodología del trabajo. Los tiempos asignados y entregas fueron plasmados en un WBS (*Work Breakdown Structure*) tal como se muestra a continuación en la figura 15.

Figura 13. WBS del trabajo "DISEÑO DEL PROYECTO DE EMPRENDIMIENTO EMPRESA DE CIBERSEGURIDAD"

EDT	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
2	**Antecedentes**	**3 días**	**jue 18/08/22**	**lun 22/08/22**	
2.1	Tipos de ciberseguridad	**3 días**	**jue 18/08/22**	**lun 22/08/22**	
2.2	Tipos de ciberataques	**3 días**	**jue 18/08/22**	**lun 22/08/22**	
3	Descripción del problema, objetivo(s) y justificación	**3 días**	**mar 23/08/22**	**jue 25/08/22**	4
4	**El contexto y la situación actual**	**16 días**	**jue 25/08/22**	**jue 15/09/22**	**5**
4.1	Entorno del mercado	**16 días**	**jue 25/08/22**	**jue 15/09/22**	
4.2	Barreras de entrada	**16 días**	**jue 25/08/22**	**jue 15/09/22**	
4.3	Entorno competitivo	**16 días**	**jue 25/08/22**	**jue 15/09/22**	
4.4	Análisis de factores de entorno e impacto	**16 días**	**jue 25/08/22**	**jue 15/09/22**	
4.5	**Contexto interno**	**16 días**	**jue 25/08/22**	**jue 15/09/22**	
4.5.1	Misión, Visión y Valores	**16 días**	**jue 25/08/22**	**jue 15/09/22**	
4.5.2	Estructura organizacional	**16 días**	**jue 25/08/22**	**jue 15/09/22**	
4.5.3	Análisis de riesgos	**16 días**	**jue 25/08/22**	**jue 15/09/22**	
5	Primer presentación de avances	6 días	vie 16/09/22	vie 23/09/22	4,5,6,11
6	**Marco teórico y conceptual**	**10 días**	vie 23/09/22	**jue 06/10/22**	**15**
6.1	Caso de negocio	**10 días**	vie 23/09/22	**jue 06/10/22**	
6.2	Business Model Canvas	**10 días**	vie 23/09/22	**jue 06/10/22**	
6.3	Análisis FODA	**10 días**	vie 23/09/22	**jue 06/10/22**	
6.4	Modelo de las 5 fuerzas competitivas de Porter	**10 días**	vie 23/09/22	**jue 06/10/22**	
6.5	**Casos de estudio**	**10 días**	vie 23/09/22	**jue 06/10/22**	
6.5.1	Cybersecurity Strategies for Small and Midsize Businesses (HBR)	**10 días**	vie 23/09/22	**jue 06/10/22**	
6.5.2	NIST to Provide Cyber-Security Advice to SMBs Under New Federal Law	**10 días**	vie 23/09/22	**jue 06/10/22**	
6.5.3	Computadora portátil robada en el hospital causa acidez estomacal	**10 días**	vie 23/09/22	**jue 06/10/22**	
7	**Alternativas de solución**	**10 días**	**vie 07/10/22**	**jue 20/10/22**	**16,24**
7.1	Propuesta de catálogo de servicios en ciberseguridad	**10 días**	**vie 07/10/22**	**jue 20/10/22**	
7.2	Propuesta de solución "no hacer nada"	**10 días**	**vie 07/10/22**	**jue 20/10/22**	
8	**Métodología de trabajo**	**5 días**	**vie 21/10/22**	**jue 27/10/22**	
8.1	Métodología MGIT Universisdad Iberoamericana	**5 días**	**vie 21/10/22**	**jue 27/10/22**	
8.2	Métodos de validación	**5 días**	**vie 21/10/22**	**jue 27/10/22**	
8.3	Solución final aplicada al problema	**5 días**	**vie 21/10/22**	**jue 27/10/22**	
9	Segunda presentación de avances	5 días	**vie 28/10/22**	jue 03/11/22	
10	Proceso de validación y aplicación de propuesta en el caso	5 días	vie 04/11/22	jue 10/11/22	
11	Plan de implementación	5 días	vie 11/11/22	jue 17/11/22	
12	Limitaciones y recomendaciones	5 días	vie 11/11/22	jue 17/11/22	
13	Conclusiones	5 días	vie 11/11/22	jue 17/11/22	
14	Bibliografía	5 días	vie 11/11/22	jue 17/11/22	
15	Introduccion	5 días	vie 11/11/22	jue 17/11/22	
16	Entrega final	15 días	vie 11/11/22	jue 01/12/22	

(Elaboración propia, 2022)

Con la metodología utilizada se busca definir y entender un problema específico, describir el contexto y situación actual donde se presenta dicha problemática, así como situar la situación dentro de un marco teórico y conceptual, lo cual nos permitirá entender de mejor manera la situación usando herramientas y modelos teóricos reconocidos y aceptados, es decir se utilizaron los siguientes modelos y conceptos para realizar un análisis de diferentes elementos como son mercado, entorno, industria, financiero, etc.

- Modelo de 5 fuerzas de Porter
- Análisis FODA
- Business Model Canvas de Alexander Osterwalder
- Plantilla de tamaño de mercado de Dynamic
- Matriz de riesgos

Modelo de 5 fuerzas de Porter. Es un marco que propone el economista y profesor de Harvard, Micheal E. Porter en su artículo How Competitive Forces Shape Strategy, (HBR, 1979) donde dice que el conocimiento de las cinco fuerzas puede ayudar a una empresa a comprender la estructura de su industria y establecer una posición que sea más rentable y menos vulnerable a los ataques. Dichas fuerzas son el poder de negociación de los clientes, el poder de negociación de los proveedores, la rivalidad del sector, productos sustitutos y finalmente nuevos competidores o entrantes. Este modelo fue utilizado en la sección 6 Marco teórico y conceptual precisamente para tratar de entender el sector, esto es, qué competidores ya existen ofreciendo servicios en el mercado y cómo podría la nueva empresa de ciberseguridad diferenciarse de las opciones existentes, así como tratar de entender el comportamiento de los posibles clientes, el de los proveedores y que productos sustitutos y nuevos competidores.

Análisis FODA. El análisis FODA fue desarrollado en la sección 7 Marco teórico y conceptual del presente trabajo de forma predictiva, es decir es un FODA proyectado, ya que el FODA comúnmente se realiza para describir condiciones internas y externas de una organización, en las internas se describen las fortalezas y amenazas de la organización o individuo y en las externas las oportunidades y amenazas que podrían afectar a la organización, o bien aprovechar para tomar ventaja de los competidores. La intención de realizar un FODA proyectado se debe a que con antelación ya se conocen algunas de las condiciones con las cuales nacerá la nueva empresa y preciso describirlas para aprovechar condiciones y tomar posibles ventajas, así como tratar de minimizar el impacto de las condiciones desfavorables.

Business Model Canvas. Este modelo fue propuesto por Alexander Osterwalder para integrar en forma de plantilla, sobre la cual construir suposiciones e hipótesis. Dicha plantilla consta de 9 bloques para exponer la racionalidad detrás de cómo se pretende generar, entregar y capturar valor por la nueva empresa de servicios de ciberseguridad. Los nueve bloques que se describirán son:

1. Segmentos de clientes
2. Propuesta de valor
3. Canales de distribución
4. Relaciones con clientes
5. Flujos de ingresos
6. Recursos clave
7. Actividades clave
8. Relaciones clave
9. Estructura de costos

Este modelo fue utilizado en la sección 7 Marco teórico y conceptual para tratar de integrar precisamente como la nueva empresa de ciberseguridad entregará valor a sus clientes, así como, la forma en que cobrar por los servicios ofertados.

Plantilla de tamaño de mercado de Dynamic. Es una plantilla desarrollada por Dynamic en la cual pretende representar el tamaño de un mercado específico, calculando el tamaño total de mercado (TAM), el mercado disponible (SAM) y finalmente el mercado accesible (SOM). En el caso del presente trabajo se calculó el mercado total como el número total de Pymes en México, el mercado disponible como el número de Pymes establecidas en la zona metropolitana y el mercado accesible como un 10 % del total de Pymes en la zona metropolitana. Esta plantilla fue empleada en la sección 6 Marco teórico y conceptual precisamente para tratar de proyectar el tamaño de mercado disponible para la nueva empresa de ciberseguridad.

Matriz de riesgos. En la sección 10 Plan de implementación se plasmó en una matriz de riesgos asociados a la implantación de la nueva empresa, considerando un mapa de calor, responsables, tratamiento de cada riesgo, impacto y probabilidad de ocurrencia. Como sabemos un plan de negocios se trata de una serie de suposiciones y es importante también identificar aquellos riesgos que pudieran presentarse para tratar de minimizar su impacto o bien evitar que se materialicen. Es por ello que un riesgo es considerado aquello pudiera producir un contratiempo o afectar los objetivos de la nueva empresa.

9.1 Métodos de validación

Con el fin de validar la alternativa de solución elegida se proponen tres distintos métodos que ayudaran confirmar si se trata de una solución viable a implementar, las cuales son:

- Entrevista con expertos de la industria
- Entrevista con prospecto de cliente
- Validación y evaluación financiera

9.1.1 Entrevista con expertos de la industria

La entrevista con expertos de la industria de ciberseguridad tiene la finalidad de conocer su punto de vista con respecto a los esfuerzos en materia de ciberseguridad que están realizando las organizaciones, el número de ciberataques que han presenciado a lo largo de su carrera, oportunidades de mejora en la materia y finalmente si ellos identifican una oportunidad de mercado en ciberseguridad enfocado a pequeñas y medianas empresas de México.

La entrevista consta de una breve introducción y propósito de la entrevista, 13 preguntas abiertas para dialogar sin sesgos ni limitaciones y está planeada para una duración aproximada de 30 minutos totales, esto significa, 2 minutos y medio por pregunta. Se desea obtener de los entrevistados algunos datos demográficos para ayudar a entender desde su perspectiva las respuestas a las preguntas realizadas durante la entrevista.

Datos demográficos:

- Tiempo de experiencia en la industria
- Nombre del entrevistado
- Carga o puesto actual
- Edad
- Empresa en la que trabaja

Por su puesto lo más importante de la entrevista son las respuestas en materia de ciberseguridad a las siguientes preguntas:

1. ¿Qué tan importante consideras la ciberseguridad en las organizaciones de México?
2. ¿Quién o quienes crees que deberían preocuparse por la ciberseguridad?
3. ¿Desde tu perspectiva consideras que la ciberseguridad debería ser importante para las Pymes?
4. ¿Qué tipo de empresas son tus principales clientes?
5. ¿Qué características tienen estas empresas?
6. ¿Consideras que las empresas están haciendo los esfuerzos necesarios para proteger sus activos digitales?
7. ¿Te ha tocado atender y contener alguna vez un ciberataque?
8. ¿Qué tipo de ciberataques te ha tocado contener?
9. ¿Qué tipo de organizaciones consideras que son las más vulnerables ante un ciberataque?
10. ¿Consideras que las Pymes cuentan con las medidas necesarias en cuanto a protección de datos?
11. De acuerdo con tu experiencia ¿Cómo ves la tendencia y comportamiento de los ciberataques?
12. ¿Consideras que hace falta capacitación en ciberseguridad?
13. ¿Consideras que existe mercado de ciberseguridad para Pymes?

9.1.2 Entrevista con prospecto de cliente

Es importante conocer la perspectiva de expertos en la industria de ciberseguridad, y de igual forma es importante conocer la perspectiva de posibles clientes. La intención de entrevistar a dueños o personal con algún cargo importante en el departamento de tecnología de pequeños y medianos

negocios, es conocer qué tan importante es para su organización la ciberseguridad, así como identificar si la ciberseguridad se encuentra dentro de su agenda.
La entrevista consta de una breve introducción y propósito de la entrevista, 12 preguntas abiertas para dialogar sin sesgos ni limitaciones y está planeada para tener una duración aproximada de 30 minutos totales, esto significa, 2 minutos y medio por pregunta. Se desea obtener de los entrevistados algunos datos demográficos para ayudar a entender desde su perspectiva las respuestas a las preguntas realizadas durante la entrevista.

Datos demográficos:

- Nombre del entrevistado
- Puesto o cargo dentro de la organización
- Años en el puesto
- Número aproximado de empleados en la organización
- Número aproximado de equipos de computo
- Nombre de la organización
- Giro de la organización

La propuesta de preguntas a realizar durante la entrevista a prospecto de cliente son las siguientes:

1. ¿Has escuchado acerca de algún ciberataque en los últimos 3 meses?
2. ¿Tu organización ha sido víctima de algún ciberataque?
3. ¿Qué tan familiar te resulta el término de ciberseguridad?
4. ¿Qué tan familiarizado te consideras con los impactos de un ciberataque?
5. ¿Qué tan importante consideras los sistemas e información digital para la operación del negocio?
6. ¿Qué tanto consideras que tu organización se preocupa por la ciberseguridad?
7. ¿Consideras que tu organización hace lo necesario para proteger sus activos digitales?
8. ¿Tu organización cuenta con protocolos de cómo actuar ante un ciberataque?
9. ¿Cuentan con mecanismos de recuperación ante pérdida de información o interrupción de negocio?
10. ¿La organización cuenta con algún presupuesto para ciberseguridad y qué porcentaje aproximado?
11. ¿Considerarías contratar servicios de ciberseguridad para proteger tus activos digitales?
12. Por la naturaleza de sus operaciones, ¿Tienen la necesidad de cumplir con algún estándar de ciberseguridad?

9.1.3 Validación y evaluación financiera

La tercera propuesta de validación es en el aspecto financiero, es decir, determinar y estimar si las proyecciones de ventas podrían hacer este modelo de negocio atractivo a la inversión. Para esta validación se realizaron proyecciones de ventas a 3 años de los 5 servicios ofrecidos por la empresa de ciberseguridad, adicionalmente se evaluó la rentabilidad por medio del cálculo de los siguientes indicadores:

- Valor Presente Neto (VPN)
- Punto de equilibrio
- Tasa Interna de Retorno (TIR)

Valor Presente Neto (VPN). El valor presente neto consiste en traer del futuro al presente cantidades monetarias, cuando esto ocurre se dice que se utiliza una tasa de descuento, contrario a lo que ocurre cuando usamos una tasa de interés para llevar cantidades monetarias del presente al futuro, es por ello que a los flujos de efectivo trasladados al presente también se les llama flujos descontados. Para calcular la VPN se deben trasladar los flujos de años futuros al tiempo presente y restarle la inversión inicial, la cual ya se encuentra expresada en tiempo presente. Esto se calcula mediante la siguiente fórmula:

$$VPN = -P + \frac{FNE}{} + \frac{FNE}{} + \frac{FNE}{}$$

(1+i)^1 (1+i)^2 (1+i)^n

FNE= Flujo neto de efectivo del año n, o sea, la utilidad neta después de impuestos.
P= Inversión inicial en el año cero.
i= Tasa de referencia, o sea, la tasa mínima aceptable de rendimiento (TMAR)

Ahora veamos cómo interpretar el resultado del VPN para determinar si una inversión es atractiva o no, en función de la TMAR que cada inversionista define al momento de evaluar un proyecto de inversión, comúnmente esta tasa debería ser superior a la tasa de inflación más un premio al riesgo, por ejemplo, si la inflación se encuentra en 6% y se considera un premio al riesgo de 10 % la TMAR debería ser de 16%. Una vez aclarado esto, el VPN debe interpretarse de la siguiente forma:

Si VPN > 0, sería conveniente aceptar la inversión, ya que se ganaría más del rendimiento definido en la TMAR.
Si VPN < 0, se debería rechazar la inversión, ya que NO se ganaría el rendimiento mínimo aceptable.

Finalmente podemos decir acerca del VPN que mientras más que el inversionista imponga una TMAR mayor el VPN se reduce.

Punto de equilibrio. Se refiere al momento en que los ingresos de la empresa son iguales a los costos fijos y variables, es decir no se gana ni se pierde. El punto de equilibrio es importante tomar en cuenta para tener visibilidad de las ventas que se requieren para cubrir los gastos de la nueva empresa. Se calcula con la siguiente fórmula:

$$PEE = \frac{\text{Costos Fijos}}{1-\left(\frac{\text{Costos Variables}}{\text{Costos de Ventas}}\right)}$$

TIR (Tasa Interna de Retorno). La TIR es la tasa de descuento que hace el VPN = 0 y su interpretación se puede realizar de la siguiente forma:

Si TIR > ó = TMAR es recomendable aceptar la inversión.
Si TIR < TMAR NO sería recomendable aceptar la inversión.

La fórmula para obtener la TIR es la siguiente:

$$VPN=0=-P+\frac{FNE}{(1+i)^1}+\frac{FNE}{(1+i)^2}+\frac{FNE}{(1+i)^n}$$

Para esta validación financiera se definieron partidas presupuestales para cubrir los siguientes aspectos de la puesta en marcha y operación de la empresa de ciberseguridad:

- Inversión inicial
- Gastos administrativos
- Gastos de Mercadotecnia
- Gastos operativos

Inversión inicial. Este presupuesto está destinado a cubrir algunos gastos para arrancar el negocio, tal como son; equipo de cómputo y oficina, acondicionamiento de oficina, mobiliario y telefonía, esto significa que, muchos de estos gastos podrían ser por única ocasión o bien con un tiempo de vida a mediano plazo antes de volver a necesitarse.

Administrativo. Este presupuesto está enfocado a cubrir gastos recurrentes y legales de la creación de la nueva empresa. Algunos de los gastos que se encuentran en este presupuesto son; nómina,

trámites de constitución de la empresa, registro de marca, renta de oficina, mantenimientos y servicios como agua, luz, telefonía e internet.

Mercadotecnia. Dentro de este presupuesto encontramos gastos para cubrir la mezcla de mercadotecnia, es decir las 4 Ps que son publicidad, precio, promoción y plaza. Algunos de los costos que están considerados aquí son; diseño de logotipo, diseño de manual corporativo, dominio, sitio web, campañas publicitarias en redes sociales, tarjetas de presentación, volantes, etc.

Operativo. El presupuesto operativo tiene la finalidad de cubrir los gastos de operación del negocio, entre ellos podemos encontrar; licencias de software, gasolina, comisiones por ventas e insumos de oficina y limpieza.

William A. Sahlman dice en el artículo "Cómo confeccionar un excelente plan de negocio" que "*Todo inversor experimentado sabe que las proyecciones financieras detalladas para una nueva empresa son un acto de imaginación*" (Cómo confeccionar un excelente plan de negocio, 1997, pág. 31.), es decir, que se dedica demasiado tiempo y tinta a este rubro y muy poco tiempo a lo que verdaderamente interesa que son preguntas clave relacionadas con factores críticos para el éxito de la nueva empresa, los cuales son; la gente, la oportunidad, el contexto, y el riesgo y recompensa. Esto tiene mucho sentido y así debe respetarse, sin embargo, sí es importante y necesario realizar al menos, algunas proyecciones financieras para tratar de anticipar en qué costos se va a incurrir y qué riesgos pudieran surgir, es por ello que el análisis financiero considera estos cuatro presupuestos y por supuesto, se parte de algunos **supuestos** los se detallarán en una sección más adelante, pero por lo pronto, es importante tener claro que esos supuestos están basados en algunas suposiciones, tal como Sahlman indica, son un acto de imaginación, o sea que aún no suceden y no se tiene la certeza de que ocurran de esa forma, pero sí es importante tener un estimado que nos permitirá reducir el riesgo financiero.

9.2 Solución final aplicada al problema

La solución propuesta para ayudar a mitigar el problema planteado de los pequeños y medianos negocios en materia de ciberdelincuencia, es crear una Pyme que ofrecerá inicialmente 5 servicios de ciberseguridad enfocados en tratar de aliviar algunos de los principales *pains* de los clientes, los cuales hemos visto anteriormente y quedaron plasmados de mejor manera en la Tabla 5. Ciberataques atendidos por propuesta de servicios en ciberseguridad, donde podemos ver cada uno de los 5 servicios y qué *pain* tratan de contrarrestar, es por eso que me permito recuperar dicha tabla para clarificar de mejor manera como la solución trata de atacar el problema inicial.

Tabla 8. Ciberataques atendidos por propuesta de servicios en ciberseguridad

Servicio a ofrecer	Tipo de ciberataque			
	Ransomware	Phishing	Spyware	Ingeniería social
Diagnóstico de nivel de madurez en ciberseguridad				●
Implementación de consola de antivirus y *endpoint*	●	●	●	
Gestión de consola de antivirus y *endpoint*	●	●	●	
Capacitación en ciberseguridad	●	●	●	●
Consultoría en implementación y cumplimiento de estándares de seguridad	●	●	●	●

(Elaboración propia, 2022)

Cada uno de los ciberataques listados en la tabla forman parte del problema planteado, ya que ocurren constantemente y muchas de las pequeñas y medianas empresas no cuentan con conocimiento ni mecanismos para contrarrestarlos y en muchas ocasiones ya fueron atacadas o bien tienen intrusos dentro de su red y no lo saben, es por eso que la nueva empresa de servicios de ciberseguridad tiene como objetivo ayudar a dichas organizaciones a revertir esta situación.

10. Proceso de validación y aplicación de propuesta en el caso

Tal como se describió en la sección 9.1 Métodos de validación, se realizaron entrevistas con expertos de la industria de ciberseguridad, así como posibles clientes para tratar de entender ambas perspectivas e identificar o ratificar necesidades y/o *pains* actuales de las organizaciones.

Los métodos de validación propuestos fueron los siguientes:

- Entrevista con expertos de la industria
- Entrevista con prospecto de cliente de servicios de ciberseguridad
- Validación y evaluación financiera

10.1 Entrevistas con expertos

Se realizaron entrevistas con tres expertos de diferentes organizaciones, por un lado un experto con un perfil académico (ver Anexo 3), que nos ayudará a ver la situación desde una perspectiva teórica y regulatoria para tratar de entender desde las bases como es la situación actual y cuál podría ser la tendencia hacia adelante. (M. López, comunicación personal, 8 de noviembre del 2022).

La segunda entrevista es con un perfil de implementador de la tecnología de ciberseguridad y atención directa a grandes empresas que realizan inversiones grandes en ciberseguridad. Ha trabajado para grandes y medianos bancos de México, por lo cual tiene una idea muy clara del contraste que existe en cuanto a esfuerzos por cumplir con estándares y protección de la información entre ambos, consultar el anexo 1 para ver la entrevista completa (A. Dominguez, comunicación personal, 2 de noviembre del 2022).

La tercera entrevista es un perfil de gerente y líder de equipo de trabajo de monitoreo y vigilancia de actividades irregulares como extracción de información de la organización, es decir monitoreo constante desde dentro de la organización, cuidando que ningún usuario interno extraiga información en medios de almacenamiento o vía internet hacia cuentas externas, ya que como hemos visto anteriormente, gran parte de los ciberataques y fuga de información ocurren desde el interior, ya sea por descuidos o conductas deliberadas de personal interno, llamados amenazas internas en la sección de antecedentes (E. Ortega, comunicación personal, 7 de noviembre del 2022).

Recomendaciones y conclusiones de las entrevistas con expertos.

De acuerdo con las opiniones y comentarios de los expertos se identifica los siguientes puntos:

- Los 3 expertos aún con perfiles distintos coinciden en que sí podría existir mercado para servicios de ciberseguridad para Pymes en México.
- Los ciberataques serán cada vez más sofisticados y frecuentes.
- El ciberespacio es cada vez más extenso y por lo mismo mayor oportunidad de ciberataques.
- Los servicios de capacitación deberían ser el primer paso en el camino de la ciberseguridad.
- Se necesita mayor sensibilización, educación y conciencia en ciberseguridad en todos los ámbitos.
- Organizaciones públicas y privadas, personas, familias, en otras palabras, todos deberían de preocuparse por la ciberseguridad.

- No necesariamente se requieren grandes inversiones para empezar a aplicar prácticas de ciberseguridad.
- Adquirir e implementar soluciones tecnológicas enfocadas a ciberseguridad no es suficiente, se requiere un mantenimiento y monitoreo constante.
- Los ciberataques van más rápido que la ciberseguridad.
- No solo las organizaciones deberían preocuparse por la ciberseguridad, sino todos, familias, casas, personas, escuelas, etc.
- Las organizaciones financieras son las más adelantadas en cuanto a protección de la información y cumplimiento de estándares y regulaciones, las demás industrias deberían hacer lo mismo.

10.2 Entrevistas con prospecto de cliente

Las entrevistas con prospectos de clientes se realizaron con la intención de conocer más acerca de la situación actual por la cual están pasando en materia de ciberseguridad y tecnología, donde se realizaron 2 entrevistas a dos distintos tipos de organizaciones que cumplen con las características definidas para el mercado objetivo, es decir Pymes con procesos digitales y al menos 25 dispositivos con accesos a sistemas e información de la organización.

La primera organización se dedica a comercializar productos médicos dentales y el encargado de infraestructura (J. Del Rel, comunicación personal, 4 de noviembre del 2022). Tiene mucha noción de la materia, sin embargo, reconoce que los esfuerzos por proteger los sistemas y activos digitales pueden ser mayores y hace falta un diagnóstico más a profundidad, la entrevista completa se puede consultar en el anexo 4.

La segunda organización se dedica a comercializar medicamentos y fórmulas lácteas donde el gerente comercial es responsable de los sistemas (J. Teacalco, comunicación personal, 5 de noviembre del 2022). Reconoce que existe poca noción y conciencia sobre ciberseguridad en su organización y que no cuentan con protocolos de recuperación y prácticamente no cuentan con mecanismos de ciberseguridad (ver anexo 5).

Recomendaciones y conclusiones de las entrevistas con prospectos de cliente.

De acuerdo con las opiniones y comentarios de los posibles clientes o usuarios de los servicios de ciberseguridad se identifica los siguientes puntos:

- Se identifica que sí se tiene la intención de invertir más en ciberseguridad, no solo económicamente, sino generar conciencia de su importancia en la organización.
- Se reconoce que existe área de oportunidad en cuanto protocolos de recuperación, contención de ciberataque y de protección de información.
- En ambos casos, los sistemas y procesos digitales son relevantes para la operación del negocio y muy probablemente esta condición se podría replicar a otros negocios.
- El acceso a los sistemas e información digital cada vez es más descentralizada, es decir los datos no solo se consumen desde un único punto que podría ser la oficina, sino que desde dispositivos móviles y lugares remotos se accede a la información.
- Se reconoce que existe una oportunidad de mejora en cuanto a educación y prácticas en ciberseguridad.
- Se tenía el paradigma de que con invertir económicamente en tecnología era suficiente.
- Se tenía el paradigma que la ciberseguridad solo compete al área de TI.

10.3 Validación y evaluación financiera

Con base en el catálogo de servicios se definieron los siguientes precios:

Figura 14. Lista de precios de los primeros 3 años

Precios por año	Precio año 1	Precio año 2	Precio año 3
Diagnóstico de nivel de madurez en ciberseguridad	$ 6,000.00	$ 6,300.00	$ 6,615.00
Implementación de consola de antivirus y endpoint	$ 500.00	$ 525.00	$ 551.25
Gestión de consola de antivirus y endpoint	$ 650.00	$ 682.50	$ 716.63
Capacitación en ciberseguridad	$ 7,500.00	$ 7,875.00	$ 8,268.75
Consultoría en implementación y cumplimiento de estándares	$40,000.00	$42,000.00	$ 44,100.00

(Elaboración propia, 2022)

El precio del diagnóstico de madurez en ciberseguridad está basado en el tiempo que toma elaborarlo, ejecutarlo, analizarlo y presentarlo, es decir, el tiempo que emplea un ingeniero o consultor para realizar todas estas acciones. Considerando esto sería $288.00 aproximadamente la hora y consumiendo 2 días de trabajo con jornada de 8 horas.

El precio de la implementación de consola de antivirus y *endpoint* está basado en el precio de lista de una licencia de antivirus, específicamente de Trend Micro. Este servicio no es un cargo recurrente ya que ocurre una vez y podría complementarse con el servicio de gestión de consola de antivirus y *endpoint* para contar con el servicio completo y volverlo recurrente, ya que este servicio sí sería un cargo recurrente por dispositivo conectado, el cual también incluye la licencia de antivirus.

El precio de la capacitación en ciberseguridad está basado en un grupo de 1 a 8 personas, o sea el precio por persona sería de $927.00 por persona.

Finalmente el servicio de consultoría en implementación y cumplimiento de estándares de seguridad es un servicio que toma más tiempo ejecutar debido a que se debe comprender los procesos y tecnología actual para diseñar un plan de implementación, así como explicar y acompañar a los clientes a cumplir las nuevas políticas de seguridad de la información.

Figura 15. Frecuencia de ventas de los primeros 3 años

Horas de servicio	1er. Sem.	2do. Sem.	3er. Sem.	4to. Sem.	5to. Sem.	6to. Sem.
Servicios al mes	15	17	19	21	23	25
Implementaciones al mes	50	100	150	200	250	300
Administración de host al mes	25	25	25	25	25	25
Capacitaciones al mes	4	6	8	10	12	14
Consultorías al mes	2	3	4	5	6	7

(Elaboración propia, 2022)

La figura 15 muestra la frecuencia de uso de cada servicio, en las columnas tenemos los 3 primeros años divididos por semestres. Estas columnas muestran cuantos servicios se pronostican vender al mes durante los primeros 6 meses de operación. Por ejemplo, para el caso del servicio de diagnóstico de nivel de madurez en ciberseguridad se pronostican entregar 15 al mes durante los primeros 6 meses y para el segundo semestre incrementar la demanda en 2, es decir, 17 servicios al mes. Esto aplicaría para el resto de los servicios.

10.3.1 Pronóstico de ventas

Figura 16. Pronóstico de ventas del primer año

Año 2023	Uds.	Enero	Uds.	Febrero	Uds.	Marzo	Uds.	Abril	Uds.	Mayo	Uds.	Junio	Uds.	Julio	Uds.	Agosto	Uds.	Septiembre	Uds.	Octubre	Uds.	Noviembre	Uds.	Diciembre	Total
Diagnóstico de nivel de madurez en ciberseguridad	0	-	15	90,000.00	15	90,000.00	15	90,000.00	15	90,000.00	15	90,000.00	17	102,000.00	17	102,000.00	17	102,000.00	17	102,000.00	17	102,000.00	17	102,000.00	1,062,000.00
Implementación de consola de antivirus y endpoint	0	-	50	25,000.00	50	25,000.00	50	25,000.00	50	25,000.00	50	25,000.00	100	50,000.00	100	50,000.00	100	50,000.00	100	50,000.00	100	50,000.00	100	50,000.00	425,000.00
Gestión de consola de antivirus y endpoint	0	-	25	16,250.00	25	16,250.00	25	16,250.00	25	16,250.00	25	16,250.00	25	16,250.00	25	16,250.00	25	16,250.00	25	16,250.00	25	16,250.00	25	16,250.00	178,750.00
Capacitación en ciberseguridad	0	-	4	30,000.00	4	30,000.00	4	30,000.00	4	30,000.00	4	30,000.00	6	45,000.00	6	45,000.00	6	45,000.00	6	45,000.00	6	45,000.00	6	45,000.00	420,000.00
Consultoría en implementación y cumplimiento de estándares	0	-	2	80,000.00	2	80,000.00	2	80,000.00	2	80,000.00	2	80,000.00	3	120,000.00	3	120,000.00	3	120,000.00	3	120,000.00	3	120,000.00	3	120,000.00	1,120,000.00
Total		**-**		**241,250.00**		**241,250.00**		**241,250.00**		**241,250.00**		**241,250.00**		**333,250.00**		**333,250.00**		**333,250.00**		**333,250.00**		**333,250.00**		**333,250.00**	**3,205,750.00**

(Elaboración propia, 2022)

Figura 17. Pronóstico de ventas del segundo año

Año 2024	Uds.	Enero	Uds.	Febrero	Uds.	Marzo	Uds.	Abril	Uds.	Mayo	Uds.	Junio	Uds.	Julio	Uds.	Agosto	Uds.	Septiembre	Uds.	Octubre	Uds.	Noviembre	Uds.	Diciembre	Total
Diagnóstico de nivel de madurez en ciberseguridad	19	119,700.00	19	119,700.00	19	119,700.00	19	119,700.00	19	119,700.00	19	119,700.00	21	132,300.00	21	132,300.00	21	132,300.00	21	132,300.00	21	132,300.00	21	132,300.00	1,512,000.00
Implementación de consola de antivirus y endpoint	150	78,750.00	150	78,750.00	150	78,750.00	150	78,750.00	150	78,750.00	150	78,750.00	200	105,000.00	200	105,000.00	200	105,000.00	200	105,000.00	200	105,000.00	200	105,000.00	1,102,500.00
Gestión de consola de antivirus y endpoint	25	17,062.50	25	17,062.50	25	17,062.50	25	17,062.50	25	17,062.50	25	17,062.50	25	17,062.50	25	17,062.50	25	17,062.50	25	17,062.50	25	17,062.50	25	17,062.50	204,750.00
Capacitación en ciberseguridad	8	63,000.00	8	63,000.00	8	63,000.00	8	63,000.00	8	63,000.00	8	63,000.00	10	78,750.00	10	78,750.00	10	78,750.00	10	78,750.00	10	78,750.00	10	78,750.00	850,500.00
Consultoría en implementación y cumplimiento de estándares	4	168,000.00	4	168,000.00	4	168,000.00	4	168,000.00	4	168,000.00	4	168,000.00	5	210,000.00	5	210,000.00	5	210,000.00	5	210,000.00	5	210,000.00	5	210,000.00	2,268,000.00
Total		**446,512.50**		**446,512.50**		**446,512.50**		**446,512.50**		**446,512.50**		**446,512.50**		**543,112.50**		**543,112.50**		**543,112.50**		**543,112.50**		**543,112.50**		**543,112.50**	**5,937,750.00**

(Elaboración propia, 2022)

Figura 18. Pronóstico de ventas del tercer año

Año 2025	Uds.	Enero	Uds.	Febrero	Uds.	Marzo	Uds.	Abril	Uds.	Mayo	Uds.	Junio	Uds.	Julio	Uds.	Agosto	Uds.	Septiembre	Uds.	Octubre	Uds.	Noviembre	Uds.	Diciembre	Total
Diagnóstico de nivel de madurez en ciberseguridad	23	152,145.00	23	152,145.00	23	152,145.00	23	152,145.00	23	152,145.00	23	152,145.00	25	165,375.00	25	165,375.00	25	165,375.00	25	165,375.00	25	165,375.00	25	165,375.00	1,905,120.00
Implementación de consola de antivirus y endpoint	250	137,812.50	250	137,812.50	250	137,812.50	250	137,812.50	250	137,812.50	250	137,812.50	300	165,375.00	300	165,375.00	300	165,375.00	300	165,375.00	300	165,375.00	300	165,375.00	1,819,125.00
Gestión de consola de antivirus y endpoint	25	17,915.63	25	17,915.63	25	17,915.63	25	17,915.63	25	17,915.63	25	17,915.63	25	17,915.63	25	17,915.63	25	17,915.63	25	17,915.63	25	17,915.63	25	17,915.63	214,987.50
Capacitación en ciberseguridad	12	99,225.00	12	99,225.00	12	99,225.00	12	99,225.00	12	99,225.00	12	99,225.00	14	115,762.50	14	115,762.50	14	115,762.50	14	115,762.50	14	115,762.50	14	115,762.50	1,289,925.00
Consultoría en implementación y cumplimiento de estándares	6	264,600.00	6	264,600.00	6	264,600.00	6	264,600.00	6	264,600.00	6	264,600.00	7	308,700.00	7	308,700.00	7	308,700.00	7	308,700.00	7	308,700.00	7	308,700.00	3,439,800.00
Total		**671,698.13**		**671,698.13**		**671,698.13**		**671,698.13**		**671,698.13**		**671,698.13**		**773,128.13**		**773,128.13**		**773,128.13**		**773,128.13**		**773,128.13**		**773,128.13**	**8,668,957.50**

(Elaboración propia, 2022)

Supuestos del pronóstico de ventas:

1. El precio del servicio de diagnóstico aumentará un 5% cada año
2. El pronóstico de venta está basado en un escenario optimista
3. Se considera que las Pymes tienen en promedio 25 equipos de computo
4. Con base en el supuesto 3 se considera 2 clientes el primer mes para el servicio de implementación de antivirus y posterior se incrementa cada semestre 1 cliente más al mes
5. Con base en el supuesto 3 se considera un incremento de un cliente por mes cada semestre para administración de antivirus
6. Se considera un incremento de 2 unidades al semestre en la venta mensual para el servicio de diagnóstico

7. Se considera un incremento de 2 unidades de venta al semestre en la venta mensual para el servicio de capacitación
8. Se considera un incremento de 1 unidad de venta al semestre en la venta mensual para el servicio de consultoría en estándares de seguridad
9. Se consideran 26 días laborales al mes
10. No se consideran ventas el primer mes de operación

10.3.2 Inversión inicial y depreciaciones

Figura 19. Presupuesto de inversión inicial

Equipo de oficina	Unidades	Precio	Total
Escritorios	7	8,000.00	56,000.00
Sillas	7	4,000.00	28,000.00
Cajoneras	3	5,000.00	15,000.00
Sala de juntas	1	15,000.00	15,000.00
Sillas de sala de juntas	6	5,000.00	30,000.00
Sala de espera	1	15,000.00	15,000.00
Total			**159,000.00**

Equipos de cómputo y general	Unidades	Precio	Total
Laptop Lenovo ideaPad 3i	7	15,000.00	105,000.00
Impresora Multifuncional HP Smart Tank 615	1	5,999.00	5,999.00
Racks	2	3,000.00	6,000.00
Telefono fijo	1	1,000.00	1,000.00
Telefono celular	7	6,000.00	42,000.00
Pantalla sala de juntas	1	15,000.00	15,000.00
Camaras de seguridad	2	2,000.00	4,000.00
Extintor	2	700.00	1,400.00
Refrigerador	1	10,000.00	10,000.00
Horno de microndas	1	2,000.00	2,000.00
Dispensador de agua	1	2,000.00	2,000.00
Botes de basura	5	1,000.00	5,000.00
Monitores 27"	5	3,500.00	17,500.00
Terminal de pago	1	1,000.00	1,000.00
Total			**217,899.00**

Acondicionamiento local	Unidades	Precio	Total
Remodelaciones	1	60,000.00	60,000.00
Total			**60,000.00**
Varios (8%)			34,951.92
Total presupuesto inicial			**471,850.92**
Activo			**376,899.00**
Capital social			**1,200,000.00**

(Elaboración propia, 2022)

Figura 20. Depreciaciones de los tres primeros años

Depreciación de equipo de oficina																
Anual	1	2	3	4	5	6	7	8	9	10	11	12	Año 1	Año 2	Año 3
11,200.00	933.33	933.33	933.33	933.33	933.33	933.33	933.33	933.33	933.33	933.33	933.33	933.33	11,200.00	11,200.00	11,200.00
5,600.00	466.67	466.67	466.67	466.67	466.67	466.67	466.67	466.67	466.67	466.67	466.67	466.67	5,600.00	5,600.00	5,600.00
3,000.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	3,000.00	3,000.00	3,000.00
3,000.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	3,000.00	3,000.00	3,000.00
6,000.00	500.00	500.00	500.00	500.00	500.00	500.00	500.00	500.00	500.00	500.00	500.00	500.00	6,000.00	6,000.00	6,000.00
3,000.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	3,000.00	3,000.00	3,000.00
31,800.00	2,650.00	2,650.00	2,650.00	2,650.00	2,650.00	2,650.00	2,650.00	2,650.00	2,650.00	2,650.00	2,650.00	2,650.00	31,800.00	31,800.00	31,800.00
Depreciación de equipo de cómputo y general																
Anual	1	2	3	4	5	6	7	8	9	10	11	12	Año 1	Año 2	Año 3
21,000.00	1,750.00	1,750.00	1,750.00	1,750.00	1,750.00	1,750.00	1,750.00	1,750.00	1,750.00	1,750.00	1,750.00	1,750.00	21,000.00	21,000.00	21,000.00
1,199.80	99.98	99.98	99.98	99.98	99.98	99.98	99.98	99.98	99.98	99.98	99.98	99.98	1,199.80	1,199.80	1,199.80
1,200.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	1,200.00	1,200.00	1,200.00
200.00	16.67	16.67	16.67	16.67	16.67	16.67	16.67	16.67	16.67	16.67	16.67	16.67	200.00	200.00	200.00
8,400.00	700.00	700.00	700.00	700.00	700.00	700.00	700.00	700.00	700.00	700.00	700.00	700.00	8,400.00	8,400.00	8,400.00
3,000.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	250.00	3,000.00	3,000.00	3,000.00
800.00	66.67	66.67	66.67	66.67	66.67	66.67	66.67	66.67	66.67	66.67	66.67	66.67	800.00	800.00	800.00
280.00	23.33	23.33	23.33	23.33	23.33	23.33	23.33	23.33	23.33	23.33	23.33	23.33	280.00	280.00	280.00
2,000.00	166.67	166.67	166.67	166.67	166.67	166.67	166.67	166.67	166.67	166.67	166.67	166.67	2,000.00	2,000.00	2,000.00
400.00	33.33	33.33	33.33	33.33	33.33	33.33	33.33	33.33	33.33	33.33	33.33	33.33	400.00	400.00	400.00
400.00	33.33	33.33	33.33	33.33	33.33	33.33	33.33	33.33	33.33	33.33	33.33	33.33	400.00	400.00	400.00
1,000.00	83.33	83.33	83.33	83.33	83.33	83.33	83.33	83.33	83.33	83.33	83.33	83.33	1,000.00	1,000.00	1,000.00
3,500.00	291.67	291.67	291.67	291.67	291.67	291.67	291.67	291.67	291.67	291.67	291.67	291.67	3,500.00	3,500.00	3,500.00
200.00	16.67	16.67	16.67	16.67	16.67	16.67	16.67	16.67	16.67	16.67	16.67	16.67	200.00	200.00	200.00
43,579.80	3,631.65	3,631.65	3,631.65	3,631.65	3,631.65	3,631.65	3,631.65	3,631.65	3,631.65	3,631.65	3,631.65	3,631.65	43,579.80	43,579.80	43,579.80
75,379.80	**6,281.65**	**6,281.65**	**6,281.65**	**6,281.65**	**6,281.65**	**6,281.65**	**6,281.65**	**6,281.65**	**6,281.65**	**6,281.65**	**6,281.65**	**6,281.65**	**75,379.80**	**75,379.80**	**75,379.80**

(Elaboración propia, 2022)

Supuestos de la inversión inicial y depreciaciones:

1. Los muebles de oficina y equipo de cómputo tendrán una depreciación del 20% anual por 5 años
2. Los equipos de cómputo y de oficina serán pagados de contado
3. Se consideran $ 1,200,00.00 como capital social, o sea $ 600,000.00 por cada socio
4. Se considera un 8% para gastos diversos o imprevistos

10.3.3 Presupuesto administrativo

Figura 21. Presupuesto administrativo del primer año

AÑO 1 Costos fijos	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	Total
Renta oficina	25,000.00	25,000.00	25,000.00	25,000.00	25,000.00	25,000.00	25,000.00	25,000.00	25,000.00	25,000.00	25,000.00	25,000.00	300,000.00
Luz	800.00	500.00	500.00	500.00	500.00	500.00	500.00	500.00	500.00	500.00	500.00	500.00	6,300.00
Agua	350.00	350.00	350.00	350.00	350.00	350.00	350.00	350.00	350.00	350.00	350.00	350.00	4,200.00
Telefono e internet	540.00	540.00	540.00	540.00	540.00	540.00	540.00	540.00	540.00	540.00	540.00	540.00	6,480.00
Agua potable	600.00	600.00	600.00	600.00	600.00	600.00	600.00	600.00	600.00	600.00	600.00	600.00	7,200.00
Telefonía movil	3,500.00	3,500.00	3,500.00	3,500.00	3,500.00	3,500.00	3,500.00	3,500.00	3,500.00	3,500.00	3,500.00	3,500.00	42,000.00
Capacitación y cursos	180,000.00												180,000.00
Mantenimiento/limpieza instalaciones	6,000.00	6,000.00	6,000.00	6,000.00	6,000.00	6,000.00	6,000.00	6,000.00	6,000.00	6,000.00	6,000.00	6,000.00	$ 72,000.00
Subtotal de costos fijos	**216,790.00**	**36,490.00**	**36,490.00**	**36,490.00**	**36,490.00**	**36,490.00**	**36,490.00**	**36,490.00**	**36,490.00**	**36,490.00**	**36,490.00**	**36,490.00**	**618,180.00**
Legal	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Acta consititutiva de empresa	25,000.00												25,000.00
Registro de marca	2,500.00												2,500.00
Gastos administrativos (contador)	2,500.00	2,500.00	2,500.00	2,500.00	2,500.00	2,500.00	2,500.00	2,500.00	2,500.00	2,500.00	2,500.00	2,500.00	30,000.00
Subtotal de costos fijos	**30,000.00**	**2,500.00**	**2,500.00**	**2,500.00**	**2,500.00**	**2,500.00**	**2,500.00**	**2,500.00**	**2,500.00**	**2,500.00**	**2,500.00**	**2,500.00**	**57,500.00**
Sueldos (RH)	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Vendedor 1	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	264,000.00
Vendedor 2	-	-	-	-	-	-	-	-	-	-	-	-	-
Implementador/Capacitador 1	30,000.00	30,000.00	30,000.00	30,000.00	30,000.00	30,000.00	30,000.00	30,000.00	30,000.00	30,000.00	30,000.00	30,000.00	360,000.00
Implementador/Capacitador 2	30,000.00	30,000.00	30,000.00	30,000.00	30,000.00	30,000.00	30,000.00	30,000.00	30,000.00	30,000.00	30,000.00	30,000.00	360,000.00
Implementador/Capacitador 3	-	-	-	-	-	-	-	-	-	-	-	-	-
Gerente 1 (Socio 1)	35,000.00	35,000.00	35,000.00	35,000.00	35,000.00	35,000.00	35,000.00	35,000.00	35,000.00	35,000.00	35,000.00	35,000.00	420,000.00
Gerente 1 (Socio 2)	35,000.00	35,000.00	35,000.00	35,000.00	35,000.00	35,000.00	35,000.00	35,000.00	35,000.00	35,000.00	35,000.00	35,000.00	420,000.00
Subtotal de Sueldos	**152,000.00**	**152,000.00**	**152,000.00**	**152,000.00**	**152,000.00**	**152,000.00**	**152,000.00**	**152,000.00**	**152,000.00**	**152,000.00**	**152,000.00**	**152,000.00**	**1,824,000.00**
Carga Social (22%)	33,440.00	33,440.00	33,440.00	33,440.00	33,440.00	33,440.00	33,440.00	33,440.00	33,440.00	33,440.00	33,440.00	33,440.00	401,280.00
Aguinaldo (25%)	-	-	-	-	-	-	-	-	-	-	-	38,000.00	38,000.00
Total de Sueldos	**185,440.00**	**185,440.00**	**185,440.00**	**185,440.00**	**185,440.00**	**185,440.00**	**185,440.00**	**185,440.00**	**185,440.00**	**185,440.00**	**185,440.00**	**223,440.00**	**2,263,280.00**
Varios (8%)	14,835.20	14,835.20	14,835.20	14,835.20	14,835.20	14,835.20	14,835.20	14,835.20	14,835.20	14,835.20	14,835.20	17,875.20	181,062.40
Total Final	**447,065.20**	**239,265.20**	**239,265.20**	**239,265.20**	**239,265.20**	**239,265.20**	**239,265.20**	**239,265.20**	**239,265.20**	**239,265.20**	**239,265.20**	**280,305.20**	**3,120,022.40**

(Elaboración propia, 2022)

Figura 22. Presupuesto administrativo del segundo año

AÑO 2													
Costos fijos	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Renta oficina	26,250.00	26,250.00	26,250.00	26,250.00	26,250.00	26,250.00	26,250.00	26,250.00	26,250.00	26,250.00	26,250.00	26,250.00	315,000.00
Luz	840.00	840.00	840.00	840.00	840.00	840.00	840.00	840.00	840.00	840.00	840.00	840.00	10,080.00
Agua	367.50	367.50	367.50	367.50	367.50	367.50	367.50	367.50	367.50	367.50	367.50	367.50	4,410.00
Telefono e internet	567.00	567.00	567.00	567.00	567.00	567.00	567.00	567.00	567.00	567.00	567.00	567.00	6,804.00
Agua potable	630.00	630.00	630.00	630.00	630.00	630.00	630.00	630.00	630.00	630.00	630.00	630.00	7,560.00
Telefonía movil	3,675.00	3,675.00	3,675.00	3,675.00	3,675.00	3,675.00	3,675.00	3,675.00	3,675.00	3,675.00	3,675.00	3,675.00	44,100.00
Capacitación y cursos	189,000.00												189,000.00
Mantenimiento/limpieza instalaciones	6,300.00	6,300.00	6,300.00	6,300.00	6,300.00	6,300.00	6,300.00	6,300.00	6,300.00	6,300.00	6,300.00	6,300.00	$ 75,600.00
Subtotal de costos fijos	**227,629.50**	**38,629.50**	**38,629.50**	**38,629.50**	**38,629.50**	**38,629.50**	**38,629.50**	**38,629.50**	**38,629.50**	**38,629.50**	**38,629.50**	**38,629.50**	**652,554.00**
Sueldos (RH)	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Vendedor 1	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	264,000.00
Vendedor 2	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	264,000.00
Implementador/Capacitador 1	31,800.00	31,800.00	31,800.00	31,800.00	31,800.00	31,800.00	31,800.00	31,800.00	31,800.00	31,800.00	31,800.00	31,800.00	381,600.00
Implementador/Capacitador 2	31,800.00	31,800.00	31,800.00	31,800.00	31,800.00	31,800.00	31,800.00	31,800.00	31,800.00	31,800.00	31,800.00	31,800.00	381,600.00
Implementador/Capacitador 3	-	-	-	-	-	-	-	-	-	-	-	-	-
Gerente 1 (Socio 1)	37,100.00	37,100.00	37,100.00	37,100.00	37,100.00	37,100.00	37,100.00	37,100.00	37,100.00	37,100.00	37,100.00	37,100.00	445,200.00
Gerente 1 (Socio 2)	37,100.00	37,100.00	37,100.00	37,100.00	37,100.00	37,100.00	37,100.00	37,100.00	37,100.00	37,100.00	37,100.00	37,100.00	445,200.00
Subtotal de Sueldos	**181,800.00**	**181,800.00**	**181,800.00**	**181,800.00**	**181,800.00**	**181,800.00**	**181,800.00**	**181,800.00**	**181,800.00**	**181,800.00**	**181,800.00**	**181,800.00**	**2,181,600.00**
Carga Social (22%)	39,996.00	39,996.00	39,996.00	39,996.00	39,996.00	39,996.00	39,996.00	39,996.00	39,996.00	39,996.00	39,996.00	39,996.00	479,952.00
Aguinaldo (25%)	-	-	-	-	-	-	-	-	-	-	-	45,450.00	45,450.00
Total de Sueldos	**221,796.00**	**221,796.00**	**221,796.00**	**221,796.00**	**221,796.00**	**221,796.00**	**221,796.00**	**221,796.00**	**221,796.00**	**221,796.00**	**221,796.00**	**267,246.00**	**2,707,002.00**
Varios (8%)	17,743.68	17,743.68	17,743.68	17,743.68	17,743.68	17,743.68	17,743.68	17,743.68	17,743.68	17,743.68	17,743.68	21,379.68	216,560.16
Total Final	**467,169.18**	**278,169.18**	**278,169.18**	**278,169.18**	**278,169.18**	**278,169.18**	**278,169.18**	**278,169.18**	**278,169.18**	**278,169.18**	**278,169.18**	**327,255.18**	**3,576,116.16**

(Elaboración propia, 2022)

Figura 23. Presupuesto administrativo del tercer año

AÑO 3													
Costos fijos	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Renta oficina	27,562.50	27,562.50	27,562.50	27,562.50	27,562.50	27,562.50	27,562.50	27,562.50	27,562.50	27,562.50	27,562.50	27,562.50	330,750.00
Luz	882.00	882.00	882.00	882.00	882.00	882.00	882.00	882.00	882.00	882.00	882.00	882.00	10,584.00
Agua	385.88	385.88	385.88	385.88	385.88	385.88	385.88	385.88	385.88	385.88	385.88	385.88	4,630.50
Telefono e internet	595.35	595.35	595.35	595.35	595.35	595.35	595.35	595.35	595.35	595.35	595.35	595.35	7,144.20
Agua potable	661.50	661.50	661.50	661.50	661.50	661.50	661.50	661.50	661.50	661.50	661.50	661.50	7,938.00
Telefonía movil	3,858.75	3,858.75	3,858.75	3,858.75	3,858.75	3,858.75	3,858.75	3,858.75	3,858.75	3,858.75	3,858.75	3,858.75	46,305.00
Capacitación y cursos	198,450.00												198,450.00
Mantenimiento/limpieza instalaciones	6,615.00	6,615.00	6,615.00	6,615.00	6,615.00	6,615.00	6,615.00	6,615.00	6,615.00	6,615.00	6,615.00	6,615.00	$ 79,380.00
Subtotal de costos fijos	**239,010.98**	**40,560.98**	**40,560.98**	**40,560.98**	**40,560.98**	**40,560.98**	**40,560.98**	**40,560.98**	**40,560.98**	**40,560.98**	**40,560.98**	**40,560.98**	**685,181.70**
Sueldos	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Vendedor 1	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	264,000.00
Vendedor 2	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	22,000.00	264,000.00
Implementador/Capacitador 1	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	404,496.00
Implementador/Capacitador 2	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	404,496.00
Implementador/Capacitador 3	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	33,708.00	404,496.00
Gerente 1 (Socio 1)	39,326.00	39,326.00	39,326.00	39,326.00	39,326.00	39,326.00	39,326.00	39,326.00	39,326.00	39,326.00	39,326.00	39,326.00	471,912.00
Gerente 1 (Socio 2)	39,326.00	39,326.00	39,326.00	39,326.00	39,326.00	39,326.00	39,326.00	39,326.00	39,326.00	39,326.00	39,326.00	39,326.00	471,912.00
Subtotal de Sueldos	**223,776.00**	**223,776.00**	**223,776.00**	**223,776.00**	**223,776.00**	**223,776.00**	**223,776.00**	**223,776.00**	**223,776.00**	**223,776.00**	**223,776.00**	**223,776.00**	**2,685,312.00**
Carga Social (22%)	49,230.72	49,230.72	49,230.72	49,230.72	49,230.72	49,230.72	49,230.72	49,230.72	49,230.72	49,230.72	49,230.72	49,230.72	590,768.64
Aguinaldo (25%)	-	-	-	-	-	-	-	-	-	-	-	55,944.00	55,944.00
Total de Sueldos	**273,006.72**	**273,006.72**	**273,006.72**	**273,006.72**	**273,006.72**	**273,006.72**	**273,006.72**	**273,006.72**	**273,006.72**	**273,006.72**	**273,006.72**	**328,950.72**	**3,332,024.64**
Varios (8%)	21,840.54	21,840.54	21,840.54	21,840.54	21,840.54	21,840.54	21,840.54	21,840.54	21,840.54	21,840.54	21,840.54	26,316.06	266,561.97
Total Final	**533,858.23**	**335,408.23**	**335,408.23**	**335,408.23**	**335,408.23**	**335,408.23**	**335,408.23**	**335,408.23**	**335,408.23**	**335,408.23**	**335,408.23**	**395,827.75**	**4,283,768.31**

(Elaboración propia, 2022)

Supuestos del presupuesto administrativo:

1. Se considera un 8% para gastos diversos o imprevistos
2. Para el primer año se considera una plantilla de trabajo 1 vendedor, 2 implementadores, un coordinador de RH y 1 gerente
3. Para el segundo año se considera la contratación de un segundo vendedor
4. Para el tercer año se considera la contratación de un tercer implementador
5. Se considera un aumento salarial anual del 6% para toda la plantilla, excepto vendedores
6. Se considera un sueldo base de $ 22,000.00 el primer año para vendedores más comisiones por venta del 5%
7. Se considera un incremento anual del 5% en todos los costos fijos
8. Se considera un aguinaldo de 25% de sueldo para toda la plantilla
9. Se considera capacitación anual para toda la plantilla

10.3.4 Presupuesto de mercadotecnia

Figura 24. Presupuesto de mercadotecnia del primer año

AÑO 1													
Producto	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Diseño logotipo	1,000.00	-	-	-	-	-	-	-	-	-	-	-	1,000.00
Diseño de manuales coorporativos	1,500.00												1,500.00
Subtotal	**2,500.00**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**2,500.00**
Plaza	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Dominio con 20 cuentas de correo	450.00	-	-	-	-	-	-	-	-	-	-	-	450.00
Hosting	1,350.00	-	-	-	-	-	-	-	-	-	-	-	1,350.00
Eventos y ferias	10,000.00	-	-	-	-	-	-	-	-	-	-	-	10,000.00
Decoración instalaciones	10,000.00	-	-	-	-	-	-	-	-	-	-	-	10,000.00
Sitio web	6,000.00	-	-	-	-	-	-	-	-	-	-	-	6,000.00
Subtotal	**27,800.00**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**27,800.00**
Promoción	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Volantes 1000 pzs.	580.00	-	-	-	-	-	-	-	-	-	-	-	580.00
Redes sociales (Facebook e intagram)	6,000.00	-	-	-	-	-	-	-	-	-	-	-	6,000.00
Campañas en redes	1,400.00	-	-	1,400.00	-	-	1,400.00	-	-	1,400.00	-	-	5,600.00
Subtotal	**7,980.00**	**-**	**-**	**1,400.00**	**-**	**-**	**1,400.00**	**-**	**-**	**1,400.00**	**-**	**-**	**12,180.00**
Precio	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Descuento en diagnóstico del 10%	2,500.00	2,500.00	2,500.00	2,500.00	2,500.00	2,500.00	2,500.00	2,500.00	2,500.00	2,500.00	2,500.00	2,500.00	30,000.00
Subtotal	**2,500.00**	**2,500.00**	**2,500.00**	**2,500.00**	**2,500.00**	**2,500.00**	**2,500.00**	**2,500.00**	**2,500.00**	**2,500.00**	**2,500.00**	**2,500.00**	**30,000.00**
Varios (8%)	3,262.40	200.00	200.00	312.00	200.00	200.00	312.00	200.00	200.00	312.00	200.00	200.00	5,798.40
Total Final	**44,042.40**	**2,700.00**	**2,700.00**	**4,212.00**	**2,700.00**	**2,700.00**	**4,212.00**	**2,700.00**	**2,700.00**	**4,212.00**	**2,700.00**	**2,700.00**	**78,278.40**

(Elaboración propia, 2022)

Figura 25. Presupuesto de mercadotecnia del segundo año

AÑO 2													
Producto	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Diseño logotipo	-	-	-	-	-	-	-	-	-	-	-	-	-
Diseño de manuales coorporativos	-												-
Subtotal	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
Plaza	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Dominio con 20 cuentas de correo	472.50	-	-	-	-	-	-	-	-	-	-	-	472.50
Hosting	1,417.50	-	-	-	-	-	-	-	-	-	-	-	1,417.50
Eventos y ferias	10,000.00	-	-	-	-	-	-	-	-	-	-	-	10,000.00
Decoración instalaciones	-	-	-	-	-	-	-	-	-	-	-	-	-
Sitio web	-	-	-	-	-	-	-	-	-	-	-	-	-
Subtotal	**11,890.00**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**11,890.00**
Promoción	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Volantes 1000 pzs.	609.00	-	-	-	-	-	-	-	-	-	-	-	609.00
Redes sociales (Facebook e intagram)	-	-	-	-	-	-	-	-	-	-	-	-	-
Campañas en redes	1,470.00	-	-	1,470.00	-	-	1,470.00	-	-	1,470.00	-	-	5,880.00
Subtotal	**2,079.00**	**-**	**-**	**1,470.00**	**-**	**-**	**1,470.00**	**-**	**-**	**1,470.00**	**-**	**-**	**6,489.00**
Precio	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Descuento en diagnóstico del 10%	2,750.00	2,750.00	2,750.00	2,750.00	2,750.00	2,750.00	2,750.00	2,750.00	2,750.00	2,750.00	2,750.00	2,750.00	33,000.00
Subtotal	**2,750.00**	**2,750.00**	**2,750.00**	**2,750.00**	**2,750.00**	**2,750.00**	**2,750.00**	**2,750.00**	**2,750.00**	**2,750.00**	**2,750.00**	**2,750.00**	**33,000.00**
Varios (8%)	1,337.52	220.00	220.00	337.60	220.00	220.00	337.60	220.00	220.00	337.60	220.00	220.00	4,110.32
Total Final	**18,056.52**	**2,970.00**	**2,970.00**	**4,557.60**	**2,970.00**	**2,970.00**	**4,557.60**	**2,970.00**	**2,970.00**	**4,557.60**	**2,970.00**	**2,970.00**	**55,489.32**

(Elaboración propia, 2022)

Figura 26. Presupuesto de mercadotecnia del tercer año

AÑO 3													
Producto	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Diseño logotipo	-	-	-	-	-	-	-	-	-	-	-	-	-
Diseño de manuales coorporativos	-												-
Subtotal	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
Plaza	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Dominio con 20 cuentas de correo	496.13	-	-	-	-	-	-	-	-	-	-	-	496.13
Hosting	1,488.38	-	-	-	-	-	-	-	-	-	-	-	1,488.38
Eventos y ferias	10,000.00	-	-	-	-	-	-	-	-	-	-	-	10,000.00
Decoración instalaciones	-	-	-	-	-	-	-	-	-	-	-	-	-
Sitio web	-	-	-	-	-	-	-	-	-	-	-	-	-
Subtotal	**11,984.50**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**11,984.50**
Promoción	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Volantes 1000 pzs.	639.45	-	-	-	-	-	-	-	-	-	-	-	639.45
Redes sociales (Facebook e intagram)	-	-	-	-	-	-	-	-	-	-	-	-	-
Campañas en redes	1,543.50	-	-	1,543.50	-	-	1,543.50	-	-	1,543.50	-	-	6,174.00
Subtotal	**2,182.95**	**-**	**-**	**1,543.50**	**-**	**-**	**1,543.50**	**-**	**-**	**1,543.50**	**-**	**-**	**6,813.45**
Precio	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Descuento en diagnóstico del 10%	3,025.00	3,025.00	3,025.00	3,025.00	3,025.00	3,025.00	3,025.00	3,025.00	3,025.00	3,025.00	3,025.00	3,025.00	36,300.00
Subtotal	**3,025.00**	**3,025.00**	**3,025.00**	**3,025.00**	**3,025.00**	**3,025.00**	**3,025.00**	**3,025.00**	**3,025.00**	**3,025.00**	**3,025.00**	**3,025.00**	**36,300.00**
Varios (8%)	1,375.40	242.00	242.00	365.48	242.00	242.00	365.48	242.00	242.00	365.48	242.00	242.00	4,407.84
Total Final	**18,567.85**	**3,267.00**	**3,267.00**	**4,933.98**	**3,267.00**	**3,267.00**	**4,933.98**	**3,267.00**	**3,267.00**	**4,933.98**	**3,267.00**	**3,267.00**	**59,505.79**

(Elaboración propia, 2022)

Supuestos del presupuesto de mercadotecnia:

1. Se considera un 8% para gastos diversos o imprevistos
2. Se considera un incremento en el costo de tarjetas de presentación de 5% cada año
3. Se considera un incremento en el costo de hosting de 5% cada año
4. Se considera un incremento en el costo del dominio de 5% cada año
5. Se considera un incremento en el costo de campañas en redes de 5% cada año

10.3.5 Presupuesto de operación

Figura 27. Presupuesto de operación del primer año

AÑO 1													
Gastos operativos	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Vales de gasolina	6,000.00	6,000.00	6,000.00	6,000.00	6,000.00	6,000.00	6,000.00	6,000.00	6,000.00	6,000.00	6,000.00	6,000.00	72,000.00
Antivirus Kaspersky Total S. (7 nodos)	2,000.00	-	-	-	-	-	-	-	-	-	-	-	2,000.00
Office 365 (2-6 personas)	1,749.00	-	-	-	-	-	-	-	-	-	-	-	1,749.00
Adminpaq (1 nodo)	3,000.00	-	-	-	-	-	-	-	-	-	-	-	3,000.00
Insumos de oficina	1,500.00	-	1,500.00	-	1,500.00	-	1,500.00	-	1,500.00	-	1,500.00	-	9,000.00
Comisiones por venta	-	12,062.50	12,062.50	12,062.50	12,062.50	12,062.50	16,662.50	16,662.50	16,662.50	16,662.50	16,662.50	16,662.50	160,287.50
Licencias de AV cliente	-	37,500.00	37,500.00	37,500.00	37,500.00	37,500.00	62,500.00	62,500.00	62,500.00	62,500.00	62,500.00	62,500.00	562,500.00
Insumos de limpieza	1,000.00	1,000.00	1,000.00	1,000.00	1,000.00	1,000.00	1,000.00	1,000.00	1,000.00	1,000.00	1,000.00	1,000.00	12,000.00
Subtotal de costos fijos	**15,249.00**	**56,562.50**	**58,062.50**	**56,562.50**	**58,062.50**	**56,562.50**	**87,662.50**	**86,162.50**	**87,662.50**	**86,162.50**	**87,662.50**	**86,162.50**	**822,536.50**
Varios (8%)	1,219.92	4,525.00	4,645.00	4,525.00	4,645.00	4,525.00	7,013.00	6,893.00	7,013.00	6,893.00	7,013.00	6,893.00	65,802.92
Total Final	**16,468.92**	**61,087.50**	**62,707.50**	**61,087.50**	**62,707.50**	**61,087.50**	**94,675.50**	**93,055.50**	**94,675.50**	**93,055.50**	**94,675.50**	**93,055.50**	**888,339.42**

(Elaboración propia, 2022)

Figura 28. Presupuesto de operación del segundo año

AÑO 2													
Gastos operativos	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Vales de gasolina	7,500.00	7,500.00	7,500.00	7,500.00	7,500.00	7,500.00	7,500.00	7,500.00	7,500.00	7,500.00	7,500.00	7,500.00	90,000.00
Antivirus Kaspersky Total S. (7 nodos)	2,100.00												2,100.00
Office 365 (2-6 personas)	1,836.45												1,836.45
Adminpaq (1 nodo)	3,150.00												3,150.00
Insumos de oficina	1,575.00	-	1,575.00	-	1,575.00	-	1,575.00	-	1,575.00	-	1,575.00	-	9,450.00
Comisiones por venta	22,325.63	22,325.63	22,325.63	22,325.63	22,325.63	22,325.63	27,155.63	27,155.63	27,155.63	27,155.63	27,155.63	27,155.63	296,887.50
Licencias de AV cliente	87,500.00	87,500.00	87,500.00	87,500.00	87,500.00	87,500.00	112,500.00	112,500.00	112,500.00	112,500.00	112,500.00	112,500.00	1,200,000.00
Insumos de limpieza	1,050.00	1,050.00	1,050.00	1,050.00	1,050.00	1,050.00	1,050.00	1,050.00	1,050.00	1,050.00	1,050.00	1,050.00	12,600.00
Subtotal de costos fijos	**127,037.08**	**118,375.63**	**119,950.63**	**118,375.63**	**119,950.63**	**118,375.63**	**149,780.63**	**148,205.63**	**149,780.63**	**148,205.63**	**149,780.63**	**148,205.63**	**1,616,023.95**
Varios (8%)	10,162.97	9,470.05	9,596.05	9,470.05	9,596.05	9,470.05	11,982.45	11,856.45	11,982.45	11,856.45	11,982.45	11,856.45	129,281.92
Total Final	**137,200.04**	**127,845.68**	**129,546.68**	**127,845.68**	**129,546.68**	**127,845.68**	**161,763.08**	**160,062.08**	**161,763.08**	**160,062.08**	**161,763.08**	**160,062.08**	**1,745,305.87**

(Elaboración propia, 2022)

Figura 29. Presupuesto de operación del tercer año

AÑO 3													
Gastos operativos	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**	**Total**
Vales de gasolina	9,000.00	9,000.00	9,000.00	9,000.00	9,000.00	9,000.00	9,000.00	9,000.00	9,000.00	9,000.00	9,000.00	9,000.00	108,000.00
Antivirus Kaspersky Total S. (7 nodos)	2,205.00												2,205.00
Office 365 (2-6 personas)	3,856.55												3,856.55
Adminpaq (1 nodo)	3,307.50												3,307.50
Insumos de oficina	1,653.75	-	1,653.75	-	1,653.75	-	1,653.75	-	1,653.75	-	1,653.75	-	9,922.50
Comisiones por venta	33,584.91	33,584.91	33,584.91	33,584.91	33,584.91	33,584.91	38,656.41	38,656.41	38,656.41	38,656.41	38,656.41	38,656.41	433,447.88
Licencias de AV cliente	137,500.00	137,500.00	137,500.00	137,500.00	137,500.00	137,500.00	162,500.00	162,500.00	162,500.00	162,500.00	162,500.00	162,500.00	1,800,000.00
Insumos de limpieza	1,102.50	1,102.50	1,102.50	1,102.50	1,102.50	1,102.50	1,102.50	1,102.50	1,102.50	1,102.50	1,102.50	1,102.50	13,230.00
Subtotal de costos fijos	**192,210.20**	**181,187.41**	**182,841.16**	**181,187.41**	**182,841.16**	**181,187.41**	**212,912.66**	**211,258.91**	**212,912.66**	**211,258.91**	**212,912.66**	**211,258.91**	**2,373,969.42**
Varios (8%)	15,376.82	14,494.99	14,627.29	14,494.99	14,627.29	14,494.99	17,033.01	16,900.71	17,033.01	16,900.71	17,033.01	16,900.71	189,917.55
Total Final	**207,587.02**	**195,682.40**	**197,468.45**	**195,682.40**	**197,468.45**	**195,682.40**	**229,945.67**	**228,159.62**	**229,945.67**	**228,159.62**	**229,945.67**	**228,159.62**	**2,563,886.97**

(Elaboración propia, 2022)

Supuestos del presupuesto de operación:

1. Se considera un 8% para gastos diversos o imprevistos
2. Se considera un incremento anual del 5% en todos los gastos operativos

10.3.6 Estado de resultados

Figura 30. Estado de resultados del primer año de operación

Año 2023		Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	Total
Ventas														
Diagnóstico de nivel de madurez en ciberseguridad		-	90,000.00	90,000.00	90,000.00	90,000.00	90,000.00	102,000.00	102,000.00	102,000.00	102,000.00	102,000.00	102,000.00	1,062,000.00
Implementación de consola de antivirus y endpoint		-	25,000.00	25,000.00	25,000.00	25,000.00	25,000.00	50,000.00	50,000.00	50,000.00	50,000.00	50,000.00	50,000.00	425,000.00
Gestión de consola de antivirus y endpoint		-	16,250.00	16,250.00	16,250.00	16,250.00	16,250.00	16,250.00	16,250.00	16,250.00	16,250.00	16,250.00	16,250.00	178,750.00
Capacitación en ciberseguridad		-	30,000.00	30,000.00	30,000.00	30,000.00	30,000.00	45,000.00	45,000.00	45,000.00	45,000.00	45,000.00	45,000.00	420,000.00
Consultoría en implementación y cumplimiento de estándares		-	80,000.00	80,000.00	80,000.00	80,000.00	80,000.00	120,000.00	120,000.00	120,000.00	120,000.00	120,000.00	120,000.00	1,120,000.00
Total de Ventas		**-**	**241,250.00**	**241,250.00**	**241,250.00**	**241,250.00**	**241,250.00**	**333,250.00**	**333,250.00**	**333,250.00**	**333,250.00**	**333,250.00**	**333,250.00**	**3,205,750.00**
Costo de venta		16,468.92	61,087.50	62,707.50	61,087.50	62,707.50	61,087.50	94,675.50	93,055.50	94,675.50	93,055.50	94,675.50	93,055.50	888,339.42
Utilidad Bruta		**- 16,468.92**	**180,162.50**	**178,542.50**	**180,162.50**	**178,542.50**	**180,162.50**	**238,574.50**	**240,194.50**	**238,574.50**	**240,194.50**	**238,574.50**	**240,194.50**	**2,317,410.58**
Gastos de operación														
Gasto de administración		447,065.20	239,265.20	239,265.20	239,265.20	239,265.20	239,265.20	239,265.20	239,265.20	239,265.20	239,265.20	239,265.20	280,305.20	3,120,022.40
Gasto de Marketing		44,042.40	2,700.00	2,700.00	4,212.00	2,700.00	2,700.00	4,212.00	2,700.00	2,700.00	4,212.00	2,700.00	2,700.00	78,278.40
Total de gasto de operación		**491,107.60**	**241,965.20**	**241,965.20**	**243,477.20**	**241,965.20**	**241,965.20**	**243,477.20**	**241,965.20**	**241,965.20**	**243,477.20**	**241,965.20**	**283,005.20**	**3,198,300.80**
Depreciación		-	-	-	-	-	-	-	-	-	-	-	-	-
Utilidad de operación		**- 507,576.52**	**- 61,802.70**	**- 63,422.70**	**- 63,314.70**	**- 63,422.70**	**- 61,802.70**	**- 4,902.70**	**- 1,770.70**	**- 3,390.70**	**- 3,282.70**	**- 3,390.70**	**- 42,810.70**	**- 880,890.22**
Intereses		-	-	-	-	-	-	-	-	-	-	-	-	-
Utilidad antes de impuestos		**- 507,576.52**	**- 61,802.70**	**- 63,422.70**	**- 63,314.70**	**- 63,422.70**	**- 61,802.70**	**- 4,902.70**	**- 1,770.70**	**- 3,390.70**	**- 3,282.70**	**- 3,390.70**	**- 42,810.70**	**- 880,890.22**
ISR	30%	-	-	-	-	-	-	-	-	-	-	-	-	-
Utilidad Neta		**- 507,576.52**	**- 61,802.70**	**- 63,422.70**	**- 63,314.70**	**- 63,422.70**	**- 61,802.70**	**- 4,902.70**	**- 1,770.70**	**- 3,390.70**	**- 3,282.70**	**- 3,390.70**	**- 42,810.70**	**- 880,890.22**

(Elaboración propia, 2022)

Figura 31. Estado de resultados del segundo año de operación

Año 2024		Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	Total
Ventas														
Diagnóstico de nivel de madurez en ciberseguridad		119,700.00	119,700.00	119,700.00	119,700.00	119,700.00	119,700.00	132,300.00	132,300.00	132,300.00	132,300.00	132,300.00	132,300.00	1,512,000.00
Implementación de consola de antivirus y endpoint		78,750.00	78,750.00	78,750.00	78,750.00	78,750.00	78,750.00	105,000.00	105,000.00	105,000.00	105,000.00	105,000.00	105,000.00	1,102,500.00
Gestión de consola de antivirus y endpoint		17,062.50	17,062.50	17,062.50	17,062.50	17,062.50	17,062.50	17,062.50	17,062.50	17,062.50	17,062.50	17,062.50	17,062.50	204,750.00
Capacitación en ciberseguridad		63,000.00	63,000.00	63,000.00	63,000.00	63,000.00	63,000.00	78,750.00	78,750.00	78,750.00	78,750.00	78,750.00	78,750.00	850,500.00
Consultoría en implementación y cumplimiento de estándares		168,000.00	168,000.00	168,000.00	168,000.00	168,000.00	168,000.00	210,000.00	210,000.00	210,000.00	210,000.00	210,000.00	210,000.00	2,268,000.00
Total de Ventas		**446,512.50**	**446,512.50**	**446,512.50**	**446,512.50**	**446,512.50**	**446,512.50**	**543,112.50**	**543,112.50**	**543,112.50**	**543,112.50**	**543,112.50**	**543,112.50**	**5,937,750.00**
Costo de venta		137,200.04	127,845.68	129,546.68	127,845.68	129,546.68	127,845.68	161,763.08	160,062.08	161,763.08	160,062.08	161,763.08	160,062.08	888,339.42
Utilidad Bruta		**309,312.46**	**318,666.83**	**316,965.83**	**318,666.83**	**316,965.83**	**318,666.83**	**381,349.43**	**383,050.43**	**381,349.43**	**383,050.43**	**381,349.43**	**383,050.43**	**5,049,410.58**
Gastos de operación														
Gasto de administración		467,169.18	278,169.18	278,169.18	278,169.18	278,169.18	278,169.18	278,169.18	278,169.18	278,169.18	278,169.18	278,169.18	327,255.18	3,576,116.16
Gasto de Marketing		18,056.52	2,970.00	2,970.00	4,557.60	2,970.00	2,970.00	4,557.60	2,970.00	2,970.00	4,557.60	2,970.00	2,970.00	55,489.32
Total de gasto de operación		**485,225.70**	**281,139.18**	**281,139.18**	**282,726.78**	**281,139.18**	**281,139.18**	**282,726.78**	**281,139.18**	**281,139.18**	**282,726.78**	**281,139.18**	**330,225.18**	**3,631,605.48**
Depreciación		6,281.65	6,281.65	6,281.65	6,281.65	6,281.65	6,281.65	6,281.65	6,281.65	6,281.65	6,281.65	6,281.65	6,281.65	75,379.80
Utilidad de operación	-	**182,194.89**	**31,246.00**	**29,545.00**	**29,658.40**	**29,545.00**	**31,246.00**	**92,341.00**	**95,629.60**	**93,928.60**	**94,042.00**	**93,928.60**	**46,543.60**	**1,342,425.30**
Intereses		-	-	-	-	-	-	-	-	-	-	-	-	-
Utilidad antes de impuestos	-	**182,194.89**	**31,246.00**	**29,545.00**	**29,658.40**	**29,545.00**	**31,246.00**	**92,341.00**	**95,629.60**	**93,928.60**	**94,042.00**	**93,928.60**	**46,543.60**	**1,342,425.30**
ISR	30% -	318,925.53	9,373.80	8,863.50	8,897.52	8,863.50	9,373.80	27,702.30	28,688.88	28,178.58	28,212.60	28,178.58	13,963.08	402,727.59
Utilidad Neta		**136,730.64**	**21,872.20**	**20,681.50**	**20,760.88**	**20,681.50**	**21,872.20**	**64,638.70**	**66,940.72**	**65,750.02**	**65,829.40**	**65,750.02**	**32,580.52**	**939,697.71**

(Elaboración propia, 2022)

Figura 32. Estado de resultados del tercer año de operación

Año 2025		Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	Total
Ventas														
Diagnóstico de nivel de madurez en ciberseguridad		152,145.00	152,145.00	152,145.00	152,145.00	152,145.00	152,145.00	165,375.00	165,375.00	165,375.00	165,375.00	165,375.00	165,375.00	1,905,120.00
Implementación de consola de antivirus y endpoint		137,812.50	137,812.50	137,812.50	137,812.50	137,812.50	137,812.50	165,375.00	165,375.00	165,375.00	165,375.00	165,375.00	165,375.00	1,819,125.00
Gestión de consola de antivirus y endpoint		17,915.63	17,915.63	17,915.63	17,915.63	17,915.63	17,915.63	17,915.63	17,915.63	17,915.63	17,915.63	17,915.63	17,915.63	214,987.50
Capacitación en ciberseguridad		99,225.00	99,225.00	99,225.00	99,225.00	99,225.00	99,225.00	115,762.50	115,762.50	115,762.50	115,762.50	115,762.50	115,762.50	1,289,925.00
Consultoría en implementación y cumplimiento de estándares		264,600.00	264,600.00	264,600.00	264,600.00	264,600.00	264,600.00	308,700.00	308,700.00	308,700.00	308,700.00	308,700.00	308,700.00	3,439,800.00
Total de Ventas		**671,698.13**	**671,698.13**	**671,698.13**	**671,698.13**	**671,698.13**	**671,698.13**	**773,128.13**	**773,128.13**	**773,128.13**	**773,128.13**	**773,128.13**	**773,128.13**	**8,668,957.50**
Costo de venta		207,587.02	195,682.40	197,468.45	195,682.40	197,468.45	195,682.40	229,945.67	228,159.62	229,945.67	228,159.62	229,945.67	228,159.62	2,563,886.97
Utilidad Bruta		**464,111.11**	**476,015.73**	**474,229.68**	**476,015.73**	**474,229.68**	**476,015.73**	**543,182.46**	**544,968.51**	**543,182.46**	**544,968.51**	**543,182.46**	**544,968.51**	**6,105,070.53**
Gastos de operación														
Gasto de administración		533,858.23	335,408.23	335,408.23	335,408.23	335,408.23	335,408.23	335,408.23	335,408.23	335,408.23	335,408.23	335,408.23	395,827.75	4,283,768.31
Gasto de Marketing		18,567.85	3,267.00	3,267.00	4,933.98	3,267.00	3,267.00	4,933.98	3,267.00	3,267.00	4,933.98	3,267.00	3,267.00	59,505.79
Total de gasto de operación		**552,426.08**	**338,675.23**	**338,675.23**	**340,342.21**	**338,675.23**	**338,675.23**	**340,342.21**	**338,675.23**	**338,675.23**	**340,342.21**	**338,675.23**	**399,094.75**	**4,343,274.10**
Depreciación		6,281.65	6,281.65	6,281.65	6,281.65	6,281.65	6,281.65	6,281.65	6,281.65	6,281.65	6,281.65	6,281.65	6,281.65	75,379.80
Utilidad de operación	-	**94,596.62**	**131,058.84**	**129,272.79**	**129,391.86**	**129,272.79**	**131,058.84**	**196,558.59**	**200,011.62**	**198,225.57**	**198,344.64**	**198,225.57**	**139,592.10**	**1,686,416.63**
Intereses		-	-	-	-	-	-	-	-	-	-	-	-	-
Utilidad antes de impuestos	-	**94,596.62**	**131,058.84**	**129,272.79**	**129,391.86**	**129,272.79**	**131,058.84**	**196,558.59**	**200,011.62**	**198,225.57**	**198,344.64**	**198,225.57**	**139,592.10**	**1,686,416.63**
ISR	30%	253,530.33	39,317.65	38,781.84	38,817.56	38,781.84	39,317.65	58,967.58	60,003.49	59,467.67	59,503.39	59,467.67	41,877.63	505,924.99
Utilidad Neta	-	**348,126.95**	**91,741.19**	**90,490.96**	**90,574.30**	**90,490.96**	**91,741.19**	**137,591.02**	**140,008.14**	**138,757.90**	**138,841.25**	**138,757.90**	**97,714.47**	**1,180,491.64**

(Elaboración propia, 2022)

Supuestos del estado de resultados:

1. Se considera que los 12 primeros meses no habrá pago de impuestos
2. Se considera que los 12 primeros meses no habrá depreciaciones
3. Se considera una tasa del 30% para el pago de impuestos
4. No se consideran pagos de intereses por ser capital propio

10.3.7 Flujos de efectivo

Figura 33. Flujo de efectivo primer año

Flujos de efectivo	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	Total
Ingresos (Entradas)													
Saldo Inicial	1,200,000.00	315,524.48	253,721.78	190,299.08	126,984.38	63,561.68	1,758.98 -	3,143.72 -	4,914.42 -	8,305.12 -	11,587.82 -	14,978.52	1,200,000.00
Ventas Totales	-	241,250.00	241,250.00	241,250.00	241,250.00	241,250.00	333,250.00	333,250.00	333,250.00	333,250.00	333,250.00	333,250.00	3,205,750.00
Otros Ingresos													
Subtotal ingresos	**1,200,000.00**	**556,774.48**	**494,971.78**	**431,549.08**	**368,234.38**	**304,811.68**	**335,008.98**	**330,106.28**	**328,335.58**	**324,944.88**	**321,662.18**	**318,271.48**	**4,405,750.00**
Egresos (Salidas)													
Inversión en muebles	376,899.00												376,899.00
Mercadotecnia	44,042.40	2,700.00	2,700.00	4,212.00	2,700.00	2,700.00	4,212.00	2,700.00	2,700.00	4,212.00	2,700.00	2,700.00	78,278.40
Operaciones	16,468.92	61,087.50	62,707.50	61,087.50	62,707.50	61,087.50	94,675.50	93,055.50	94,675.50	93,055.50	94,675.50	93,055.50	888,339.42
Administrativo	447,065.20	239,265.20	239,265.20	239,265.20	239,265.20	239,265.20	239,265.20	239,265.20	239,265.20	239,265.20	239,265.20	280,305.20	3,120,022.40
Financianciero	-												-
Pago de impuestos 30%	-	-	-	-	-	-	-	-	-	-	-	-	-
Subtotal Egresos	**884,475.52**	**303,052.70**	**304,672.70**	**304,564.70**	**304,672.70**	**303,052.70**	**338,152.70**	**335,020.70**	**336,640.70**	**336,532.70**	**336,640.70**	**376,060.70**	**4,463,539.22**
Saldo Final	**315,524.48**	**253,721.78**	**190,299.08**	**126,984.38**	**63,561.68**	**1,758.98 -**	**3,143.72 -**	**4,914.42 -**	**8,305.12 -**	**11,587.82 -**	**14,978.52 -**	**57,789.22 -**	**57,789.22**

(Elaboración propia, 2022)

Figura 34. Flujo de efectivo del segundo año

Flujos de efectivo	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	Total
Ingresos (Entradas)													
Saldo Inicial	57,789.22 -	291,675.93 -	263,522.08 -	236,558.93 -	209,516.41 -	182,553.26 -	154,399.42 -	83,479.07 -	10,256.70	61,774.96	133,886.01	205,917.68 -	57,789.22
Ventas Totales	446,512.50	446,512.50	446,512.50	446,512.50	446,512.50	446,512.50	543,112.50	543,112.50	543,112.50	543,112.50	543,112.50	543,112.50	5,937,750.00
Otros Ingresos													
Subtotal ingresos	**388,723.28**	**154,836.57**	**182,990.42**	**209,953.57**	**236,996.09**	**263,959.24**	**388,713.08**	**459,633.43**	**532,855.80**	**604,887.46**	**676,998.51**	**749,030.18**	**5,879,960.78**
Egresos (Salidas)													
Inversión en muebles	376,899.00												376,899.00
Mercadotecnia	18,056.52	2,970.00	2,970.00	4,557.60	2,970.00	2,970.00	4,557.60	2,970.00	2,970.00	4,557.60	2,970.00	2,970.00	55,489.32
Operaciones	137,200.04	127,845.68	129,546.68	127,845.68	129,546.68	127,845.68	161,763.08	160,062.08	161,763.08	160,062.08	161,763.08	160,062.08	888,339.42
Administrativo	467,169.18	278,169.18	278,169.18	278,169.18	278,169.18	278,169.18	278,169.18	278,169.18	278,169.18	278,169.18	278,169.18	327,255.18	3,576,116.16
Financianciero													
Pago de impuestos 30%	318,925.53 -	9,373.80	8,863.50	8,897.52	8,863.50	9,373.80	27,702.30	28,688.88	28,178.58	28,212.60	28,178.58	13,963.08	402,727.59
Subtotal Egresos	**680,399.21**	**418,358.65**	**419,549.35**	**419,469.97**	**419,549.35**	**418,358.65**	**472,192.15**	**469,890.13**	**471,080.83**	**471,001.45**	**471,080.83**	**504,250.33**	**5,299,571.49**
Saldo Final	**291,675.93 -**	**263,522.08 -**	**236,558.93 -**	**209,516.41 -**	**182,553.26 -**	**154,399.42 -**	**83,479.07 -**	**10,256.70**	**61,774.96**	**133,886.01**	**205,917.68**	**244,779.84**	**580,389.29**

(Elaboración propia, 2022)

Figura 35. Flujo de efectivo del tercer año

Flujos de efectivo	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	Total
Ingresos (Entradas)													
Saldo Inicial	580,389.29	- 138,355.01	- 40,332.17	56,440.44	153,296.39	250,069.00	348,091.84	491,964.50	638,254.29	783,293.84	928,416.74	1,073,456.29	580,389.29
Ventas Totales	671,698.13	671,698.13	671,698.13	671,698.13	671,698.13	671,698.13	773,128.13	773,128.13	773,128.13	773,128.13	773,128.13	773,128.13	8,668,957.50
Otros Ingresos													
Subtotal ingresos	**1,252,087.42**	**533,343.12**	**631,365.96**	**728,138.56**	**824,994.52**	**921,767.12**	**1,121,219.96**	**1,265,092.63**	**1,411,382.42**	**1,556,421.97**	**1,701,544.87**	**1,846,584.42**	**9,249,346.79**
Egresos (Salidas)													
Inversión en muebles	376,899.00												376,899.00
Mercadotecnia	18,567.85	3,267.00	3,267.00	4,933.98	3,267.00	3,267.00	4,933.98	3,267.00	3,267.00	4,933.98	3,267.00	3,267.00	59,505.79
Operaciones	207,587.02	195,682.40	197,468.45	195,682.40	197,468.45	195,682.40	229,945.67	228,159.62	229,945.67	228,159.62	229,945.67	228,159.62	2,563,886.97
Administrativo	533,858.23	335,408.23	335,408.23	335,408.23	335,408.23	335,408.23	335,408.23	335,408.23	335,408.23	335,408.23	335,408.23	395,827.75	4,283,768.31
Financianciero													
Pago de impuestos 30%	253,530.33	39,317.65	38,781.84	38,817.56	38,781.84	39,317.65	58,967.58	60,003.49	59,467.67	59,503.39	59,467.67	41,877.63	505,924.99
Subtotal Egresos	**1,390,442.42**	**573,675.28**	**574,925.52**	**574,842.17**	**574,925.52**	**573,675.28**	**629,255.46**	**626,838.34**	**628,088.57**	**628,005.22**	**628,088.57**	**669,132.00**	**7,789,985.06**
Saldo Final	**- 138,355.01**	**- 40,332.17**	**56,440.44**	**153,296.39**	**250,069.00**	**348,091.84**	**491,964.50**	**638,254.29**	**783,293.84**	**928,416.74**	**1,073,456.29**	**1,177,452.42**	**1,459,361.73**

(Elaboración propia, 2022)

Supuestos del flujo de efectivo:

1. Se considera una tasa del 30% para el pago de impuestos
2. No se consideran pagos de intereses por ser capital propio

10.3.8 Balance general, TIR y PE

Figura 36. Balance general

Activos		Año 1		Año 2		Año 3
Activo Circulante						
Efectivo	-	57,789.22		957,288.29		2,213,159.73
Valores Negociables		-		-		-
Clientes (a crédito)		-		-		-
Inventarios		-		-		-
Activo Circulante Total	**-**	**57,789.22**		**957,288.29**		**2,213,159.73**
Activo No Circulante						
Activo fijo bruto		376,899.00		376,899.00		376,899.00
Depreciación acumulada		-		75,379.80		150,759.60
Activo No Circulante Total		**376,899.00**		**301,519.20**		**226,139.40**
ACTIVO TOTAL	**$**	**319,109.78**	**$**	**1,258,807.49**	**$**	**2,439,299.13**
Pasivos						
Pasivo circulante		-		-		-
Proveedores		-		-		-
Pasivo Bancario CP		-		-		-
Total Pasivo Circulante		-		-		-
Pasivo Largo Plazo		-		-		-
Pasivo Bancario		-		-		-
Pasivo Largo Plazo Total		-		-		-
Total Pasivo Circulante		-		-		-
Pasivo Total		**-**		**-**		**-**
Capital contable						
Capital social		1,200,000.00		1,200,000.00		1,200,000.00
Utilidades retenidas		-	-	880,890.22		58,807.49
Utilidades del ejercicio	-	880,890.22		939,697.71		1,180,491.64
Capital Contable Total		**319,109.78**		**1,258,807.49**		**2,439,299.13**
PASIVO TOTAL + CAPITAL CONTABLE TOTAL	**$**	**319,109.78**	**$**	**1,258,807.49**	**$**	**2,439,299.13**
PASIVO TOTAL + CAPITAL CONTABLE TOTAL - ACTIVO		**-**		**-**		**-**

(Elaboración propia, 2022)

Figura 37. VPN y TIR

Tasa de descuento	20%
VP	1,897,389.58
Inversión de los accionistas	- 57,789.22
VPN	1,955,178.80
VAN	1,927,577.55
TIR	44.03%

(Elaboración propia, 2022)

Figura 38. Punto de equilibrio

Punto de equilibrio	Año 1	Año 2	Año 3	Total
Costos Fijos	3,120,022.40	3,576,116.16	4,283,768.31	10,979,906.87
Costos variables to	966,617.82	1,800,795.19	2,623,392.76	5,390,805.77
Ventas Totales	3,205,750.00	5,937,750.00	8,668,957.50	17,812,457.50
PE	**4,466,914.41**	**5,132,781.16**	**6,142,652.84**	**15,745,017.55**

(Elaboración propia, 2022)

Supuestos generales:

1. Se consideran prestaciones de ley para la plantilla de trabajo
2. Se considera herramientas de trabajo como laptop, celular, vales de gasolina, tarjetas de presentación y línea de teléfono para gerente, vendedores e implementadores
3. Se considera contratar personal con experiencia y certificaciones en ciberseguridad y/o tecnologías de seguridad
4. Se considera rentar una oficina para 10 personas con sala de juntas
5. Se considera usar capital propio para cubrir el capital social de la empresa
6. Inicialmente solo se considera ofrecer 5 servicios
7. Costo de licenciamiento basado en precio de lista

11. Plan de implementación

Figura 39. WBS de implantación de empresa de ciberseguridad

EDT	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1	**EMPRENDIMIENTO EMPRESA DE SERVICIOS DE CIBERSEGURIDAD PARA PYMES**	0 días	lun 02/01/23	lun 02/01/23	
2	**Lista de clientes**	**23 días**	**lun 02/01/23**	**mié 01/02/23**	
2.1	Definir caracteristicas de prospectos de clientes	3 días	lun 02/01/23	mié 04/01/23	1
2.2	Explorar mercado y prospectos	15 días	jue 05/01/23	mié 25/01/23	3
2.3	Filtrar prospectos de clientes	3 días	jue 26/01/23	lun 30/01/23	4
2.4	Registrar prospectos	2 días	mar 31/01/23	mié 01/02/23	5
2.5	Confirmación lista de cliente	0 días	mié 01/02/23	mié 01/02/23	6
3	**Definición de catalogo de servicios**	**11 días**	**jue 02/02/23**	**jue 16/02/23**	**6**
3.1	Definir servicio	5 días	jue 02/02/23	mié 08/02/23	7
3.2	Desarrollo de servicio	5 días	jue 09/02/23	mié 15/02/23	9
3.3	Liberación de catalogo de servicios	1 día	jue 16/02/23	jue 16/02/23	10
3.4	Confirmación catalogo de servicios	0 días	jue 16/02/23	jue 16/02/23	11
4	**Evaluación de proyecto**	**34 días**	**vie 17/02/23**	**mié 05/04/23**	**12**
4.1	Diseño de caso de negocio	1 día	vie 17/02/23	vie 17/02/23	12
4.2	Ejecución de caso de negocio	30 días	lun 20/02/23	vie 31/03/23	14
4.3	Evaluación de caso de negocio	3 días	lun 03/04/23	mié 05/04/23	15
4.4	Confirmación de evaluación de proyecto	0 días	mié 05/04/23	mié 05/04/23	16
5	**Constitución legal de la empresa**	**11 días**	**jue 06/04/23**	**jue 20/04/23**	**17**
5.1	Definición de contratos legales y penalizaciones	5 días	jue 06/04/23	mié 12/04/23	17
5.2	Elaboración de contratos legales y penalizaciones	5 días	jue 13/04/23	mié 19/04/23	19
5.3	Firma de contratos legales y penalizaciones	1 día	jue 20/04/23	jue 20/04/23	20
5.4	Confirmación de contratos legales y penalizaciones	0 días	jue 20/04/23	jue 20/04/23	21
6	**Complemento de recursos y Tecnología clave**	**26 días**	**vie 21/04/23**	**vie 26/05/23**	**22**
6.1	**Tecnología clave**	**10 días**	**vie 21/04/23**	**jue 04/05/23**	**22**
6.1.1	Definición de herramienta de diagnostico	3 días	vie 21/04/23	mar 25/04/23	22
6.1.2	Adquisición de herramienta de diagnostico	1 día	mié 26/04/23	mié 26/04/23	25
6.1.3	Firma de contrato de soporte por 3 años y licencia	1 día	jue 27/04/23	jue 27/04/23	26
6.1.4	Configuración de herramienta de diagnostico	5 días	vie 28/04/23	jue 04/05/23	27
6.1.5	Confirmación de adquisición de tecnología clave	0 días	jue 04/05/23	jue 04/05/23	28
6.2	**Recursos humanos**	**26 días**	**vie 21/04/23**	**vie 26/05/23**	**22**
6.2.1	**Incorporación**	**15 días**	**vie 21/04/23**	**jue 11/05/23**	**22**
6.2.1.1	Filtrado y selección de candidato	5 días	vie 21/04/23	jue 27/04/23	22
6.2.1.2	Contratación	5 días	vie 28/04/23	jue 04/05/23	32
6.2.1.3	Onboarding	5 días	vie 05/05/23	jue 11/05/23	33
6.2.1.4	Confirmación de incorporación	0 días	jue 11/05/23	jue 11/05/23	34
6.2.2	**Capacitación**	**11 días**	**vie 12/05/23**	**vie 26/05/23**	**35**
6.2.2.1	Diseño de la capacitación	5 días	vie 12/05/23	jue 18/05/23	35
6.2.2.2	Ejecución de la capacitación	5 días	vie 19/05/23	jue 25/05/23	37
6.2.2.3	Evaluación de la capacitación	1 día	vie 26/05/23	vie 26/05/23	38
6.2.2.4	Confirmación de capacitación	0 días	vie 26/05/23	vie 26/05/23	39
6.3	**Inmobiliario**	**10 días**	**vie 21/04/23**	**jue 04/05/23**	**22**
6.3.1	**Adquisición**	**10 días**	**vie 21/04/23**	**jue 04/05/23**	**22**
6.3.1.1	**Adecuación**	**10 días**	**vie 21/04/23**	**jue 04/05/23**	**22**
6.3.1.1.	Diseño de inmobiliario	2 días	vie 21/04/23	lun 24/04/23	22
6.3.1.1.	Remodelaciones de inmobiliario	7 días	mar 25/04/23	mié 03/05/23	44
6.3.1.1.	Liberación de inmobiliario	1 día	jue 04/05/23	jue 04/05/23	45
6.3.1.1.	Confirmación adecuación	0 días	jue 04/05/23	jue 04/05/23	46
6.4	**Infraestructura y mobiliario**	**10 días**	**vie 05/05/23**	**jue 18/05/23**	**47**
6.4.1	**Adquisición**	**10 días**	**vie 05/05/23**	**jue 18/05/23**	**47**
6.4.1.1	Definición de infraestructura	2 días	vie 05/05/23	lun 08/05/23	47
6.4.1.2	Adquisición de infraestructura	5 días	mar 09/05/23	lun 15/05/23	50
6.4.1.3	Instalación de infraestructura	3 días	mar 16/05/23	jue 18/05/23	51
6.4.1.4	Confirmación adquisición	0 días	jue 18/05/23	jue 18/05/23	52
7	**Pruebas de diagnostico**	**15 días**	**vie 05/05/23**	**jue 25/05/23**	**29**
7.1	Definición de pruebas y laboratorios de diagnostico	3 días	vie 05/05/23	mar 09/05/23	29
7.2	Ejecución de pruebas y laboratorio de diagnostico	10 días	mié 10/05/23	mar 23/05/23	55
7.3	Documentación de resultado de pruebas	2 días	mié 24/05/23	jue 25/05/23	56
7.4	Confirmación de pruebas y laboratorio	0 días	jue 25/05/23	jue 25/05/23	57
8	**Validación de propuestas**	**6 días**	**vie 26/05/23**	**vie 02/06/23**	**58**
8.1	Definición de requerimientos de propuesta por parte de gerencias	3 días	vie 26/05/23	mar 30/05/23	58
8.2	Validación de propuesta por parte de gerencias	2 días	mié 31/05/23	jue 01/06/23	60
8.3	Aprobación de propuesta por parte de gerencias	1 día	vie 02/06/23	vie 02/06/23	61
8.4	Confirmación de propuestas	0 días	vie 02/06/23	vie 02/06/23	62
9	**Demostraciones**	**19 días**	**lun 05/06/23**	**jue 29/06/23**	**63**
9.1	Definición de demostraciones a prospectos de cliente	2 días	lun 05/06/23	mar 06/06/23	63
9.2	Ejecución de demostraciones a prospectos de cliente	15 días	mié 07/06/23	mar 27/06/23	65
9.3	Evaluar resultado de demostraciones a prospectos de cliente	2 días	mié 28/06/23	jue 29/06/23	66
9.4	Confirmación de demostraciones a prospectos de cliente	0 días	jue 29/06/23	jue 29/06/23	67
10	**Campañas de publicidad y promoción**	**38 días**	**lun 05/06/23**	**mié 26/07/23**	**63**
10.1	Diseño de campañas de publicidad y promoción	5 días	lun 05/06/23	vie 09/06/23	63
10.2	Ejecución de campañas de publicidad y promoción	30 días	lun 12/06/23	vie 21/07/23	70
10.3	Evaluación de campañas de publicidad y promoción	3 días	lun 24/07/23	mié 26/07/23	71
10.4	Confirmación de campañas de publicidady promoción	0 días	mié 26/07/23	mié 26/07/23	72
11	**Cierre del proyecto**	**5 días**	**jue 27/07/23**	**mié 02/08/23**	**73**
11.1	Cierre físico	2 días	jue 27/07/23	vie 28/07/23	73
11.2	Cierre administrativo	2 días	lun 31/07/23	mar 01/08/23	75
11.3	Liberación de recursos del proyecto de innovación	1 día	mié 02/08/23	mié 02/08/23	76
11.4	Confirmación de cierre de proyecto	0 días	mié 02/08/23	mié 02/08/23	77

(Elaboración propia, 2022)

La figura 39 muestra el plan de implantación de forma muy general, resultando en un plan de 11 grandes bloques, que a su vez se divide en dos etapas de la actividad 1 a la 4 es exploración y planeación, la cual en gran parte fue cubierta por el presente trabajo y de la actividad 5 a la 11 serían los siguientes pasos, es decir, una vez evaluado el proyecto sería materializarlo, realizar la inversiones, contrataciones, capacitaciones, etc.

- Lista de clientes
- Definición de catálogo de servicios
- Evaluación de proyecto
- Constitución legal de la empresa
- Tecnología clave
- Recursos humanos
- Infraestructura y mobiliario
- Pruebas de diagnóstico
- Validación de propuestas
- Demostraciones
- Campañas de publicidad y promoción
- Cierre del proyecto

Fase de exploración y planeación

Lista de clientes. En esta fase se pretende explorar el mercado, así como plasmar una lista concreta de posibles clientes con base en la información obtenida en la sección de contexto externo de este trabajo.
Definición de catálogo de servicios. Durante esta fase del proyecto se pretende definir el catálogo de servicios con alcances y responsabilidades de cliente y proveedor, tal como se describió en la sección 8.1 Propuesta de catálogo de servicios en ciberseguridad.
Evaluación de proyecto. Una vez cubiertos los puntos anteriores en esta fase se pretende realizar un ejercicio de proyecciones de ventas y gastos para realizar un análisis y un posible escenario de cómo se podrían comportar las ventas y tener una referencia de rentabilidad y qué tan atractivo puede ser el proyecto para invertir. Como parte de los objetivos del trabajo esto se desarrolló en la sección 10.3 Validación y Evaluación financiera.

Fase de implantación

Constitución legal de la empresa. Como parte de la materialización del proyecto evaluado es debido constituir legalmente la empresa y firmar los contratos necesarios para mitigar los riesgos descritos en la sección 11.1. Por ejemplo renuncia de personal clave o bien salida de socio.
Tecnología clave. Durante esta fase se incorporará la tecnología clave necesaria para cumplir con los servicios a entregar a los clientes, esta tecnología clave se refiere a los agentes de antivirus y licencias
Recursos humanos. Esta sección se refiere a la contratación formal del personal que hará posible la entrega del servicio a los clientes como son; implementadores, vendedores, gerentes, etc. Así como definición de personal como contador, mercadólogo, limpieza, etc.
Infraestructura y mobiliario. En esta fase del proyecto se realizarán adquisiciones de equipo de oficina, computo, instalaciones físicas, remodelaciones, etc. Básicamente todo lo relacionado al presupuesto de Inversión inicial de la sección 10.3.2.
Pruebas de diagnóstico. Ya con personal y tecnología clave se deberán realizar pruebas de funcionamiento previo a salir a mercado a realizar implementaciones.
Validación de propuestas. Una vez realizadas las pruebas de forma exitosa se armarán propuestas técnicas y económicas que podrían ser enviadas a los posibles clientes, esto siempre con base en el resultado de las pruebas y catálogo de servicios y lista de precios. Dichas pruebas serán validadas por las gerencias comercial y operacional.
Demostraciones. Con propuestas integradas se estaría listo para realizar demostraciones a los posibles clientes para conocer los beneficios de los servicios ofertados.
Campañas de publicidad y promoción. En paralelo a las demostraciones deben ocurrir las campañas de publicidad y promoción definidas dentro del presupuesto de mercadotecnia de la sección 10.3.4.

Cierre del proyecto. Finalmente el proyecto de implantación terminaría y a partir de ahí seguiría la operación diaria de la nueva empresa de servicios de ciberseguridad.

11.1 Análisis de riesgos

Para analizar los riesgos asociados al presente caso de negocios se plantea una matriz de tratamiento de cada riesgo, donde fueron clasificados y tratados de acuerdo con su impacto, probabilidad de que ocurran y si se trata de una oportunidad o amenaza.

Figura 40. Matriz de calor de riesgos

Oportunidad			Probabilidad	Amenazas		
			Alta			
			Media			
			Baja			
Bajo	Medio	Alto	**Impacto**	Alto	Medio	Bajo

(Elaboración propia, 2022)

Acción al riesgo de amenaza:

Evitar: Se genera un plan para eliminar cualquier amenaza de ocurrencia.
Transferir: Se transfiere responsabilidad e impacto en caso de ocurrencia.
Mitigar: Se busca reducir la probabilidad de ocurrencia.
Aceptar: Se acuerda que no es posible realizar acciones reactivas y en caso de ocurrencia se aceptaran las consecuencias.

Tabla 9. Matriz de riesgos empresa de ciberseguridad

ID	Riesgo	Actividad o tarea	¿Qué puede provocar?	¿Cómo impacta a la empresa?	Responsable	Probabilidad	Impacto	Tipo de riesgo	¿Qué acción vamos a tomar con relación al riesgo?	¿Qué acciones vamos a seguir para evitar el riesgo?
1	Accidente laboral	Traslados de personal para visitar a algún cliente o en las propias instalaciones	Ausencia de personal para actividades clave en la entrega del servicio	Retraso en el proceso o incumplimiento de las fechas comprometidas	Gerente	Bajo	Medio	Amenaza	Transferir	- Contar con prestaciones de ley como el IMSS. - Cumplir con normas de protección civil dentro de las instalaciones. - Contar con suficiente personal para cubrir posibles ausencias.
2	No contar con ventas suficientes	Ventas insuficientes para cubrir los costos fijos de la empresa	Pérdidas en el Estado de Resultados	Cierre de la empresa o endeudamiento	Gerente	Medio	Alto	Amenaza	Mitigar	- Reforzar la labor de venta con promoción y publicidad - Contar con capital social suficiente para operar sin ventas algunos meses - Plan de reducción de costos inmediato
3	No contar con personal calificado	Entrega del servicio y cumplimiento de compromisos	Implementaciones, diagnósticos y capacitaciones de baja calidad	Mala reputación y disminución de ventas	Gerente	Bajo	Medio	Amenaza	Mitigar	- Priorizar el proceso de contratación - Capacitación formal continua
4	Renuncia de personal clave	Entrega del servicio y cumplimiento de compromisos	Ausencia de personal para actividades clave en la entrega del	Retraso en el proceso o incumplimiento de las fechas comprometidas	Gerente	Medio	Medio	Amenaza	Mitigar	- Priorizar el proceso de contratación - Capacitación formal continua - Mejorar sueldos

			servicio							continuamente
5	No contar con socio	Creación de empresa nueva para brindar servicios de ciberseguridad	No contar con presupuesto suficiente	Cancelación de emprendimiento	Gerente	Medio	Alto	Amenaza	Evitar	- Contar con opciones extra de posibles socios - Financiar la otra mitad de presupuesto con bancos
6	Inseguridad y delincuencia	Robo de equipo y asalto	Pérdidas en activo	Pérdidas en el Estado de Resultados	Gerente	Bajo	Medio	Amenaza	Mitigar	- Contar con sistema de seguridad como cámaras - Instalaciones en zonas consideradas de no alto riesgo - Contar con presupuesto de 8% en cada rubro para imprevistos
7	Falta de cobro	Cuentas incobrables	Pérdidas en el Estado de Resultados	Esfuerzo desperdiciado	Gerente	Bajo	Medio	Amenaza	Evitar	Se cobrará el 50% por adelantado y al finalizar el servicio el 50% restante

(Elaboración propia, 2022)

12. Limitaciones y recomendaciones

Es natural que en el trabajo existan varias limitaciones a lo largo de sus diferentes secciones y es por ello que la intención de este apartado es describir esas limitaciones y recomendaciones para tomarse en cuenta y evaluarse antes de tomar decisiones.

12.1 Limitaciones

- Los pronósticos de ventas y evaluación financiera en general se realizaron en un escenario intermedio, es decir, no se cuenta con un escenario pesimista y optimista.
- Las entrevistas realizadas a expertos y prospectos de cliente fueron muy enriquecedoras, sin embargo, fueron limitadas por agendas y tiempos de entrega.
- El análisis FODA fue un ejercicio de proyección con algunas de las condiciones que se esperan una vez creada la empresa.
- Para definir el nombre de la nueva empresa de servicios de ciberseguridad se requiere un análisis e investigación para encontrar el ideal y libre, lo cual no fue cubierto en el presente escrito.
- Para el análisis y desarrollo del presente escrito se utilizaron los modelos tradicionales como 5 fuerzas de porter, análisis FODA, Business Model Canvas, entre otros.
- La definición de precios fue establecida con pocos elementos, como el costo por hora de un ingeniero especializado y el tiempo invertido en cada actividad, es por ello que se requiere una investigación más profunda para mejorar de ser necesario la tabla de precios.
- En el trabajo no se alcanzó a cubrir pruebas y prototipos de funcionamiento de los servicios, por lo cual a pesar de estar claros en su descripción requieren de una validación y puesta en marcha en escenarios de prueba.

12.2 Recomendaciones

- Realizar ejercicios de proyección y evaluación financiera en escenario pesimista y optimista.
- Profundizar en la definición de precios derivado de los comentarios resultantes durante las entrevistas, esto con el fin de establecer el mejor precio.
- Analizar y evaluar el caso de estudio *Is Porter 's Five Forces Framework Still Relevant? A study of the capital/labour intensity continuum via mining and IT industries* de Technology Innovation Management Review como modelo alternativo al tradicional y más enfocado en industrias de TI.
- Realizar más entrevistas a prospectos de cliente para una muestra más grande.
- Explorar y evaluar ampliar el catálogo de servicios derivado de los comentarios recibidos durante las entrevistas realizadas a expertos de la industria.
- Evaluar un escenario donde se combine capital de los socios con un crédito bancario para beneficiarse de las deducciones de impuestos.
- Evaluar un escenario donde se integre a un tercer socio para amortiguar el riesgo que representa una inversión.
- Se recomienda realizar el análisis FODA nuevamente una vez creada la empresa y operando para tener una actualización y con base en la información resultante adecuar estrategia de ser necesario.
- Realizar un *benchmarking* de los competidores actuales para entender más a profundidad su propuesta, así como, extender la lista de competidores.
- Realizar pruebas y laboratorios de todos los servicios del catálogo en otra fase fuera de este proyecto.

Entiendo las limitantes y el trabajo que queda por realizarse se podría emitir como recomendación final desde la perspectiva del análisis financiero es invertir en el proyecto, si bien se trata de un ejercicio de pronósticos permite tener una referencia de cómo podría comportarse los ingresos y egresos de la empresa, resultando en un negocio atractivo para invertir con una TIR de 44% al final de los 3 primeros

años de operación. Existe aún trabajo por mejorar en cuanto a costos debido a que los precios están basados en precio lista y es muy probable que una vez operando se logren acuerdos con precios más accesibles con proveedores o canales.

13. Conclusiones

De acuerdo con los objetivos definidos al inicio del presente trabajo, en la sección 3, puedo concluir que se cumplieron conforme a lo planeado, es decir, a pesar de ser objetivos ambiciosos se logró cubrir su contenido y obtener la información deseada en cada uno de ellos. Es posible decir que, de acuerdo con la metodología propuesta por la coordinación de la maestría en Gestión de la Innovación Tecnológica también fue aplicada y seguida en todas sus secciones y cubiertas en cuanto a su contenido.

Con respecto al objetivo general "*Desarrollar y diseñar un caso de negocio sobre una empresa nueva de servicios de ciberseguridad orientada a Pymes de la zona metropolitana de México que permita analizar aspectos de mercado, evaluación financiera, entorno e industria, así como oferta de servicios y se pueda ejecutar a partir en el transcurso de un año*." se puede concluir que se logró contar con un caso de negocio terminado, ya que se realizó un análisis de mercado en la sección 4 por medio del modelo cuadrícula de expansión Producto - Mercado y el modelo de TAM, SAM y SOM, así como una descripción del tipo de Pymes que son susceptibles a requerir servicios de ciberseguridad.

En cuanto a la evaluación financiera se realizó un ejercicio de proyección de ventas, definición de precios, asignación de presupuestos para la implantación y operación de los 3 primeros años de la nueva empresa de ciberseguridad, con los cuales se tiene una referencia de cómo podrían comportarse los ingresos y egresos de la nueva empresa. No obstante, hace falta explotar más escenarios y variables para diseñar planes de contingencia en caso de una desviación en las finanzas.

Finalmente para el objetivo general se analizó el entorno e industria en el cual competirá la nueva empresa, esto es, una breve descripción de los competidores actuales, sus características y la oferta para así buscar diferenciar el servicio a ofrecer. A pesar de que se cumplió el objetivo, muchos de estos análisis e investigaciones no son trabajos de una sola vez. Tal como se mencionó en las recomendaciones es vital realizar un *benchmarking* más profundo. Esto con el fin de afinar y apuntalar aún más la propuesta de valor, o sea, esa característica que diferenciará a la nueva empresa del resto que tienen más tiempo en el mercado.

Retomando los objetivos específicos tenemos que, para el objetivo 1 "*Describir cada uno de los servicios a ofrecer, así como su alcance y responsabilidades del cliente y proveedor.*" se describió el catálogo de servicios con alcances y responsabilidades de cliente y proveedor de los 5 servicios a ofrecer durante la sección 8.1 Propuesta de catálogo de servicios, así como los problemas que ayudarían a solventar. El catálogo quedó conformado por estos 5 servicios; Diagnóstico de nivel de madurez en ciberseguridad, Implementación de consola de antivirus y endpoint, Gestión de consola de antivirus y endpoint, Capacitación en ciberseguridad, Consultoría en implementación y cumplimiento de estándares de seguridad. Con esto se cuenta con una primera propuesta de catálogo, pero es importante entender que es un documento vivo y se debe revisar periódicamente, así como, escuchar constantemente al cliente y al mercado para adaptar la propuesta de ser necesario.

El objetivo 2 "Identificar el perfil y tipo de Pyme, así como sus características y tamaño de mercado objetivo." Fue cubierto en la sección 5 y 10 donde se detalló el tipo de Pyme que se busca atender y por medio de entrevistas comprobar aspectos del modelo de negocio propuesto. Se cuenta con una aproximación muy concreta del tipo de empresa que se beneficiarían de la oferta de servicios de ciberseguridad, el reto es persuadirlo de los riesgos actuales que representan los ciberataques y sus impactos en la operación del negocio, así como, crear conciencia de que no es un asunto ajeno a ellos y todas las organizaciones y personas que están conectas y poseen datos digitales están expuestas a los ciberataques. Pyme es una clasificación muy amplia y general, por lo cual tomó mucha relevancia acotar en estas secciones las características específicas de Pymes que podrían requerir servicios de ciberseguridad, es decir, probablemente un restaurante con 25 empleados y 5 equipos de cómputo no necesariamente sería el candidato ideal para realizar una inversión en servicios de ciberseguridad, por el contrario un *call center* con 50 posiciones de trabajo y algunos servidores sí serían un prospecto

más aproximado al perfil de Pyme que requeriría dichos servicios, en otras palabras, se trata de Pymes con procesos digitales y un aproximado de 25 dispositivos o equipos de cómputo conectados a una red.

Para el objetivo 3 “Evaluar viabilidad financiera como proyecto de inversión para la creación de una empresa de ciberseguridad enfocada en Pymes.” En la sección 10 se realizó un ejercicio de proyección de ventas y gastos arrojando resultados atractivos a la inversión como son una TIR de 44%, un VPN de $1,955,178.00 con una tasa de descuento del 20%. El escenario actual es una proyección de cómo podrían comportarse los flujos, sin embargo, para tomar decisiones sobre inversión se requiere conocer al menos 2 escenarios más, que serían el mismo ejercicio pero con ventas proyectadas de forma optimista y pesimista. También se podría ajustar variables como precio, promociones y descuentos, costos, etc.

Adicionalmente se puede afirmar que con los modelos teóricos usados se logró desarrollar información valiosa para analizar y llevar las soluciones propuestas a una validación con expertos y prospectos de clientes quienes brindaron ideas nuevas en cuanto a precios, ideas de más *pains* que atender, así como recomendaciones puntuales que fueron detalladas en la sección 9 Proceso de validación. Con base en análisis FODA proyectado, se tiene claro qué aspectos se tendrá que trabajar desde el día uno de operación, por ejemplo, en debilidades tenemos que al ser una marca nueva su reconocimiento será nulo y sport eso que parte de la estrategia general es generar un presupuesto para actividades de mercadotecnia como campañas en redes sociales, imagen y logo de la marca, entre otras. En este mismo sentido la cartera de clientes podría ser limitada, es por ello que también se presupuesto una bolsa para vendedores y gastos de representación que en conjunto con la mercadotecnia permitirá romper con esta barrera de ser desconocidos.

Con base en la información presentada acerca de las principales tendencias digitales y considerando que estas van a la alza en cuanto a adopción, resulta en una enorme oportunidad para la ciberseguridad ya que representa un mercado en crecimiento. La ciberseguridad recientemente se está tomando más en serio y viendo como una prioridad en las agendas de las empresas. Los mercados en crecimiento y en sus primeras etapas resultan más atractivos para invertir. También representa un enorme reto seguir el paso de las nuevas amenazas y modalidades de ciberataques, pero justo por eso es importante diseñar una estrategia de ciberseguridad adecuada.

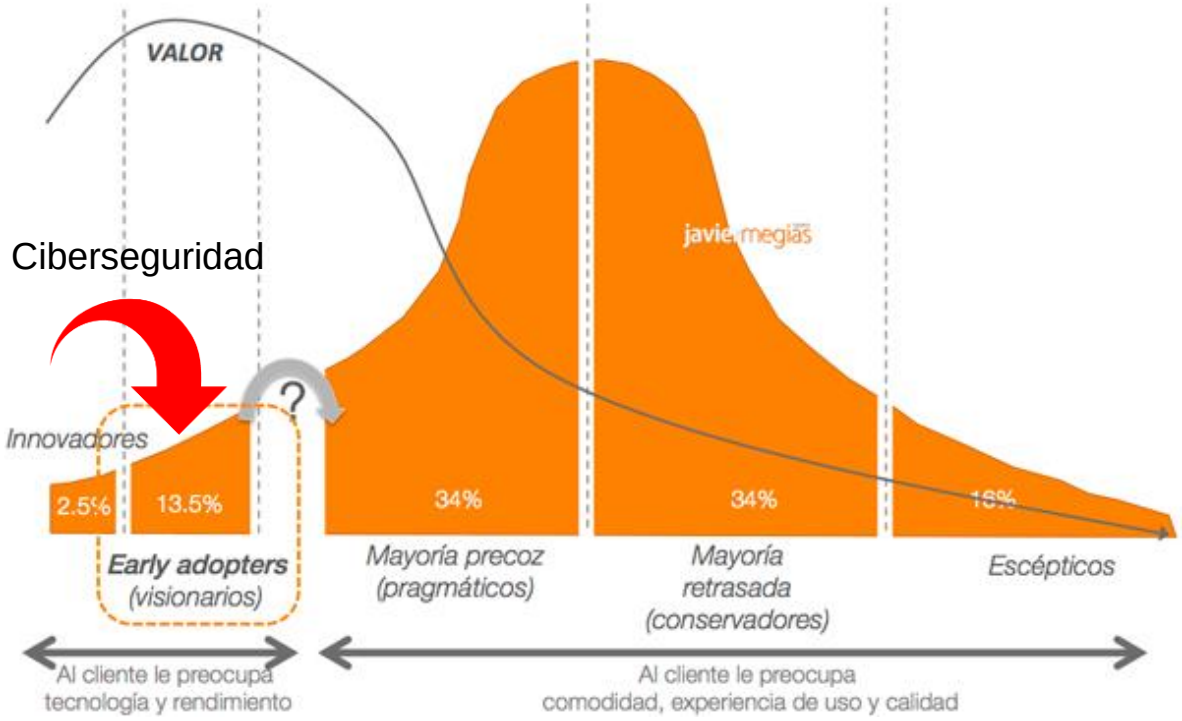
El día de hoy es el mejor momento para iniciar el trayecto hacia la ciberseguridad, no solo desde una perspectiva de negocio, sino en todos los aspectos, como usuario, como cliente que entrega datos personales a empresas, como empleado de una empresa y responsable de información de clientes, proveedores, socios, etc.

13.1 Reflexiones finales

Lo que se buscó con el presente trabajo, es contar con un caso de negocio que ayude a integrar información sobre mercado, validación de alternativas de solución, precios, industria y tendencias de ciberseguridad, entre otros aspectos, ya que cuando se trata de inversiones y de innovar en un producto o servicio se debe considerar el cómo y para qué se pretende ejecutar determinado proyecto, de lo contrario se podría poner en riesgo capital propio o ajeno (crédito) con iniciativas poco estudiadas. Es por ello que, este trabajo me ayudó a cuestionar esos aspectos y entender que aún falta profundizar en algunos de ellos, como es, esa comparativa con los competidores actuales, más escenarios financieros, reflexionar si es necesario integrar a todo el personal desde el día uno de operación, ya que a pesar de que se estimaron un par de meses sin ingresos y costos corriendo, esto podría dificultar la solvencia económica.

Desde una perspectiva de innovación tecnológica, me doy cuenta de que, si se tratara de ubicar la ciberseguridad en una curva de adopción exclusivamente para Pymes de México, se podría decir que se encuentra en la fase de *Early adopters*, esto quiere decir que es una etapa en la cual se podría percibir mayor valor de los servicios de ciberseguridad y los clientes que adopten los servicios podrían aprovecharla como una ventaja competitiva. La curva que estoy imaginando con base en lo estudiado y evaluado en este trabajo, se vería de la siguiente forma:

Figura 41. Curva de adopción tecnológica para ciberseguridad en Pymes de México



(Megias, 2012)

La flecha roja del lado izquierdo de la figura 41 indica en qué fase de la curva de adopción tecnológica se encontrarían los servicios de ciberseguridad, esto exclusivamente para Pymes de México, ya que como se ha descrito a lo largo del documento, las grandes empresas son las que actualmente realizan mayores esfuerzos en esta materia, mientras que, para las Pymes aún representa un reto hacerlas conscientes de los riesgos que representan los ciberataques y la importancia de la ciberseguridad. En la misma gráfica se muestra una línea gris empieza en la parte superior izquierda de la figura y termina en la parte inferior derecha, la cual representa el valor generado en este caso por los servicios de ciberseguridad.

Finalmente, quiero mencionar que un sector de tecnología tan cambiante y acelerado podría ser conveniente adoptar la tecnología en sus primeras fases, ya que en esta era de transformación digital representaría quedar completamente fuera de combate sin procesos digitales y sin protección de ellos.

14. Referencias

Baca Urbina, G. (2011). *FUNDAMENTOS DE INGENIERÍA ECON*. McGraw-Hill Interamericana de España S.L.

Dynamic. (2020). ▷ TAM SAM SOM. Explicado al detalle. Guía definitiva en 2022. Dynamic. Retrieved November 22, 2022, from https://www.dynamicgc.es/tam-sam-som-calculemos-el-tamano-del-mercado/

Endeavor & Paypal. (2020). Panorama del ecosistema de ciberseguridad. 2022, de Endeavor Sitio web: *https://public.tableau.com/views/DashboardCiberseguridad/Menu?:language=es&:embed=y&:embed_code_version=3&:loadOrderID=0&:display_count=y&:origin=viz_share_link*

EY & Kio Networks & Needed Education. (2020). Informe de madurez digital en México 2020-2021. 2022, de Needed Education Sitio web: *https://needed.education/informe-madurez-2021/*

Forbes staff (2021). México, primer lugar en ciberataques en Latinoamérica. *Forbes México. https://www.forbes.com.mx/negocios-mexico-primer-lugar-en-ciberataques-en-latinoamerica/*

Forbes staff (2021). Cada minuto se producen 299 intentos de ciberataques en México. *Forbes México. https://www.forbes.com.mx/cada-minuto-se-producen-299-intentos-de-ciberataques-en-mexico/*

Infosecurity México, (s.f.). Ciberseguridad. Una guía completa del concepto, tipos, amenazas y estrategias. *https://www.infosecuritymexico.com/es/ciberseguridad.html*

FortiGuard Labs presenta reporte de ciberataques en América Latina. (2022, February 8). Fortinet. Retrieved November 22, 2022, from https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-reporte-ciberataques-america-latina-2021

Gustafsson, P. (2021, septiembre 29). *4 estrategias de ciberseguridad para pequeñas y medianas empresas*. Harvard Business Review. Retrieved November 23, 2022, from https://hbr.org/2021/09/4-cybersecurity-strategies-for-small-and-midsize-businesses?language=es

Herrera Mendoza, A. (2022, Agosto 18). *LINEAMIENTOS OTOÑO 2022 [PROYECTO DE VINCULACIÓN INDUSTRIAL].* Universidad Iberoamericana, CDMX, México

LAS 5 TENDENCIAS DIGITALES QUE MARCARÁN EL 2021. (2020, December 14). Revista Logistec. Retrieved November 21, 2022, from https://www.revistalogistec.com/logistica/global-2/3156-las-5-tendencias-digitales-que-marcaran-el-2021

Lefferts, R. (2021, May 11). *Gartner names Microsoft a Leader in the 2021 Endpoint Protection Platforms Magic Quadrant*. Microsoft. Retrieved November 23, 2022, from https://www.microsoft.com/en-us/security/blog/2021/05/11/gartner-names-microsoft-a-leader-in-the-2021-endpoint-protection-platforms-magic-quadrant/

Losing Paradise. (2012, October 29). YouTube. Retrieved November 22, 2022, from https://pwebebsco.ibero.elogim.com/ehost/detail/detail?vid=5&sid=e0e5d291-4cbe-4fab-ae76-8e72aa0273c2%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#AN=131330503&db=a9h

Megias, J. (2012, December 18). *Early adopters: la clave al lanzar un nuevo modelo de negocio | Startups, Estrategia y Modelos de negocio*. Javier Megias. Retrieved December 12, 2022, from https://javiermegias.com/blog/2012/12/early-adopters-clave-nuevo-modelo-de-negocio-curva-adopcion-tecnologia/

National Cybersecurity Alliance (2020, september 3). Case 3: Stolen Hospital Laptop Causes Heartburn. Retrieved November 30, 2022, from https://www.nist.gov/system/files/documents/2020/09/30/Cybersecurity-Case-3.pdf

Ovans, A. (2015, January 23). *What Is a Business Model?* Harvard Business Review. Retrieved November 22, 2022, from https://hbr.org/2015/01/what-is-a-business-model

¿Qué es la ciberseguridad? (n.d.). IBM. Retrieved November 22, 2022, from https://www.ibm.com/mx-es/topics/cybersecurity

¿Qué es un ataque cibernético? (n.d.). IBM. Retrieved November 22, 2022, from https://www.ibm.com/mx-es/topics/cyber-attack

Rash, W., & Maguire, J. (2018, August 18). *New U.S. Law Directs NIST to Provide Cyber-Security Resources to SMBs*. eWeek. Retrieved November 23, 2022, from https://www.eweek.com/security/nist-to-provide-cyber-security-advice-to-smbs-under-new-federal-law/

14. Anexos

14.1 Anexo 1 Entrevista con experto 1 (Perfil de implementador)

Fecha: 2 de noviembre de 2022
Tiempo de experiencia en la industria: 12 años
Nombre del entrevistado: Ana Laura Dominguez
Carga o puesto actual: Consultor de implementación Sr.
Edad: 38 años
Empresa: Empresa mexicana de Tecnología

1. **¿Qué tan importante consideras la ciberseguridad en las organizaciones de México?**

Es relevante, es alta, crítica, la tecnología ha evolucionado demasiado rápido de 20 años para acá, también ha evolucionado la forma en que se puede atacar, por eso es importante que las organizaciones, personas, gobiernos y empresas privadas protejan su información.

2. **¿Quién o quienes crees que deberían preocuparse por la ciberseguridad?**

Gobierno, sino lo hace está condenado a queno puede generar confianza, el nivel de protección no solo es físico o nivel demográfico,
bancos, la preocupación debe ser al 100% ya que maneja datos muy sensibles, pero también la gente que trabaja en entidades de gobierno y bancos, deben ser conscientes de la importancia de los datos que manejan, no solo los propios.
Pero también todos, o sea a nivel familiar, esto no es ajeno, esto no me va a pasar a mi, eso debe quedar atrás, debemos tener cuidado, proteger nuestros dispositivos, conversaciones, no hablar de más, etc.

3. **¿Desde tu perspectiva consideras que la ciberseguridad debería ser importante para las Pymes?**

Sí, la ciberseguridad debe ser importante para cualquier organización, lugar, persona, etc.

4. **¿Qué tipo de empresas son tus principales clientes?**

Casi todas apuntan a bancos. Siempre he tenido bancos para desplegar seguridad perimetral y últimamente todo está apuntando a la nube, pero sigue siendo lo mismo, protección perimetral, aunque también me ha tocado atender afores, tiendas departamentales, que son las que le meten más a la protección de datos.

5. **¿Qué características tienen estas empresas?**

Mercado de comercio electrónico y observo que tratan de cumplir con estándares como ISO o auditorías, supongo que siempre apuntan a la protección de la información por cumplimiento, como PCI, para obtener permisos para poder operar, tengo duda de que si no existiera esa necesidad de cumplimiento de estándar de verdad se procuparían y atenderían la ciberseguridad, quiero pensar que sí.

6. **¿Consideras que las empresas están haciendo los esfuerzos necesarios para proteger sus activos digitales?**

Sí y a la vez no, solo las empresas muy grandes lo están haciendo, o sea bancos grandes y los pequeños solo lo mínimo, es decir de panzazo. Los bancos grandes tratan de educar a los trabajadores y han invertido mayor presupuesto, pero creo que menos porcentaje son quienes sí tratan de tratan de cumplir que los que no han hecho nada, probablemente porque no les ha tocado ningún robo de información.

7. **¿Te ha tocado atender y contener alguna vez un ciberataque?**

En mi experiencia no, porque siempre he estado en un nivel transitorio, solo entrego proyecto a operaciones, pero sí me ha tocado escuchar de ataques que han sufrido los clientes y que se han contenido por parte del SOC.

8. **¿Qué tipo de ciberataques te ha tocado contener?**

Ransomware, algunas veces ha sido exitoso y otras no, como 10, denegación de servicio y phishing también he escuchado
La ingeniería social es tan relevante que en HSBC lo ejecutan como prueba para identificar vulnerabilidades, montaban una escena, o sea como una simulación para poner a prueba al personal de TI y de seguridad física, se hacían pasar por alguien externo y veían hasta dónde podían llegar.

9. **¿Qué tipo de organizaciones consideras que son las más vulnerables ante un ciberataque?**

Gobierno, cualquier institución pública, no tienen la tecnología que se requiere y minimizan el esfuerzo que requiere la ciberseguridad.

10. **¿Consideras que las Pymes cuentan con las medidas necesarias en cuanto a protección de datos?**

Sí, intentan cumplir, existen esfuerzos, pero falta mucho camino, se necesita un CISO y área de ciberseguridad, asegurar los procesos y el cumplimiento, no basta poner un firewall. Se necesita un análisis más allá de ponerlo.

11. **De acuerdo con tu experiencia ¿Cómo ves la tendencia y comportamiento de los ciberataques?**

Tiende a crecer de manera exponencial, está creciendo la forma de la presentación de la información y la tendencia es en la nube. La nube apenas está empezando a atender la seguridad, por ejemplo SAAS no ofrece garantía de seguridad. Existe bastante mercado. No va a parar, ahora todo es digital.

12. **¿Consideras que hace falta capacitación en ciberseguridad?**

Sí, falta mucho, ¡demasiado! que, a nivel empresas intenten educar a las personas, no compartir datos, cuidar contraseñas, en un nivel técnico se necesita conocimiento calificado, pero también todo el personal debe entender algo de ciberseguridad.

13. **¿Consideras que existe mercado de ciberseguridad para Pymes?**

Si creo que invertirán en ciberseguridad, existe mercado, pero deben tener conciencia de ciberseguridad. Es un must, no se requiere una millonada, se tiene que empezar por sensibilizar y educar, la inversión en tecnología no es suficiente.

14.2 Anexo 2 Entrevista con experto 2 (Perfil de gerente de monitoreo)

Fecha: 7 de noviembre de 2022
Tiempo de experiencia en la industria: 2 años en ciberseguridad y 10 años en infraestructura
Nombre del entrevistado: Erick Ortega
Carga o puesto actual: Manager de *Data Loss Protection* DLP
Empresa: Empresa de industria automotriz con presencia en México

1. **¿Qué tan importante consideras la ciberseguridad en las organizaciones de México?**

Sumamente importante para empresas grandes, pero para pymes es muy distinto, ya que la solución es muy costosa, la cultura es muy pobre con respecto a la ciberseguridad, tienen otras preocupaciones antes.

2. **¿Quién o quienes crees que deberían preocuparse por la ciberseguridad?**

Todas las organizaciones tanto públicas como privadas, generalmente se asigna la responsabilidad al área de TI, pero es un tema compete a control interno, RH, temas regulatorios y todas las áreas de la empresa porque al final de dia, para tener una buena ciberseguridad debes ser invasivo, corresponsal desde todos los ángulos.

3. **¿Desde tu perspectiva consideras que la ciberseguridad debería ser importante para las Pymes?**

Sí totalmente, por dos factores, los intereses propios de la empresa, todo es digital y compartido y debes cuidar de esos activos, pero toda organización maneja datos de proveedores y clientes y por regulación debe hacer un manejo de datos de terceros. No hay mucha cultura de ciberseguridad y se necesita permear.

4. **¿Qué tipo de empresas son tus principales clientes?**

Empresas más robustas, o sea empresas grandes que tienen una visión más amplia y asociada a su estrategia, logran integrar la ciberseguridad con su estrategia general.

5. **¿Qué características tienen estas empresas?**

Reputación que cubrir, o sea que tienen inversiones importantes, están en crecimiento e intereses grandes.

6. **¿Consideras que las empresas están haciendo los esfuerzos necesarios para proteger sus activos digitales?**

Se está empezando a tener conciencia, pero no va a la misma velocidad que los ciberataques.

7. **¿Te ha tocado atender y contener alguna vez un ciberataque?**

Estoy en una área de monitoreo de adentro hacia afuera, para evitar que se extraiga información, por eso a veces es difícil distinguir cuando es un robo de información o es parte de la operación. Pero a nivel empresa el ataque ransomware nos tocó, no lo atendí directamente, pero escuche de cerca que fueron afectadas algunas computadoras y fueron contenidas, o sea no pasó a mayores y solo se quedó en esas computadoras.

8. **¿Qué tipo de ciberataques te ha tocado contener?**

Ransomware “WannaCry”

9. **¿Qué tipo de organizaciones consideras que son las más vulnerables ante un ciberataque?**

Organizaciones expuestas en sector gobierno, no cuentan con esquemas robustos de ciberseguridad. No están preparados y no cuentan con una buena estrategia proactiva.

10. **¿Consideras que las Pymes cuentan con las medidas necesarias en cuanto a protección de datos?**

La respuesta es no, no la hay y menos en los últimos 2 años, su prioridad es pasar los efectos post pandemia y recuperarse económicamente.

11. **De acuerdo con tu experiencia ¿Cómo ves la tendencia y comportamiento de los ciberataques?**

Estamos tratando de tapar el sol con un dedo, las empresas apenas pueden hacer esfuerzos mínimos por tratar de cumplir, pero los ciberataques van más rápido que la ciberseguridad.

12. **¿Consideras que hace falta capacitación en ciberseguridad?**

Sí, del 100% de ciberataques un porcentaje grande empiezan con temas de phishing y desde dentro de las organizaciones.

13. **¿Consideras que existe mercado de ciberseguridad para Pymes?**

Si hay mercado, ¡totalmente! El reto es encontrar una solución balanceada entre costo y eficiencia para las Pymes.

14.3 Anexo 3 Entrevista con experto 3 (Perfil académico)

Fecha: 8 de noviembre de 2022
Tiempo de experiencia en la industria: 15 años
Nombre del entrevistado: Miguel Angel López
Carga o puesto actual: Jefe de sección de infraestructura
Edad: 40 años
Empresa en la que trabaja: Universidad Mexicana

1. **¿Qué tan importante consideras la ciberseguridad en las organizaciones de México?**

Muy importante porque ahora todo está en internet, es un mundo digital, con la pandemia todo fue remoto y acceder a sistemas desde fuera, el reto se hizo mayor para cada institución. Al estar en internet todo está expuesto.

2. **¿Quién o quienes crees que deberían preocuparse por la ciberseguridad?**

Todos, gente de casa, directivos que deben velar por la seguridad de la información de la organización.

3. **¿Desde tu perspectiva consideras que la ciberseguridad debería ser importante para las Pymes?**

Sí y revisar cual es core o núcleo de negocio y en función de eso revisar su estrategia de ciberseguridad.

4. **¿Qué tipo de empresas son tus principales clientes?**

No he tenido empresas como clientes, ya que estoy trabajando en una universidad, mis clientes son usuarios internos o sea los alumnos y maestros.

5. **¿Qué características tienen estas empresas?**

No he tenido empresas como clientes, pero supongo que todas las empresas deberían preocuparse.

6. **¿Consideras que las empresas están haciendo los esfuerzos necesarios para proteger sus activos digitales?**

Pienso que sí y todo mundo en medida de sus posibilidades lo están haciendo. Los hacen darse cuenta que a todos les puede pasar.y no son ajenos al riesgo de ciberataques.

7. **¿Te ha tocado atender y contener alguna vez un ciberataque?**

Sí, alguno durante el monitoreo de los sistemas y minimizando el impacto, con un servidor apache de un usuario que no cambió las credenciales por default y alguien entró, lo que se hizo fue bajar el servidor, reinstalarlo y cambiar las credenciales en el nuevo.

8. **¿Qué tipo de ciberataques te ha tocado contener?**

Antes de la pandemia se tenía el correo local o sea en nube privada, el phishing era casi de todos los días, estar alertando y eliminando el correo no deseado.

9. **¿Qué tipo de organizaciones consideras que son las más vulnerables ante un ciberataque?**

Todas las empresas, depende del actor malicioso, el sector financiero podría estar más protegido y pudieran no intentarlo los delincuentes, pero nadie se salva.

10. **¿Consideras que las Pymes cuentan con las medidas necesarias en cuanto a protección de datos?**

Pienso que sí y deberían, ya no pueden quedarse atrás, no pueden pensar que no les va a pasar a ellos.

11. **De acuerdo con tu experiencia ¿Cómo ves la tendencia y comportamiento de los ciberataques?**

Están aumentando, cada día se detecta una nueva vulnerabilidad, se filtran datos. No creo que esto pare, es la lucha del bien contra el mal y así seguirá en adelante.

12. **¿Consideras que hace falta capacitación en ciberseguridad?**

Sí a todos los niveles, concientización de los usuarios, empresas, usuarios, familias, etc.

13. **¿Consideras que existe mercado de ciberseguridad para Pymes?**

Sí, seguramente sí, es una carrera de hoy y el futuro

14.4 Anexo 4 Entrevistas con prospecto de cliente 1

Fecha: 4 de noviembre de 2022
Nombre del entrevistado: Daniel del Real
Puesto o cargo dentro de la organización: Administrador de infraestructura y ventas
Años en el puesto: 5
Número aproximado de empleados en la organización: 40
Número aproximado de equipos de cómputo: 30
Nombre de la organización: Deposito Dental

Giro de la organización: Venta de productos médicos dentales

1. **¿Has escuchado acerca de algún ciberataque en los últimos 3 meses?**

Si el ataque contra la SEDENA, el cual fue público en diversos medios de comunicación, demostrando que cualquier empresa o entidad de gobierno está expuesta a ataques.

2. **¿Tu organización ha sido víctima de algún ciberataque?**

Si, se ha tenido equipos de cómputo contaminados con virus, los cuales provocan que alguna terminal sea inaccesible, la mayoría de estos ataques se ha debido a desconocimiento de uso de procedimientos de seguridad, por ejemplo, uso correcto de los navegadores web, uso de dispositivos extraíbles y acceso a los equipos vía inalámbrica ya sea por bluetooth o wifi.

3. **¿Qué tan familiar te resulta el término de ciberseguridad?**

Me siento familiarizado con el tema, ya que sé que existe el robo de información, alterar la información, secuestro de la información o inclusive destrucción de la misma.También estoy consciente de que existen diversos métodos para realizar ataques, remotamente, por medio de visitas a sitios inseguros o de las mismas personas que trabajan en la organización de manera interna.

4. **¿Qué tan familiarizado te consideras con los impactos de un ciberataque?**

Creo que familiarizado, estoy consciente de que se puede perder información de manera parcial o total, tener información alterada la cual impacte el correcto funcionamiento de las ventas. En caso extremo sé que también pueden existir disrupciones a la operación en caso de un ataque mayor.

5. **¿Qué tan importante consideras los sistemas e información digital para la operación del negocio?**

Muy importante, actualmente en el depósito más del 90% de las operaciones ocurren de manera digital, altas y bajas en los inventarios, pagos a proveedores y a empleados, si bien se considera un negocio mediano, es muy difícil a esta alturas imaginar su funcionamiento sin equipos y sistema de ventas y nómina.

6. **¿Qué tanto consideras que tu organización se preocupa por la ciberseguridad?**

Considero que es un tema que es importante pero no está en las prioridades de la empresa, ya que solo se actúa de manera básica (antivirus), contraseñas y esos controles que realmente están implementados de manera implícita en la seguridad en la mayoría de las empresas. Se da más prioridad al proceso de movimiento de inventarios y de ventas que a la seguridad.

7. **¿Consideras que tu organización hace lo necesario para proteger sus activos digitales?**

Hace lo básico, prácticamente porque los mismos sistemas así lo requieren. Acceso al sistema de ventas con contraseña, correo electrónico y a los equipos de cómputo. Solo personal autorizado tiene acceso a los equipos de cómputo. Considero que se puede mejorar

8. **¿Tu organización cuenta con protocolos de cómo actuar ante un ciberataque?**

Cuenta con los protocolos básicos sin tener nada por escrito, entre ellos.
-El personal está informado que debe de cerrar las sesión tanto del sistema como de las terminales de cómputo.
-Se tiene prohibido extraer información de la empresa ya sea vía correo o por medio de medios extraíbles.
-Se tiene prohibido el acceso a sitios de internet que pongan en riesgo la integridad de la información.

9. **¿Cuentan con mecanismos de recuperación ante pérdida de información o interrupción de negocio?**

Se cuentan con respaldos del inventario de manera semanal y mensual, en la cual se reportan las ventas y las compras realizadas, esto se hace por medio del mismo software de ventas.

10. **¿La organización cuenta con algún presupuesto para ciberseguridad y qué porcentaje aproximado?**

No está determinado en los presupuestos anuales, pero podrían considerarse la renovación del soporte de software y la renovación de los antivirus en las terminales y servidores.

11. **¿Considerarías contratar servicios de ciberseguridad para proteger tus activos digitales?**

Se tiene contratado antivirus y cámaras de seguridad, sin embargo, no se ha realizado un estudio a profundidad para reforzar los diferentes sectores de la empresa.

12. **Por la naturaleza de sus operaciones, ¿Tienen la necesidad de cumplir con algún estándar de ciberseguridad?**

No se tienen determinados o por escrito los estándares de seguridad de activos digitales, no se cuenta con algún acuerdo ya sea con los clientes o con los proveedores para cumplir alguna norma que no sea fiscal.

13. **¿Estarías dispuesto a pagar estos precios por los siguientes servicios?**

El de diagnóstico y capacitación me parece que serían más atractivos si fueran más baratos y el de implementación y gestión considero que hasta podrían ser más altos.

14.4 Anexo 4 Entrevistas con prospecto de cliente 2

Fecha: 5 de noviembre de 2022
Nombre del entrevistado: Jesús Teacalco
Puesto o cargo dentro de la organización: Gerente comercial
Años en el puesto: 5
Número aproximado de empleados en la organización: 30
Número aproximado de equipos de cómputo: 45
Nombre de la organización: Comercializadora de productos médicos y lácteos
Giro de la organización: Venta de productos médicos y lácteos

1. **¿Has escuchado acerca de algún ciberataque en los últimos 3 meses?**

Si, en el gobierno, el de la SEDENA, no se bien como estuvo pero al parecer hubo robo de información.

2. **¿Tu organización ha sido víctima de algún ciberataque?**

No, que yo sepa, pero sí han llegado mails (phishing) diciendo que entres a algun link y hagas tal cosa

3. **¿Qué tan familiar te resulta el término de ciberseguridad?**

Muy poco, la verdad.

4. **¿Qué tan familiarizado te consideras con los impactos de un ciberataque?**

Que pueden obtener acceso a información y de ahí pudiera ser información bancaria.

5. **¿Qué tan importante consideras los sistemas e información digital para la operación del negocio?**

Podrían continuar sin los sistemas pero tomaría un tiempo organizarnos para continuar con las operaciones.

6. **¿Qué tanto consideras que tu organización se preocupa por la ciberseguridad?**

Casi no, como solo tengo una persona para el mantenimiento de los equipos, instala antivirus, administra el correo y nos da algunas alertas

7. **¿Consideras que tu organización hace lo necesario para proteger sus activos digitales?**

No estoy seguro, pensaría que sí.

8. **¿Tu organización cuenta con protocolos de cómo actuar ante un ciberataque?**

No, desconocemos que haríamos en dado caso.

9. **¿Cuentan con mecanismos de recuperación ante pérdida de información o interrupción de negocio?**

No, solo manejamos algunos archivos de excel

10. **¿La organización cuenta con algún presupuesto para ciberseguridad y qué porcentaje aproximado?**

Si, solo una persona que ayuda con el antivirus y mantenimiento a los equipos, también lleva el correo de la empresa y nos avisa de alertas y correos que no debemos abrir.

11. **¿Considerarías contratar servicios de ciberseguridad para proteger tus activos digitales?**

Si, ahora que lo veo sí debería.

12. **Por la naturaleza de sus operaciones, ¿Tienen la necesidad de cumplir con algún estándar de ciberseguridad?**

No.

13. **¿Estarías dispuesto a pagar estos precios por los siguientes servicios?**

En este momento no los entiendo bien, pero el precio parece razonable para estar más protegido.