UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE INGENIERÍA INDUSTRIAL

PLAN DE NEGOCIOS CONSULTORA DE CIBERSEGURIDAD PARA PyMES CHILENAS

TESIS PARA OPTAR AL GRADO DE MAGÍSTER EN GESTIÓN Y DIRECCIÓN DE EMPRESAS

LEONARDO ANDRÉS CALFUMIL VARGAS

PROFESOR GUÍA:
MANUEL RODRIGO VERGARA TRINCADO

MIEMBROS DE LA COMISIÓN:
ANTONIO AGUSTÍN HOLGADO SAN MARTÍN
WLADIMIR FRANCISCO REYES MUÑOZ

SANTIAGO DE CHILE
2022

RESUMEN

PLAN DE NEGOCIOS CONSULTORA DE CIBERSEGURIDAD PARA PyMES CHILENAS

En los últimos años el escenario empresarial cambió, los clientes evolucionaron en sus necesidades y cada vez los canales remotos de atención, las aplicaciones , los sitios web son más relevantes para el funcionamiento de las empresas, por lo que hoy es difícil pensar en una que no use tecnología para su funcionamiento, si bien esto genera enormes oportunidades de desarrollo y expansión de negocios, también abre la puerta a los ciberdelincuentes y desde aquí nace la interrogante ¿Están preparadas las pequeñas y medianas empresas para enfrentar un ciberataque? De acuerdo con el estudio de "Estado de ciberseguridad 2020" realizado por Entel a negocios chilenos, un 43,3% de las Pymes en Chile no está consciente de los riesgos a nivel de ciberseguridad que corren diariamente y un 27% no hace nada para resguardarse, incluso si ya han sido atacadas.

En este contexto y dada la escaza oferta actual dirigida a las Pymes de Chile es que se plantea el objetivo de crear una consultora centrada en entregar soluciones adaptadas a las necesidades de este tipo de empresas, Consiguiendo una rentabilidad sobre el 50% en un plazo de 5 años.

Para esto se realizó un plan de negocios que abarcó la evaluación del contexto de la ciberseguridad en Chile y las necesidades de las pymes en este ámbito, que, sumado al robustecimiento de las leyes y aumento del cibercrimen, permiten identificar un mercado atractivo, por otra parte, las bajas barreras de entrada para empresas tecnológicas podrían generar la aparición de nuevos competidores.

Se diseñó una plan estratégico que apunta a conseguir el mejor producto(de acuerdo con el modelo de Arnoldo Hax), para el que se realizó la evaluación económica en 3 escenarios posibles, obteniendo como resultado un VPN de $12.816.115; considerando una tasa de descuento de un 24,79% y una TIR de 57%, con un *payback* de 2 años en un escenario probable, en el escenario pesimista el invertir en este negocio es indiferente ya que no tendría el resultado esperado, pero no generaría perdidas, por lo tanto, se convierte en una buena oportunidad de negocio, considerando el tamaño del mercado objetivo y los competidores actuales.

Agradecimientos

Llegar a este punto que parecía tan lejano no fue fácil, es la consecuencia de muchas acciones y decisiones que me han llevado aquí hoy. Por esto quiero agradecer a mi mujer Kathy, mis hijos Vicente, Tomás y Santiago por acompañarme, apoyarme, alentarme y tener infinita paciencia en estos 2 largos años de estudio.

También quiero agradecer a mis papás Carmen y Toño, mis hermanos (José, Susana y Ximena), a mis sobrinos (Alexis, Bayron, Carla y Diego) por creer siempre en mí, por alentarme a avanzar día a día. A Fresia por apoyarme siempre y también a Jorge que desde donde esté, sé que me ayudó a llegar hasta aquí.

Agradecer también a Carola y Jorge Luis por estar ahí siempre, a mis amigos de la Junta! con quienes día a día hacemos crecer nuestros sueños y metas.

Agradezco también a todos los profesores y ayudantes del programa, sin duda me ayudaron a avanzar enormemente en mi carrera y a crecer como persona, cuando miro hacia atrás, me doy cuenta lo mucho que aprendí de ustedes.

Por último, a mis compañeros y amigos del programa, quienes fueron un pilar fundamental en el desarrollo de esta etapa, sobre todo, al mejor Grupo MBA Ricardo, Andrea, Jope, Clau, Seba y el Dr. Juan Luis.

TABLA DE CONTENIDO

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

En los últimos años el escenario empresarial cambió, los clientes evolucionaron en sus necesidades y cada vez los canales remotos de atención, las aplicaciones, los sitios web son cada día más relevantes para el funcionamiento de las empresas, por lo que hoy es difícil pensar en una que no use tecnología para su funcionamiento, si bien esto genera enormes oportunidades de desarrollo y expansión de negocios, también abre la puerta a los ciberdelincuentes y desde aquí nace la interrogante ¿Están preparadas las pequeñas y medianas empresas para enfrentar un ciberataque? De acuerdo con el estudio de "Estado de ciberseguridad 2020"[1] realizado por Entel a negocios chilenos, un 43,3% de las Pymes en Chile no está consciente de los riesgos a nivel de ciberseguridad que corren diariamente y un 27% no hace nada para resguardarse, incluso si ya han sido atacadas.

Creer que una empresa o negocio es muy pequeño o que sus datos no son del interés de los ciberdelincuentes, es uno de los errores más comunes que cometen las pymes, por otra parte, las grandes empresas comienzan a invertir mayores cifras en tecnología y protección de sus datos, lo que convierte al sector de las pymes en el eslabón débil de la cadena de empresas, por lo que, se puede presumir un alza en los próximos años de ciberataques e incidentes en este sector.

Por otra parte, las herramientas que la industria de la ciberseguridad entrega hoy, generan una barrera de entrada grande para estas empresas, por otra parte, las consultoras actuales del mercado se han centrado en prestar servicios de protección a las grandes empresas como Bancos, Retailers, grandes manufactureras, instituciones previsionales entre otras, por lo que este sector del mercado chileno no cuenta con una oferta *ad-hoc* en servicios de ciberseguridad sino más bien cuenta con la adaptación de algunos servicios diseñados para grandes empresas, que si bien otorgan un grado de seguridad importante, muchas veces pueden complejizar la operación de empresas más pequeñas..

Estos factores del entorno contribuyen a conformar un contexto favorable para la conformación de una empresa consultora de servicios de ciberseguridad especializada en las Pymes y de esta manera apoyar el desarrollo de la economía nacional con una estructura de ciberseguridad robusta.

[1] Informe: https://informacioncorporativa.entel.cl/estado-de-la-ciberseguridad

2. DESCRIPCIÓN DEL TEMA

La pandemia COVID-19 aceleró la transformación digital en el mundo entero, en Chile por ejemplo aumentó del uso de internet en un 81% para el 2020 en comparación con el 2019, por otra parte el uso de los teléfonos móviles y aplicaciones de mensajería como Whatsapp o Telegram aumentó en más de un 600%, por otra parte, las proyecciones de la Cámara de Comercio de Santiago (CCS), para el 2021, el comercio electrónico crecerá un 20% en el país, lo que se traducirá en ventas por más de USD 11.500 millones.

Si bien estos son datos que se pueden ver de manera positiva, también es un aumento conocido por los cibercriminales que ven en esta masificación del uso una oportunidad de ataques o fraudes cibernéticos a empresas y personas que antes de la pandemia no estaban en el objetivo de ataque.

De acuerdo con el informe de Riesgos Globales 2020 del Foro Económico Mundial[2], el riesgo de ciberataques a la infraestructura crítica y el fraude o robo de datos confidenciales se clasificaron entre los 10 principales riesgos con mayor probabilidad de ocurrir (Ver Anexo A), por otra parte, la Perspectiva de Riesgos del COVID-19 del Foro Económico Mundial, identificó los ciberataques como la tercera mayor preocupación, producto de la realidad actual y la transformación digital que han vivido innumerables empresas en el mundo.

Para el 2021, se estima que los daños por delitos de cibercrimen o ciberataques alcanzarán la cifra de US$6 billones a nivel mundial y las cifras no serán menores para los próximos años, si bien esta es la situación a nivel mundial, no es diferente a la realidad chilena, de acuerdo con la empresa Fortinet[3], Chile recibió 410 millones de intentos de ciberataques sólo en el primer trimestre de 2021.

Esto sumado a la abrupta adopción de tecnología vivida por muchas empresas en los últimos años y a la mayor dependencia para sus operaciones diarias, aumenta preocupantemente la exposición a los riesgos de ciberseguridad.

Si bien muchas de las pymes cuentas con antivirus que las protegen de un sin número de amenazas, ¿son suficientes? La respuesta a esta pregunta es: no, son útiles, pero no suficientes, día a día las amenazas son más variadas y en su mayoría ingresan en las empresas a través de las personas, por un correo, uso navegación por sitios no seguros, uso de software no registrado entre muchas otras variables.

[2] https://www.weforum.org/reports/the-global-risks-report-2020
[3] https://www.fortiguardthreatinsider.com/es/bulletin/Q1-2021

Un reciente estudio realizado a pymes españolas [4]mostró que el 95% de los ciberataques a este tipo de empresas se produce a través de ingeniería social, es decir, a través del engaño de las personas, es por esto por lo que la concientización de las personas, el uso de contraseñas seguras, los filtros de navegación entre otras medidas son cada vez más necesarias. Es por esto, que todas las empresas deben estar preparadas para enfrentar ese nuevo escenario, el uso de dispositivos móviles para labores personales y laborales es más común.

Si pensamos en la distribución de las ventas de las Pymes chilenas, se puede decir que aproximadamente 24.000 de ellas, generan ventas anuales entre 25.000 a 100.000 UF anuales como se puede observar en la siguiente tabla:

Tabla 1. Cuadro resumen Pymes, Actualizado a octubre de 2020

Tramo de Ventas	Empresas con ventas en 10 o más meses del año calendario	Empresas con ventas en 12 o más meses del año calendario	Empresas con ventas y uno o más trabajadores dependientes informados	Empresas individuales con ventas y sin trabajadores dependientes informados
Hasta 25.000 UF	508.799	397.501	302.125	491.575
25.000,01 a 75.000 UF	21.406	19.394	21.937	491
75.000,01 a 100.000 UF	3.105	2.875	3.212	33
Total PYMES	**533.310**	**419.770**	**327.274**	**492.099**

Fuente: Elaborado por la Subdirección de Gestión Estratégica y Estudios Tributarios en base a información contenida en los formularios 22 y 29 y en la declaración jurada 1887 (sueldos).[5]

Por otra parte, contar con profesionales especializados en seguridad tiene un costo elevado y en el mercado chileno son cada vez más requeridos por las grandes empresas, por otra parte, para contar con un entorno de seguridad adecuado, no es sólo 1 persona quien lo logrará, sino un equipo de profesionales, en donde los sueldos rondan los 1.8 hasta los 8 millones mensuales, de acuerdo con estudio realizado por IT Hunter; firma especializada en la búsqueda y selección de talentos tecnológicos en Chile y la Región, por lo que, para una Pyme, se convierte en un gasto excesivo mantener áreas internas con esta función.

Actualmente, existen consultoras especializadas en ciberseguridad, pero están centradas en los macro presupuestos en ciberseguridad de las grandes empresas, los que rondan los $1.500 a $9.000 millones anuales (Fuente: ENCI, datos actualizados a octubre 2019)

Adicionalmente a lo mencionado, en Chile se presentó en marzo de 2020 el proyecto de ley de protección de datos personales que viene a actualizar la ley 19.628[6], que incorpora una serie de exigencias en el tratamiento y protección de los datos

[4] Informe Escudos 2021 de la agencia española Exsel.
[5] https://www.sii.cl/sobre_el_sii/estadisticas_de_empresas.html
[6] https://www.bcn.cl/leychile/navegar?idNorma=141599

personales de las personas, es decir, en los próximos meses, contar con controles de seguridad será una exigencia regulatoria.

Dado lo anterior, se observa un universo de 533.000 empresas en Chile que no contarían con una oferta especializada en servicios de seguridad, generando una oportunidad para que ingrese una consultora a desarrollar servicios específicos de seguridad con foco en las Pymes.

3. PREGUNTAS CLAVES Y FACTORES CRITICOS

Respecto a la factibilidad de este plan de negocios, las preguntas claves a resolver son las siguientes:

- ¿Qué tan sensibles están las Pymes a los temas relacionados con Ciberseguridad?
- ¿Cómo incentivar la inversión en ciberseguridad para las Pymes?
- ¿Cuál debiese ser la estrategia de crecimiento de esta empresa?
- ¿Se puede generar un modelo adaptado a las necesidades de las Pymes?
- ¿En cuántos años se recupera la inversión de esta empresa?

Los factores críticos para el desarrollo de este negocio son:

El nivel de sensibilización de las pymes chilenas en temas de ciberseguridad: Es importante determinar el nivel ya que, si esto es bajo, se podría convertir en una barrera de entrada a este tipo de empresas.

Disposición a pagar por servicios de ciberseguridad: al igual que la sensibilización, es importante determinar el monto o porcentaje de las ventas que están dispuestas a pagar las pymes.

Nuevas leyes y normativas relacionadas: Chile suscribió el Segundo Protocolo Adicional al Convenio de Budapest sobre Ciberdelincuencia. Esto generará mayores restricciones y protección que deberá implementar el sector público y privado entorno al manejo de los datos de las personas

Desarrollo tecnológico: el aumento en el uso de tecnologías en diferentes industrias; como por ejemplo el internet de las cosas, en conjunto con la tendencia de aumento del cibercrimen, generarían un aumento en las necesidades relacionadas con la protección de las empresas.

Adopción del teletrabajo o modelos de operación híbridos: estas modalidades de trabajo incrementan las posibilidades de las empresas a sufrir incidentes de relacionados con ciberseguridad.

Capital humano: Día a día el mercado laboral en ciberseguridad está más intenso, es mayor la demanda de profesionales de estas materias que los existentes, lo que podría dificultar la conformación y mantención de un equipo de calidad con un plan de costos administrable.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Desarrollar un plan de negocios para la implementación de una consultora orientada a los servicios de ciberseguridad con foco en las Pymes chilenas, que consiga una rentabilidad sobre el 50% en un plazo de 5 años.

4.2. OBJETIVOS ESPECIFICOS

- Generar una propuesta de servicios adaptable a las necesidades de las Pymes chilenas.
- Crear un modelo de negocio escalable con una oferta diferenciada para los clientes.
- Crear un modelo operacional sustentable en el tiempo garantizando la continuidad en el tiempo.
- Comprobar la factibilidad económica del plan y el retorno de la inversión. realizando la evaluación económica de la implementación de la consultora, para estimar atractivo de la realización del negocio.

4.3. RESULTADOS ESPERADOS

Al finalizar el desarrollo del plan de negocios se espera contar con el análisis de factibilidad económica determinando los requerimientos de capital para el cumplimiento del plan de negocios, el segmento de clientes especifico a captar con una propuesta de valor diferenciada que sea capaz de atraer clientes pyme, para la implementación de la consultora de ciberseguridad.

5. ALCANCE

Este plan de negocios busca describir la oportunidad que existe en la creación de una consultora de ciberseguridad enfocada en las Pymes de Chile, para esto se analizarán los siguientes tópicos:

- Industria de las consultoras de ciberseguridad,
- Población chilena
- Uso y dependencia de tecnologías para la operación de las pymes chilenas.
- Conciencia y conocimiento de los riesgos de ciberseguridad en las pymes chilenas.

Por otra parte, se describen los puntos clave para la creación de una consultora de ciberseguridad, incluyendo, las definiciones estratégicas, marketing, operacional, financiera y de gestión de personas. Además, se generan las proyecciones financieras a 5 años para evaluar el atractivo del negocio en diferentes escenarios.

6. MARCO CONCEPTUAL

Este documento explica la oportunidad de negocio que existe en torno a la ciberseguridad de las pymes chilenas y contiene una guía para el desarrollo y puesta en marcha de la idea. De manera general se incluirán el análisis del entorno e industria, Plan estratégico, Plan de marketing, Plan operacional, Plan organizacional, Plan financiero y Conclusiones.

Para la mejor comprensión de este plan de negocio, se detallan los principales conceptos de acuerdo con las definiciones publicadas por la empresa de ciberseguridad Karpersky y el INCIBE (Instituto nacional de ciberseguridad de España.):

Ciberseguridad: Es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos.

Ciberataque: es un intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema.

Incidente de seguridad: Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

Phishing: Técnica o tipo de ataque en el que alguien suplanta a una entidad/servicio mediante un correo electrónico o mensaje instantáneo para conseguir las credenciales o información de la tarjeta de crédito de un usuario. Ese correo/mensaje suele tener un enlace (o fichero que contiene ese enlace) a un sitio web que suplanta al legítimo y que usan para engañarlo.

ingeniería social: Conjunto de técnicas que los delincuentes usan para engañar a los usuarios de sistemas/servicios TIC para que les faciliten datos que les aporten valor, ya sean credenciales, información sobre los sistemas, servicios instalados etc.

Malware: Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información.

CSIRT: Un Equipo de Respuesta ante Emergencias Informáticas es un centro de respuesta para incidentes de seguridad en tecnologías de la información. Está formado por un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

NIST Cybersecurity Framework: conjunto de pautas para mitigar los riesgos de ciberseguridad organizacional, publicado por el Instituto Nacional de Estándares y Tecnología de EE. UU.

Marco de controles COBIT: (Control Objetives for Information and Related Technology) COBIT es un marco de trabajo (framework) para el gobierno y la gestión de las tecnologías de la información (TI) empresariales y dirigido a toda la empresa.

CIS controls: es una publicación de pautas de mejores prácticas para la seguridad informática. El proyecto se inició a principios de 2008 en respuesta a las pérdidas extremas de datos experimentadas por organizaciones en la base industrial de defensa de EE. UU.

ISO 27032: El término ISO/IEC 27032 se refiere a "Ciberseguridad" o a "seguridad en el ciberespacio", que se define como la protección de la privacidad, la integridad y accesibilidad de los datos de información que se encuentran en el ciberespacio

Ya descritos los principales conceptos, se procede con la descripción de los análisis y planes a realizar:

El análisis del entorno se realizará utilizando el modelo PESTEL que permitirá la comprensión del entorno Político, Económico, Sociocultural, Tecnológico, Ecológico o medioambiental y Legal en que se implementará la consultora. Para el análisis del microentorno se realizará el análisis de las 5 fuerzas de Porter, lo que permitirá comprender de mejor manera los siguientes puntos:

- El poder de negociación de los **Clientes,** Conocer la distribución de los clientes, los comportamientos de compra, conocimiento y sensibilización en temas de ciberseguridad
- El poder de negociación de **Proveedores** que pueden ejercer sobre las consultoras de ciberseguridad, entendiendo como proveedores aquellas empresas fabricantes de software o herramientas relacionadas con la ciberseguridad.
- La entrada de nuevos **competidores** con ofertas adaptables a las pymes chilenas.
- La amenaza o existencia de **productos sustitutos**, es decir, como las pymes se podrían proteger sin los servicios de una consultora especializada en ciberseguridad.
- Intensidad de la **rivalidad del mercado.**

Luego de la comprensión del entorno, se realizará el análisis FODA de la consultora en donde se definirán las directrices para enfrentar las amenazas y aprovechar las oportunidades que entrega el mercado, potenciando las fortalezas y trabajando en las debilidades que podría presentar la consultora en su operación y puesta en marcha.

Para el desarrollo del plan del plan estratégico se utilizará el modelo Delta de Arnoldo Hax, con lo que se podrá definir claramente cuál es el rol que desempeñará la consultora en el mercado. Con esto claro se procederá a la definición del Plan de marketing analizando las 4P’s generando una propuesta que sea sustentable en el tiempo con foco en la experiencia de los clientes. Por otra parte, se realizará la determinación del segmento objetivo y el posicionamiento que tendrá la consultora en la industria de la ciberseguridad chilena.

Con relación al plan Operacional y Organizacional, se definirá el modelo de operación, el cual debe ser sustentable y escalable en el tiempo, para esto se tomarán como marco de referencia los principales estándares de ciberseguridad y generarán indicadores de eficiencia del modelo. Por otra parte, el plan organizacional permitirá identificar los sistemas de control y la estructura organizacional con la que debe contar la consultora para cumplir con el plan estratégico y evaluar si esta es o no conveniente.

El plan financiero, buscará determinar la inversión requerida para la puesta en marcha de la consultora y la tasa de retorno que tendrá, con lo que se podrá concluir el atractivo de la idea planteada en este plan de negocios.

7. PROPUESTA METODOLÓGICA

La metodología que se contempla para llevar a cabo este plan de negocio considera las siguientes etapas:

I. **Estudio del macro y microentorno:** Para la realización del análisis del macroentorno se realizará un análisis que comprenda las variables Políticas, Económicas, Sociales, Tecnológicas y Legales de Chile para el que se utilizarán estudios formales de entidades internacionales y empresas especializadas en ciberseguridad además de entrevistas a lideres de asociaciones de emprendedores y expertos relacionados a la ciberseguridad realizadas por diferentes medios de comunicación(diarios, revistas especializadas y journals), con el objetivo de comprender las principales amenazas y oportunidades que se podrían generar en Chile para el negocio de la ciberseguridad. Con relación al microentorno, este se realizará basado en el modelo de 5 fuerzas, para esto se realizará un análisis del mercado de las pymes chilenas que permita identificar como resuelven hoy las necesidades relacionadas a ciberseguridad y las posibles barreras de entrada que podrían tener nuevos competidores para ofertar en este tipo de empresas.

II. **Plan de Marketing:** Esta etapa se realizará a través de una investigación sobre las pymes chilenas, para lo que se analizarán diferentes estudios realizados tanto a nivel nacional como internacional, además se generarán entrevistas con lideres de pymes de diferentes rubros con el objetivo de contrastar los resultados de los estudios y definir la mejor estrategia para ingresar al mercado. Con estos resultados, se podrá determinar segmento objetivo de clientes y la declaración de posicionamiento.

III. **Plan Estratégico:** Luego de analizar el entorno revisar las variables externas e internas, se definirá la estrategia utilizando el modelo Delta de Arnoldo Hax,[7] con el que se buscará el posicionamiento estratégico de la consultora y definirán los indicadores para medir su evolución, con foco en la atracción y captación de nuevos clientes y posteriormente la retención de ellos, permitiendo sacar el máximo provecho de las oportunidades identificadas, mitigar las amenazas, trabajar en las debilidades y potenciando las fortalezas. Este plan incluirá la visión, misión, y estrategia competitiva de la empresa.

IV. **Plan Operacional:** Implementar un modelo de operación sustentable basado en los principios de los marcos de referencia de controles relacionados con ciberseguridad, tales como:

- NIST Cybersecurity Framework[8],
- Marco de controles COBIT[9],
- CIS controls[10],
- ISO 27032 Gestión de ciberseguridad.

Para esto, se analizarán las principales herramientas de ciberseguridad para seleccionar aquellas que permitieron generar procesos simples y agiles para los clientes, ayudando a las pymes chilenas operar con altos niveles de seguridad sin la necesidad de contar con equipos propios dedicados a esta labor.

V. **Plan Organizacional:** En este apartado se definirá la estructura organizacional, el modelo de reclutamiento y selección, el plan de capacitación interna.

VI. **Plan Financiero:** Realizar un análisis financiero que permita definir la inversión requerida para iniciar con las operaciones de la consultora, para posteriormente construir el flujo de caja a 5 años y determinar el VAN y TIR del proyecto.

VII. **Conclusiones:**

[7] Hax, A. (2010). The Delta Model. Springer New York.
[8] https://www.nist.gov/cyberframework
[9] https://www.isaca.org/resources/cobit
[10] https://www.cisecurity.org/controls/

Consolidación de los temas más relevantes obtenidos en el desarrollo del plan de negocios, con el objetivo de presentar la visión completa de la factibilidad técnico-financiera del modelo evaluado.

8. DESCRIPCION DEL MERCADO DE LA CIBERSEGURIDAD

Se puede definir como mercado de ciberseguridad la demanda de soluciones, productos o servicios que existen para la protección de la infraestructura tecnológica y la seguridad de la información, esto para las personas, empresas y entidades públicas, para el entendimiento del mercado se describirán el mercado global, latinoamericano y chileno.

8.1. MERCADO GLOBAL

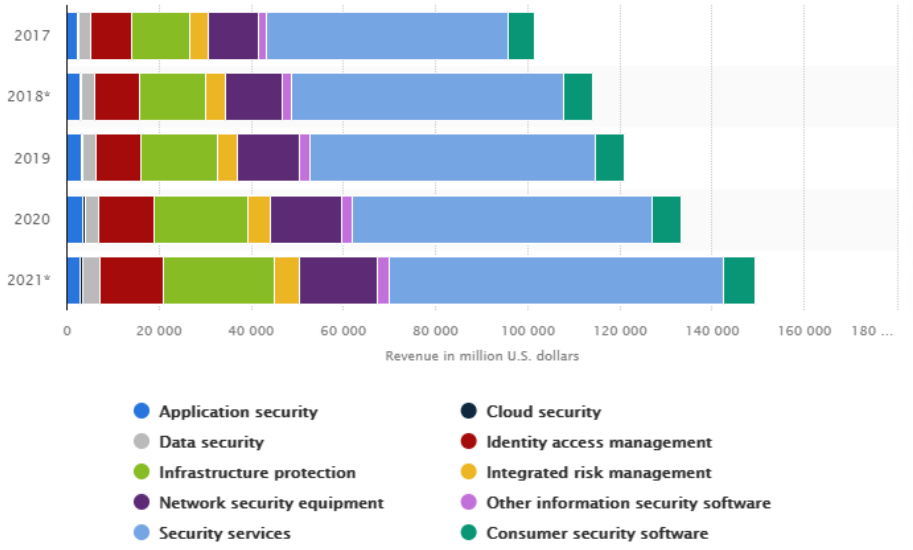
En los últimos años y producto de la pandemia, la adopción de tecnologías a nivel mundial ha tenido un crecimiento exponencial y la dependencia a esta, es cada día mayor, sea para personas, empresas de todo ámbito y organizaciones gubernamentales, en este contexto la preocupación a nivel mundial por los riesgos relacionados a la ciberseguridad son cada vez mayores, como podemos ver en la Figura 1, los costos promedios de los ciberataques o incidentes de seguridad están en promedio por sobre los 2 millones de dólares.

***Figura 1**. Estadísticas de amenazas de ciberseguridad 2020*

Fuente: CompTia 2020.

Por otra parte, esto se ve reflejado en el gasto mundial en ciberseguridad, según Gartner, el mercado de la ciberseguridad es una actividad económica en auge y constante crecimiento (Ver figura 2), el gasto mundial en productos y servicios de seguridad alcanzará más de 150.000 millones de dólares anuales.

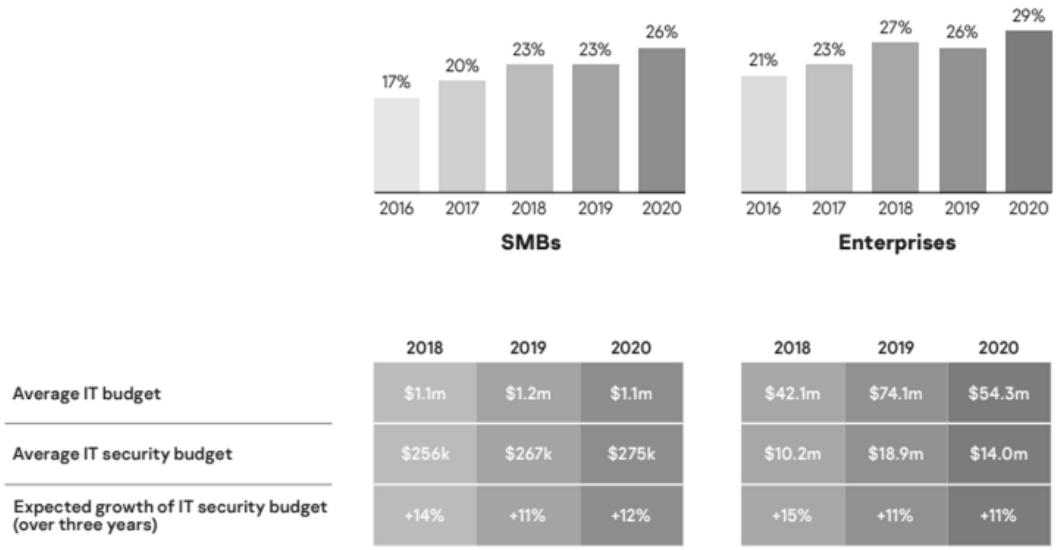
Figura 2. Gasto mundial en seguridad por segmento, 2017-2021(en millones de dólares estadounidenses).



Fuente: Gartner (junio 2020)

Con relación al presupuesto dedicado a ciberseguridad, las empresas a nivel global destinan en promedio un 31% del presupuesto total de tecnología, esto de acuerdo con los datos recogidos por la empresa Karpersky en un estudio realizado a más de 5000 empresas de diferentes industrias de Mundiales [11](ver figura 3)

Figura 3. Proporción del presupuesto destinado a ciberseguridad del presupuesto total de Tecnología 2020, para empresas pymes (SMB: Small and Medium Business) y grandes empresas.



	2018	2019	2020	2018	2019	2020
Average IT budget	$1.1m	$1.2m	$1.1m	$42.1m	$74.1m	$54.3m
Average IT security budget	$256k	$267k	$275k	$10.2m	$18.9m	$14.0m
Expected growth of IT security budget (over three years)	+14%	+11%	+12%	+15%	+11%	+11%

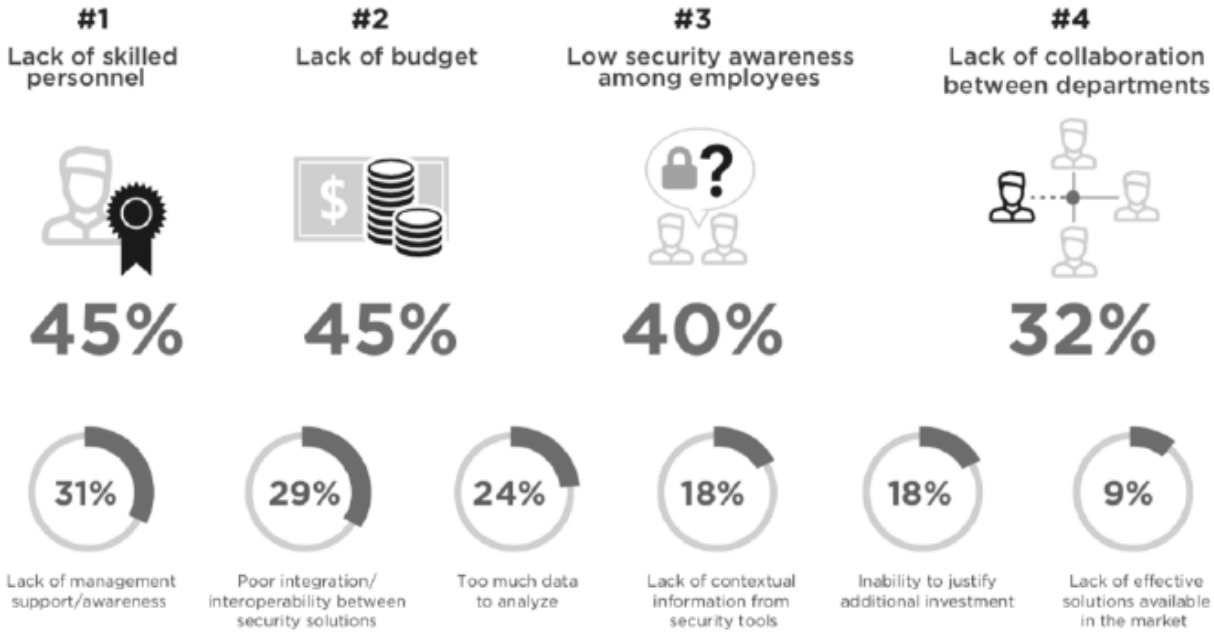
Fuente: Karspersky, 2020

[11] Investment adjustment: aligning IT budgets with changing security priorities, 2020, Karspersky

Si bien la pandemia generó una recesión económica a nivel mundial, la adopción de nuevas tecnologías como la nube, hizo que el mercado de la seguridad sea algo más resistente, principalmente porque generó un ahorro importante para las empresas en compra de infraestructura tecnológica, de acuerdo con Gartner, en 2019, los modelos de servicios basados en la nube ya habían superado el 50% de las implementaciones en mercados como el correo electrónico seguro y controles de navegación.

Por otra parte, el informe del Cybersecurity Trends establece que de los principales obstáculos para la implementación de una estrategia de ciberseguridad para las empresas corresponden a la falta de profesionales con conocimientos expertos, el presupuesto, la baja concientización de los empleados y la colaboración entre las áreas (ver figura 4).

Figura 4. Principales obstáculos para la implementación de una estrategia de ciberseguridad en las empresas



Fuente: Spotlight Report, Cybersecurity Trends, 2017.

Se puede concluir que, el mercado global de la ciberseguridad tiene un alto potencial de crecimiento en los próximos años con una tasa de crecimiento proyectada por Garner de un 12% anual, sobre todo en el segmento de los servicios, ya que cada día son más las empresas que requieren de ellos, pero no cuentan con las capacidades de implementar un marco de controles de manera interna.

8.2. MERCADO LATINOMAERICANO

La evolución del mercado de la ciberseguridad en Latinoamérica en el 2020 creció en torno a un 7%, lo que la ubica por debajo de la media global, pero de todas maneras representa un crecimiento sostenido desde el año 2018, lo que hace proyectar en el 2025 el mercado de la ciberseguridad en Latinoamérica crezca un 51% en comparación con el 2019, alcanzando el monto de 26.000 millones de dólares.

Con relación al presupuesto dedicado a ciberseguridad, las empresas de Latinoamérica en promedio destinan un 31% del presupuesto total de tecnología, esto de acuerdo con los datos recogidos por la empresa Karpersky en un estudio realizado a más de 5000 empresas de diferentes industrias de Mundiales.[12]

Según refleja la investigación realizada por Karpersky, la proporción del presupuesto de tecnología dedicada a la seguridad sigue creciendo año tras año en los países de la región: de $114,000 dólares en 2019 a $250,000 dólares en 2020 en el caso de las pymes latinoamericanas, y de $13 millones de dólares en 2019 a $20 millones de dólares en 2020 en las grandes empresas.

Sin embargo, un pequeño porcentaje de las empresas, el 9% de las pymes y el 13.5% de las grandes compañías latinoamericanas tienen previsto reducir el gasto en ciberseguridad en los próximos tres años. De estas últimas, el 28% alega que la alta dirección no ve ninguna razón para realizar la inversión, mientras que otro 28% comentó que pueden tomar esta decisión, debido a que las funciones de Seguridad Informática han sido asumidas por empresas de outsourcing.

Tabla 2. Razones para disminuir la inversión en ciberseguridad

Reasons given for expecting to reduce IT security spending over the next three years	SMB		Enterprise	
	%	Rank	%	Rank
Overall cuts to company expenses/general budget optimization	29%	1	26%	5
Large investments in past years solved key problems – now only maintenance is needed	25%	3	30%	2
Top management sees no reason to invest so much in IT security	23%	5	32%	1
We are secure enough and there is no need to invest more in IT security	25%	2	22%	7
Outsourcing some IT security functions allows us to cut costs	22%	7	26%	4
IT budget re-allocated to other needs in the company	19%	8	27%	3
Due to a decrease in business	23%	4	20%	10
There were no security incidents experienced in the last 12 months	22%	6	21%	8
Switched to a cheaper endpoint protection solution/vendor	19%	8	23%	6
Demand from our shareholders and investors	15%	10	21%	9

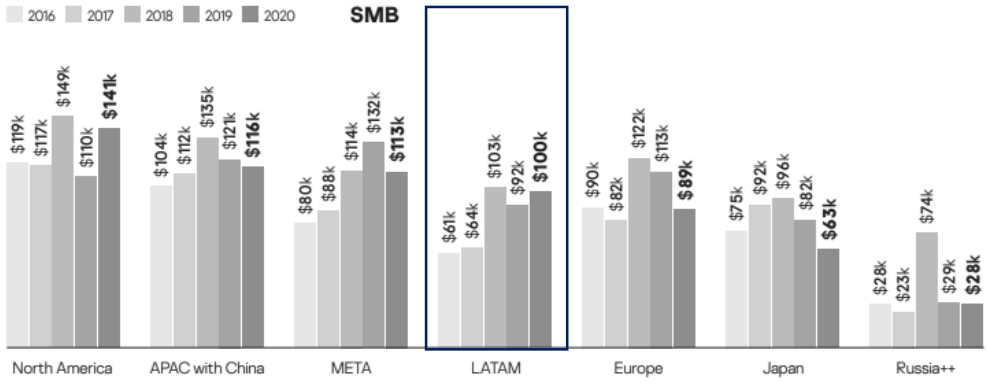
Fuente: Karspersky, 2020

En este contexto desde el 2016 el impacto financiero de los incidentes de ciberseguridad sufridos por las pymes en Latinoamérica ha aumentado en un 80%,

[12] Investment adjustment: aligning IT budgets with changing security priorities, 2020, Karspersky

convirtiéndose en la región que más ha aumentado en este concepto, pasando de tener en 2016 un promedio de $61.000USD a superar los $100.000USD por evento de ciberseguridad sufrido, sin duda un fuerte golpe a las empresas de la región. (Ver figura 5)

Figura 5. Impacto promedio de incidentes de ciberseguridad en el mundo



Fuente: Karspersky, 2020

En conclusión, se puede observar que el mercado latinoamericano sigue la tendencia mundial de crecimiento, pero también ha mostrado un aumento significativo en el costo de los incidentes para las pymes, esto principalmente por la baja preparación en este aspecto para la implementación de una estrategia de ciberseguridad adaptada a sus necesidades, por otra parte hay una creciente tendencia a tratar estos riesgos a través de empresas outsoursing generando una oportunidad para las empresas que quieran ingresar en este mercado.

8.3. MERCADO CHILENO

Actualmente en Chile, de acuerdo con el índice de ciberseguridad Global desarrollado por Unión Internacional de Telecomunicaciones[13] (ITU, agencia de las Naciones Unidas especializada en la coordinación de las telecomunicaciones a nivel global), Chile se ubica en el puesto 74 a nivel global y 7 de América (Ver tabla 3)

[13] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Tabla 3. Resultados índices de ciberseguridad global, América. 2021

Country Name	Overall Score	Regional Rank
United States of America**	100	1
Canada**	97.67	2
Brazil	96.6	3
Mexico	81.68	4
Uruguay	75.15	5
Dominican Rep.	75.07	6
Chile	68.83	7
Costa Rica	67.45	8
Colombia	63.72	9
Cuba	58.76	10

Fuente: Unión Internacional de Telecomunicaciones

Esto muestra un avance del país en términos regulatorios y de comunicación de los incidentes a nivel de estado, con la implementación del CSIRT y el nuevo marco normativo en desarrollo, para ver el resultado de cada una de las dimensiones evaluadas revisar Anexo B.

En cuanto a la inversión en ciberseguridad, Chile se encuentra por debajo del promedio de Latinoamérica, pese a contar con un mayor gasto en tecnología aún las empresas deben mejorar sus controles y prioridad de inversión para cubrir estos riesgos, al 2018 un 12% de las empresas está realizando inversión en ciberseguridad, 8 puntos porcentuales menos que el promedio de 21% de las empresas de Latinoamérica, por otra parte hay una tendencia en crecimiento a la contratación de servicios outsourcing para la gestión de los riesgos de ciberseguridad, dados los costos y complejidades que se han identificado a nivel global, para los que Chile no es ajeno. Ver figura 6.

Figura 6. Resumen de mercado de la ciberseguridad en Chile

Fuente: Fortinet

Por otra parte, la inversión en ciberseguridad ha aumentado año a año y cada día son más las empresas que cuentan con un presupuesto dedicado a ciberseguridad,

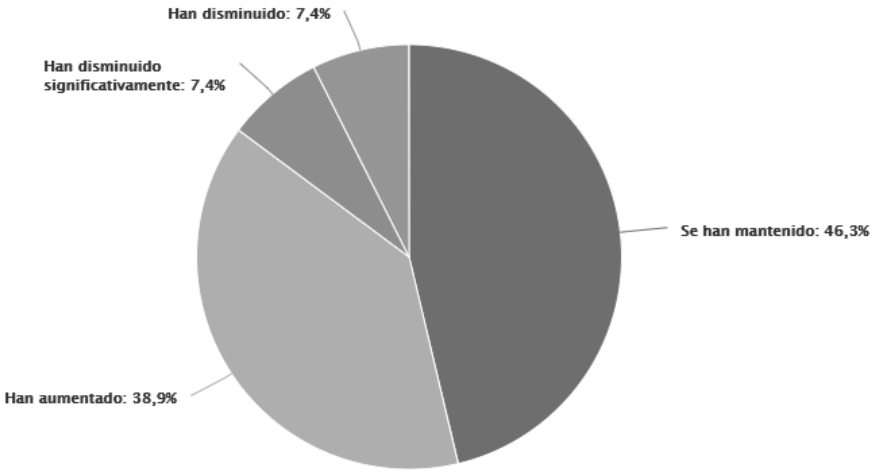
como se ve en la figura 7 desde 2017, esto se ha mantenido en los años posteriores ya que el aumento del teletrabajo y el uso de nuevas tecnologías aumentó la superficie de ataque. Por otra parte, de acuerdo con el programa de investigación Future of Trust de IDC[14], el 40% de las empresas chilenas aumentará su inversión en ciberseguridad para el 2022

Figura 7. Inversión de empresas chilenas en ciberseguridad

Fuente: Gartner

Por otra parte, la adopción del teletrabajo o modelos de operación híbridos ha aumentado el impacto de los incidentes de ciberseguridad en un 38.9% de las empresas. Ver figura 8.

Figura 8. Impacto en incidentes de ciberseguridad debido al teletrabajo en Chile**.**



Fuente: ENTI

[14] https://www.idc.com/

De los datos recopilados del mercado chileno, podemos concluir que, si bien ha aumentado la inversión en términos de ciberseguridad, aún falta por mejorar, por otra parte, la adopción de nuevas tecnologías hace necesaria la cobertura sobre los riesgos relacionados a la ciberseguridad.

8.4. CADENA DE VALOR CIBERSEGURIDAD

En el mercado de la ciberseguridad hay diferentes grupos de actores cuando pensamos en la cadena de servicios, de acuerdo con el INCIBE, la cadena se divide en 4 bloques principales: Fabricación, Distribución, Servicios y los Clientes. Como se muestra en la figura 9.

Figura 9. Cadena de valor servicios de ciberseguridad

Fuente: INCIBE, 2020.

Posteriormente con la aplicación de la metodología se definirá el posicionamiento que tendrá la consultora de ciberseguridad.

9. ANALISIS DEL MACROENTORNO

Para la comprensión del entorno en que se desarrollará el plan de negocios, se analizaron las diferentes variables Políticas, Económicas, Tecnológicas y Legales, las que se describen a continuación:

9.1. POLÍTICO

Desde el 18 de octubre de 2019 Chile ha enfrentado un entorno político de incertidumbre, que involucró una alta desaprobación de la clase política y del gobierno chileno, lo que desencadenó en un plebiscito para decidir si se debía reescribir la constitución del país, lo que fue aprobado por amplia mayoría en el año

2020, generando una Convención Constituyente con miembros escogidos por la ciudadanía a través del voto, todo este entorno más el cambio de mando, de un gobierno conservador a uno más de centro izquierda han provocado un entorno de incertidumbre para los próximos años, lo que ha afectado negativamente las inversiones y la economía del país. Estas situaciones sin duda generan un ambiente complejo para realizar inversiones de largo plazo en el país.

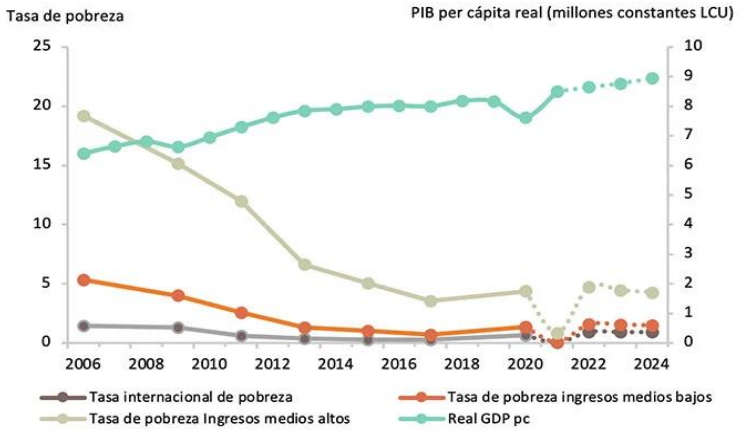
Por otra parte, con fecha 12 de mayo, Chile suscribió el Segundo Protocolo Adicional al Convenio de Budapest sobre Ciberdelincuencia, lo que generará que el país adopte diferentes medidas en los próximos años referidas a las materias de ciberseguridad y prevención del cibercrimen.

9.2. ECONÓMICO

En los últimos años se ha vivido uno de los shocks económicos más grandes de la historia producto de la masificación del covid en el mundo, Chile no ha sido ajeno a esto y vivió un estancamiento del PIB en este año que luego en 2021 creció un 11,7%, una de las recuperaciones más rápidas del mundo. Esto principalmente por el aumento del consumo, propiciado por los retiros de los fondos de pensiones y el apoyo fiscal directo a las personas que alcanzó 9% del PIB. Por otra parte, la normalización de la actividad económica con una de las tasas de vacunación más rápidas del mundo.

Por el lado de la recuperación del mercado laboral, esta no ha sido la esperada ya que solo un 60% de los empleos que se perdieron en 2020 fueron recuperados en 2021, siendo las mujeres las más afectadas con este punto.

Figura 10. PIB real y proyectado per cápita y tasas de pobreza



Fuente: Banco Mundial Marzo, 2022.

Por otra parte, de acuerdo con el IPOM del mes de junio de 2022, La inflación en Chile ha seguido escalando, alcanzado su máximo nivel de las últimas décadas. El principal factor tras el alza de la inflación continúa siendo el significativo aumento de la demanda durante 2021. No obstante, en los últimos meses se ha profundizado el impacto de las altas presiones de costos globales, consecuencia de los mayores precios de las materias primas, la energía y los alimentos. Todo esto en un contexto en que se han mantenido las dificultades en las cadenas de distribución global, el peso permanece depreciado y la brecha de actividad sigue siendo positiva. Las perspectivas de inflación de corto plazo aumentan de forma importante, respondiendo a esta suma de factores. Pese a este escenario preocupante para varias industrias, diferentes empresas relacionadas con la tecnología han logrado obtener crecimientos importantes en el periodo de pandemia producto de la adopción del teletrabajo, los cambios en los hábitos de compra y la creciente adopción de nuevas tecnologías.

9.3. SOCIAL

En los últimos años tanto en Chile como en la región se ha experimentado un aumento del cibercrimen principalmente relacionado con la estrategia del engaño a las personas y robo de credenciales para realizar suplantación de identidad, esto sumado a la masificación del uso de la tecnología y al surgimiento de los nativos digitales, que no son más que las nuevas generaciones que ya no concibe el desarrollo de la vida sin contar con un dispositivo o conexión a internet. Por otra parte, el aumento de las compras online ha generado una expansión notable en la superficie de ataque para los cibercriminales

9.4. TECNOLÓGICO

En los últimos años Chile ha vivido un crecimiento explosivo en el ámbito tecnológico, producto de la pandemia y de las nuevas generaciones con el uso masivo de dispositivos.

De acuerdo con un informe de la consultora IDC, se espera que más del 50% del PIB de 2022 en Latinoamérica será digitalizado, Chile no está ajeno a esta situación. De acuerdo con indagaciones realizadas en diferentes medios digitales del país y a la revisión de entrevistas e informes de los principales lideres tecnológicos del país, se puede resumir que las tendencias en términos de tecnología para los próximos años serán las siguientes:

- **Big Data y decisiones basadas en datos:** El aumento de dispositivos conectados a la red y la dependencia de las personas en la tecnología, abren una oportunidad gigante de trazabilidad y manejo de información de las personas, en este sentido uno de los principales desafíos de las diferentes organizaciones en Chile y el mundo es generar una arquitectura de datos que sea capaz de soportar estas informaciones, día a día las organizaciones tenderán a basar sus decisiones en datos, y quien sea capaz de administrarlos de mejor manera, serán los que tendrán la ventaja competitiva sobre el resto.

- **Metaverso:** "Es una nueva convergencia entre el mundo físico y digital. Es un lugar donde la gente puede interactuar y donde los activos digitales -terrenos, edificios, objetos, avatares- pueden crearse, comprarse y venderse. Esto cambiará la cultura y las expectativas del comportamiento digital", afirma Nicolás Goldstein, presidente ejecutivo de Accenture, en entrevista con el Diario Financiero.

  Si bien es una tecnología incipiente en Chile, se cree que en los próximos años tendrá un crecimiento explosivo y las personas cada día interactuarán más en este metaverso, esto crea una oportunidad para las empresas ya que podrían generar experiencias personalizadas para los usuarios con un costo mucho menor de operación, como por ejemplo sucursales virtuales u otras aplicaciones.

  Esta situación, no sólo genera una oportunidad para las empresas sino también para los ciberdelincuentes, es por esto por lo que a medida que más empresas entren en el metaverso, existirá la necesidad creciente de tomar medidas de seguridad que protejan a las organizaciones y a las personas.

- **5G** "Equivale a la masificación de la conectividad de alta velocidad, a billones de sensores y dispositivos interactuando de manera inteligente en tiempo real, lo que conlleva un gran desafío en términos de despliegue tecnológico", dice Francisco Guzmán, director de Claro Empresas. en entrevista con el Diario Financiero.

  Si bien el 5G trae preocupaciones a algunos sectores por las ondas milimétricas en adición a las microondas y a las afectaciones que esto podría generar en la salud de las personas, esta no es la única preocupación ni situación de complejidad en la adopción, ya que si sumamos la cantidad de sensores y dispositivos que tendrán una conexión de alta velocidad, con la

tendencia del Big Data, el resultado es contar con grandes cantidades de información modeladas que podrían inferir en el comportamiento humano y generar cambios de conducta que las personas verían como naturales. Ir conduciendo un automóvil en el futuro y ver publicidades en la calle dirigidas tal cual las redes sociales, adaptadas a cada persona podría ser una realidad en el corto plazo, es por esto y por otras situaciones que la discusión de la adopción del 5G no es sólo por la salud de las personas sino también ética y de privacidad.

- **Inteligencia Artificial**
  Víctor Muscillo, líder de Tecnología y Transformación de Oracle en Chile, en entrevista con el Diario Financiero, afirma que la IA "está encontrando rápidamente un lugar en el corazón de las organizaciones", por su capacidad de automatizar tareas, anticipar tendencias y reducir el tiempo en puesta de marcha de soluciones.

  La suma de las tendencias tecnológicas, llega a su apogeo con la implementación de la IA, esto es más que ciencia ficción y día a día los dispositivos conocen más a las personas, incluso más que ellos mismos, esto conlleva debates éticos y de privacidad de los datos que aún están sin resolver y las personas muchas veces por no informarse entregan informaciones que realmente no les gustaría compartir y peor aún esta información es procesada y mediante la aplicación de modelos matemáticos y estadísticos se pueden inferir sentimientos y emociones de las personas.
  La adopción de estas tecnologías en las organizaciones puede traer innumerables beneficios y eficiencia en los procesos, por ejemplo, los *call centers* serán cada vez más automatizados en algunos años hablar en lenguaje natural con una máquina será una realidad y así como están estas aplicaciones con el tiempo serán cada vez más comunes en diferentes funciones en las empresas.

- **Ciberseguridad,** al ver las tendencias tecnológicas que van día a día creciendo en el uso de los datos, sensores y dispositivos conectados a internet de alta velocidad (permitiendo análisis en tiempo real de las informaciones) y el mayor uso de estos por las organizaciones y personas en su día a día, se puede observar un crecimiento en las necesidades de ciberseguridad para los próximos años en Chile y el mundo, dado que los ciberdelincuentes van avanzando rápidamente en el uso de las nuevas tecnologías y ataques relacionados a secuestro informático (ransomware) o suplantación de identidad tendrán cada día nuevas formas de afectar a las empresas y personas. Es por esto que la adquisición de medidas de

seguridad se verá en alza en los próximos años ya no sólo pensando en las grandes empresas sino también en las pequeñas, medianas y también las personas.

"Mientras la tecnología siga cambiando, evolucionando y logrando mayor penetración en el día a día de las personas, organizaciones y gobiernos, este tema no dejará de ser un riesgo", dice Nicolás Corrado, socio líder de Ciberseguridad en Deloitte, en entrevista con el Diario Financiero.

9.5. LEGAL

El marco legal en Chile ha estado en constante evolución en los últimos años y se vienen diferentes desafíos para los próximos años relacionadas principalmente con la protección de datos de las personas, propiedad intelectual y la ley marco en ciberseguridad, a continuación, algunos de los principales aspectos legales que vivirá Chile en los próximos meses y años:

- La modificación del artículo de la Ley 19.496, [15]sobre derechos del consumidos incorporó exigencias especificas en torno a la protección de datos personales a las empresas reguladas en temas de consumo.
- La implementación de la política nacional de inteligencia artificial y la política nacional de ciberseguridad, son 2 grandes de safíos a implementar en los siguientes años, para el 2022 esta última plantea los siguientes objetivos:

    - El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos
    - El Estado velará por los derechos de las personas en el ciberespacio
    - Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales.
    - El país establecerá relaciones de cooperación en ciberseguridad con otros actores y participará activamente en foros y discusiones internacionales
    - El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos.

[15] https://www.bcn.cl/leychile/navegar?idNorma=1160403

- El congreso finalizó la tramitación de la reforma a la Ley 19.2223 sobre delitos informáticos incorporando nuevas figuras delictivas y ajustando la normativa al convenio de Budapest, al que Chile se suscribió inicialmente 2017 y en mayo de 2022 suscribió el segundo protocolo adicional sobre ciberdelincuencia.

Si bien este no es un escenario favorable para la inversión ya que hay una alta incertidumbre referida al entorno político y económico del país, por lo que empresas podrían caer en *default* en los próximos años, también abre oportunidades a nuevas empresas que podrían aparecer en el mercado ofreciendo servicios más eficientes a costos menores que las grandes empresas, esto impulsado por las tendencias regulatorias y tecnológicas de Chile para los próximos años.

9.6. CONCLUSIONES PESTEL

Luego de analizar las diferentes variables del macroentorno, se puede ver un escenario favorable para la implementación de la consultora de ciberseguridad, dado el aumento en el uso de tecnologías y nuevas tendencias diversificación del ataque y las nuevas leyes que entrarán en vigor en los próximos años. Adicionalmente a esto el entorno macroeconómico y su incertidumbre hará que las empresas trabajen en abaratar sus costos, lo que podría abrir la oportunidad que nuevos competidores ingresen a este mercado.

10. ANALISIS DEL ENTORNO (5 FUERZAS)

10.1. AMENAZA DE NUEVOS PARTICIPANTES

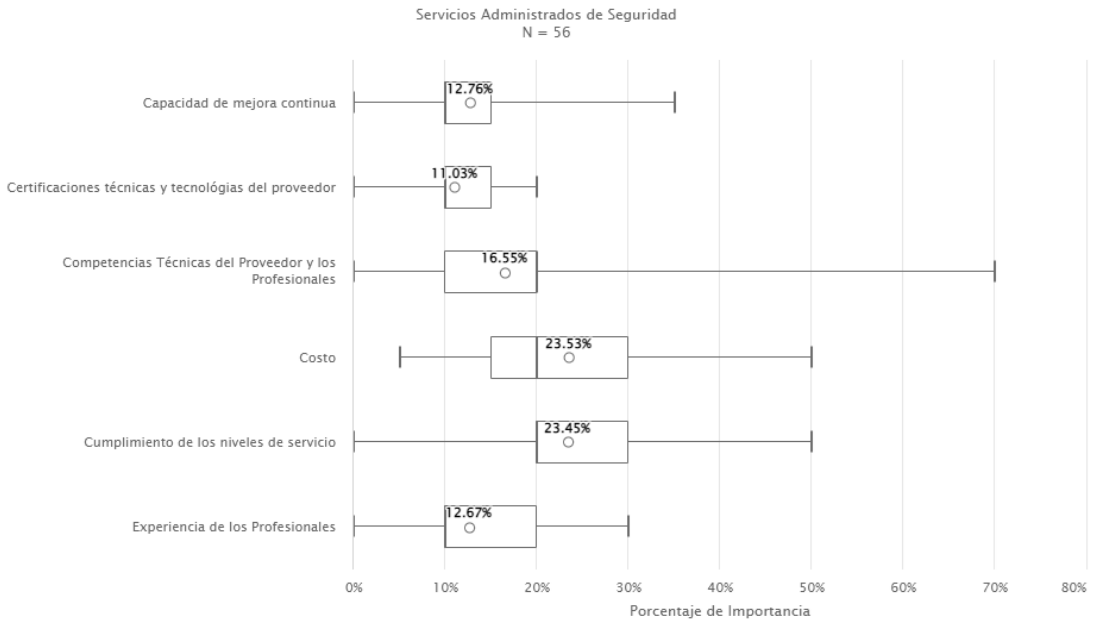
En el mercado chileno existen varias empresas dedicadas exclusivamente a temas de ciberseguridad y otras que si bien su *core bussiness* es tecnológico, han empezado a entrar en el mundo de la ciberseguridad, si bien actualmente no hay un catastro de empresas en Chile que prestan servicios de ciberseguridad, de acuerdo con indagaciones propias realizadas en este plan de negocio se puede mencionar que hay al menos 30 empresas dedicadas exclusivamente a este ámbito, lo que muestra una oferta variada para el mercado chileno, en este contexto las barreras de entrada actualmente están dadas por el capital humano y la especialización que estos tengan. Un ingeniero en ciberseguridad se forma por la práctica y el aprendizaje de diferentes técnicas en el tiempo, por lo que no todo ingeniero en tecnologías se puede convertir rápidamente en un ingeniero de ciberseguridad. Esta situación genera que las principales barreras de entrada a este negocio sean el conseguir los mejores profesionales.

En este contexto, existen empresas especialistas que en el tiempo han conseguido formar profesionales expertos, lo que para las empresas que ingresan en este mercado es difícil de conseguir, por lo que cualquier nueva empresa que quiera explorar en la entrada de este mercado tendrá que comprar el conocimiento y conseguir profesionales con alto nivel de conocimiento si quiere mantenerse.

Por otra parte, las principales empresas relacionadas con ciberseguridad tienen una oferta de servicios más bien estándar, que incluye servicios de consultorías, implementación de proyectos y servicios gestionados, que requieren de una contraparte con conocimiento en el tema, es decir requieren de la función de ciberseguridad interna en la empresa.

En la figura 11, se pueden observar las variables más críticas que consideran las empresas chilenas a la hora de evaluar a un proveedor, siendo el costo y el cumplimiento de los niveles de servicio las que tienen mayor relevancia.

Figura 11. Criticidad de variables para evaluar a un proveedor



Fuente: CE IT

De igual manera, de acuerdo con las proyecciones realizadas por Gartner[16], dado el crecimiento de los ciberataques y el aumento de uso de tecnologías, la demanda

[16] https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022

por servicios de ciberseguridad es mayor día a día, lo que ha generado la aparición de nuevas empresas prestadoras de servicios.

Esto genera que el mercado tenga muchos competidores, pero con alta demanda de servicios, por lo que hay oportunidades para la entrada de nuevos competidores, dada la granularidad del mercado.

Actualmente, no existen barreras legales para la creación de empresas en este rubro ni regulaciones específicas que se deban cumplir, al contrario, el nuevo marco legal de Chile relacionado con la ciberseguridad fomenta la implementación de controles que protejan las informaciones de las personas y combatan el cibercrimen.

Para analizar en detalle la oferta de servicios de ciberseguridad en las pyme, se realizó una búsqueda de proveedores que ofrecen servicios a empresas en Chile, por lo que se analizó la oferta de 10 empresas que prestan este tipo de servicios(como se puede ver en el Anexo C), de aquí se observa que el 90% de ellas no cuenta con servicios de suscripción mensual a través de la web y la modalidad de contacto es a través de formularios o correo electrónico, por otra parte la única empresa del análisis que cuenta con esta modalidad de suscripción es Movistar, quienes ofrecen un servicio de protección que incluye la implementación de herramientas en los equipos de las personas, esta suscripción es mensual, por usuario con base en un contrato anual, este servicio no incluye acompañamiento de la estrategia de la seguridad ni un programa de concientización, por otra parte solo 2 de las empresas analizadas se dedican exclusivamente a ciberseguridad, las otras prestan diferentes servicios tecnológicos en donde la ciberseguridad es uno más

10.2. PODER NEGOCIADOR DE LOS PROVEEDORES

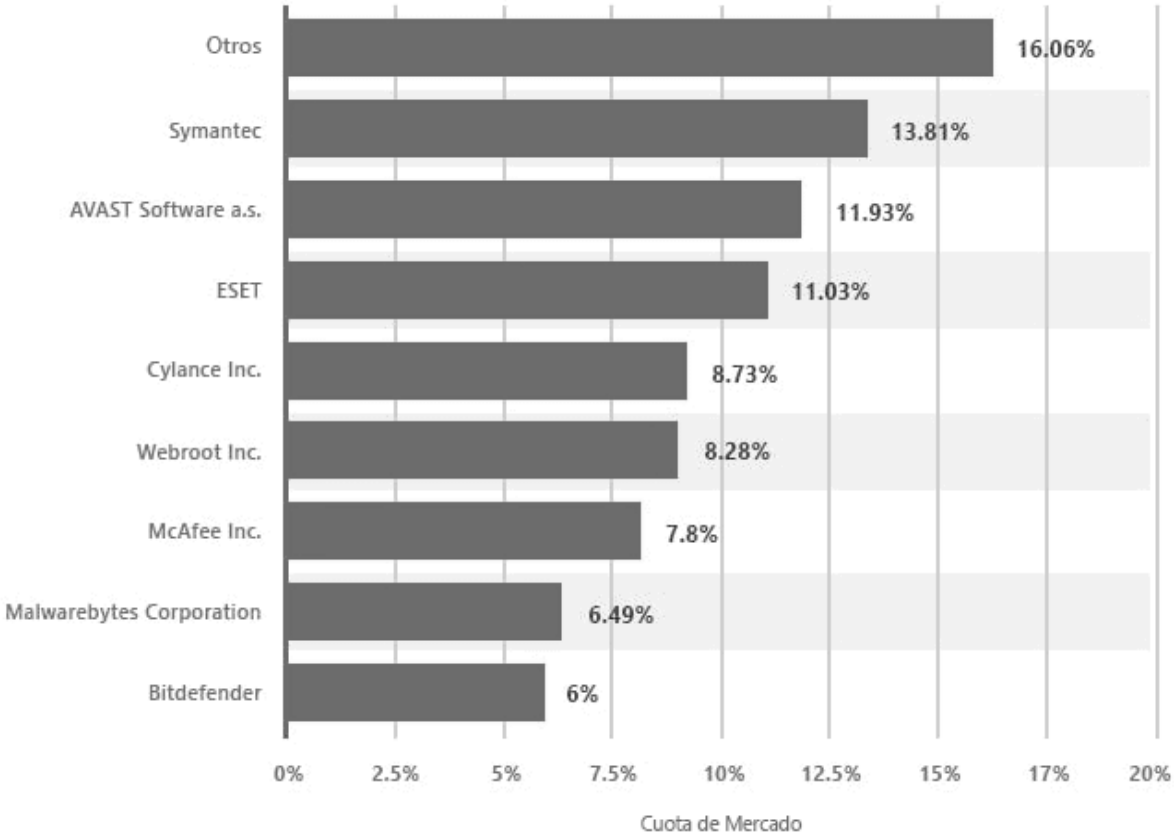
Actualmente existen diferentes tipos de servicios relacionados a la ciberseguridad, de acuerdo con la figura 9; Cadena de valor servicios de ciberseguridad, de este documento si pensamos en proveedores se debe situar la mirada en los primeros 2 bloques, relacionados con la fabricación o desarrollo de soluciones de ciberseguridad o en la distribución de estas.

Con respecto a la fabricación de soluciones, la mayoría de estas es realizada fuera de Chile, en países como Estados Unidos, China, Japón, Israel y algunos países de Europa, por lo que para acceder a vender sus servicios existe la posibilidad de acercamiento directo o a través de distribuidores definidos por país, en algunos casos se requiere de personal certificado para trabajar con determinadas herramientas, en este sentido la posibilidad de una empresa negociar con los

fabricantes más grandes es reducida, por lo que se está a merced de los precios que pueda determinar el mercado en estas situaciones.

En la figura 12, se puede observar la distribución del mercado en los fabricantes de antimalware, la que se concentra principalmente en 4 empresas.

Figura 12. Cuota de mercado de los mayores desarrolladores de antivirus para Windows.



Fuente: statista

Si bien esta es una situación de pocos proveedores, han aparecido nuevos actores en el desarrollo de soluciones, los que han apuntado a personalizar y adaptar sus soluciones a las necesidades específicas de algunas industrias, incluso en Chile hay algunas empresas que han tomado este camino en el desarrollo de soluciones relacionadas con la gestión de vulnerabilidades y monitoreos de seguridad, tales como *camel secure y widefense*.

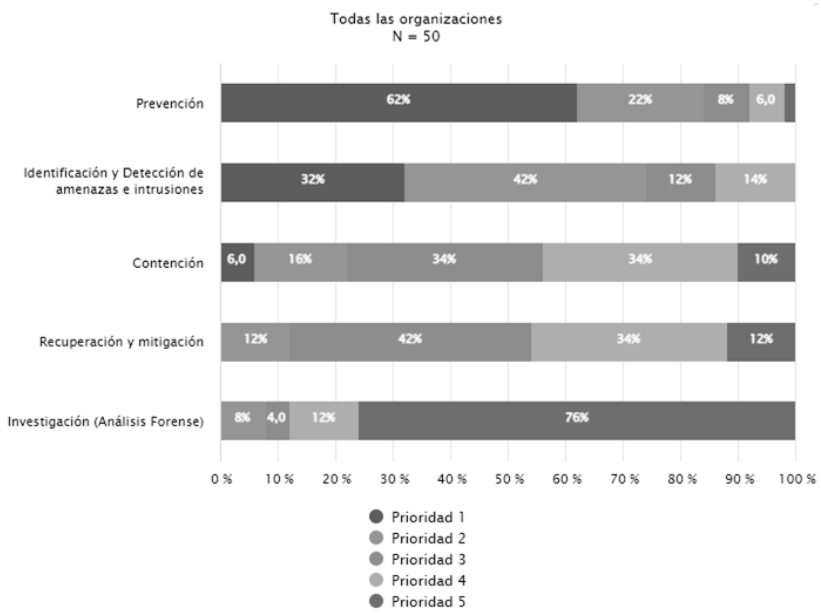
Esto muestra que existe una oferta de proveedores de herramientas de ciberseguridad amplia permitiendo evaluar diferentes opciones a la hora de construir un catálogo de servicios.

10.3. PODER NEGOCIADOR DE LOS COMPRADORES

Como se ha mencionado en este plan de negocios, habrá un crecimiento exponencial de la necesidad de protección de la infraestructura y los datos en los próximos años tanto a nivel nacional como internacional. Esto empujado por el avance tecnológico y las nuevas normativas que imponen más restricciones en el uso de los datos de las personas, en ese sentido en Chile el sector de las empresas privadas se verá obligado a implementar soluciones de seguridad, no sólo por garantizar la integridad, disponibilidad y confidencialidad de sus sistemas, sino también por los requerimientos regulatorios.

En un estudio realizado por universidad católica, se puede observar las prioridades de inversión de las empresas chilenas de acuerdo con las actividades a realizar, en este contexto las actividades orientadas a la prevención y detección de amenazas tienen la primera prioridad

Figura 13. Prioridades de inversión



Fuente: ENC I

Si bien este es un estudio acotado con 50 empresas chilenas muestra una tendencia que las empresas prefieren invertir en prevención que en remediación.

Por otra parte, como se observaba en la figura 11, uno de los puntos de mayor criticidad a la hora de escoger a un proveedor es el costo, de acuerdo con entrevistas realizadas con dueños de pequeñas y medianas empresas uno de los factores determinantes a la hora de decidir sobre la implementación de herramientas

de seguridad o de contratación de servicios relacionados es el costo, por lo que dependiendo del tamaño de la empresa la sensibilidad puede ser mayor o menor.

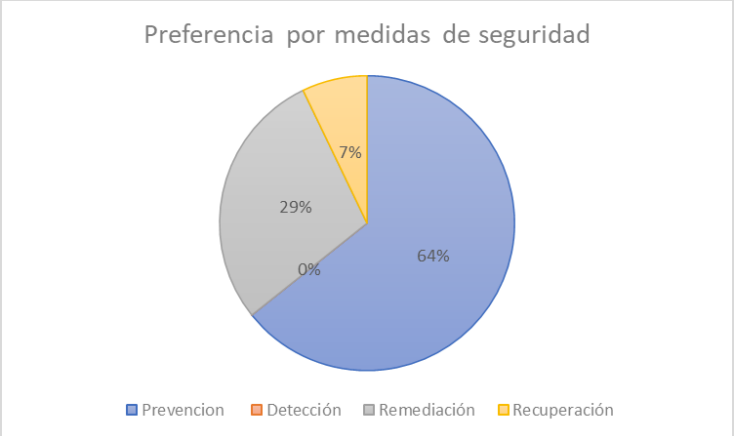
Estos resultados fueron contrastados con entrevistas realizadas a lideres de pequeñas y medianas empresas en Chile, estas se realizaron entre los meses de enero y junio de 2022, realizándose un total de 14, con los siguientes resultados (Las preguntas realizadas en las entrevistas se encuentran en el Anexo D de este documento):

- Se observa un bajo nivel de concientización en temas de ciberseguridad en las empresas entrevistadas, si bien el 70% de los entrevistados declara que le preocuparía a sufrir un incidente de este tipo, no lo ve como algo probable que puede ocurrir en su empresa, sino más bien en otras industrias, el otro 30% declara que no está preocupado por sufrir incidentes relacionados con ciberseguridad, viendo está posibilidad como algo remoto.

- En el momento de preguntar por ¿Cuál o cuáles son los factores determinantes de no invertir en ciberseguridad? Las respuestas se orientaron al costo, desconocimiento de las herramientas y desinterés, siendo el costo el más valorado en las entrevistas.

- Al preguntar por las medidas de seguridad en las que preferiría invertir, el 40% declaró que no conocía las opciones al ser preguntas abiertas se explicaron 4 grandes alternativas, prevención, detección, remediación o recuperación, explicando en la entrevista de manera general cada una de estas opciones, los resultados fueron los siguientes:

Figura 14. Prioridades de Inversión



Fuente: Elaboración Propia

- Con esta respuesta se puede confirmar la tendencia planteada por el estudio realizado por el ENCI, si bien no hay una relación entre las empresas del estudio con las que participaron de las entrevistas, el resultado da una tendencia que puede ser utilizada para plantear las soluciones en esta línea de trabajo. en remediación o recuperación.

- Por otra parte, se preguntó por las medidas de seguridad que actualmente tienen las empresas, obteniendo como resultado que el 70% no tiene conocimiento del nivel de protección actual de su operación esto sumado a que el 100% no cuenta con un plan de recuperación o de manejo de incidentes de ciberseguridad definido, es una combinación que pone en riesgo las operaciones de cualquier compañía.

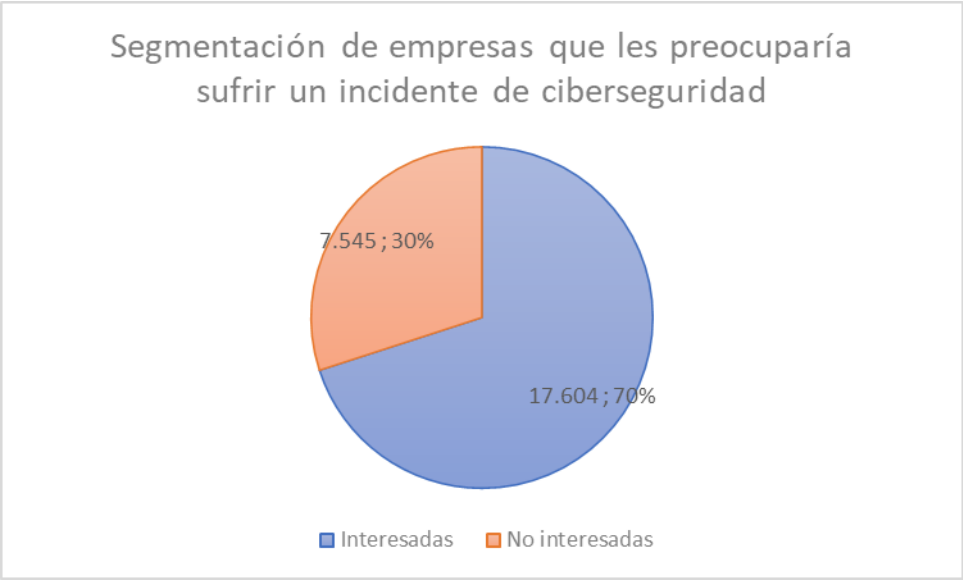
- Por otra parte, se consultó si estarían dispuestos a contratar a personas dedicadas a temas de ciberseguridad de manera interna en la empresa, a lo que el 100% respondió que no está interesada.

Como dato adicional a la entrevista realizada, varias de las personas entrevistadas se mostraron más interesadas en evaluar servicios de ciberseguridad posterior a la entrevista, por lo que se detecta que se debe realizar la sensibilización previo al ofrecimiento de servicios de esta materia.

Producto de las entrevistas y los estudios analizados en este plan se puede observar que existe un grupo potencial de clientes del total de pymes chilenas, en el que se encuentran aquellas que cuentan con 1 o más trabajadores dependientes y cuentan con ventas entre 25.000 y 75.000 UF al año lo que representa 25.149 empresas con potencialidad de clientes, de estos el 70% podría estar preocupado por sufrir un incidente de ciberseguridad

.

Figura 15. Segmentación de pymes chilenas

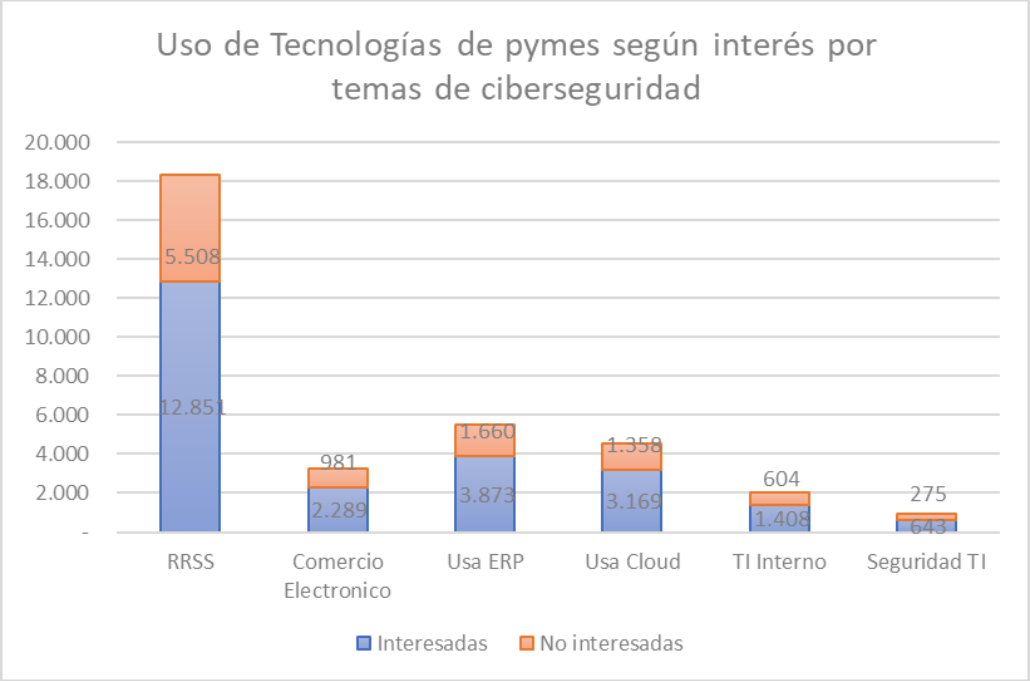


Fuente: Elaboración Propia

Por otra parte, de acuerdo con la Encuesta de Acceso y Uso de Tecnología de Información y Comunicación (TIC) en Empresas, realizada por el ministerio de Economia de Chile(ver Anexo E), se pueden desprender los siguientes datos:

- El 73% de las pymes chilenas utiliza redes sociales para publicidas y un 24% cuenta con presencia activa.
- El 13% de las pymes realiza comercio elecronico
- El 22% de las pymes declara usar sistema ERP
- El 18% de las pymes declara usar servicios de cloud computing
- El 8% de las pymes declara contar con personal TI interno.
- El 5% de las pymes cuenta con encargado de seguridad tecnológica.

Figura 16. Tecnología e interés en la ciberseguridad



Fuente: Elaboración propia, tomando como base la información del ministerio de economía de Chile

10.4. AMENAZA DE SUSTITUTOS

En los productos sustitutos relacionados a la protección ante incidentes de ciberseguridad se podrían considerar los seguros o ciberseguros, estas son pólizas que poco a poco se han masificado en distintos países y han comenzado a llegar a Chile, de la mano de algunas aseguradoras.

Si bien esto no es una protección directamente ante incidentes, podría prevenir el impacto económico que tenga un incidente de ciberseguridad, mas no los impactos reputacionales o regulatorios a los que se podrían enfrentar las compañías, adicionalmente la llegada de los ciberseguros que cubren el pago del secuestro de datos se convierte en un anzuelo para los cibercriminales, ya que saben que la probabilidad de pago de rescate aumenta considerablemente.

Por otra parte, un sustituto a los servicios externalizados es realizar las funciones de manera interna en las empresas, lo que no para todas es factible, dados los costos del personal especialista en ciberseguridad[17] o tecnología como se puede observar en la figura 17.

[17] https://it-talenthh.com/2021/01/24/estudio-rentas-profesionales-to-2021/

Figura 17. Tipo dificultades para contratar especialista TIC

Fuente: Encuesta TIC, Ministerio de economía de Chile

En este contexto para empresas medianas y grandes la opción de internalizar la función podría estar presente en el mediano largo plazo dependiendo de su plan estratégico y regulaciones particulares, para el caso de las empresas pequeñas y algunas medianas esto es un poco más complejo.

10.5. RIVALIDAD ENTRE LAS EMPRESAS EXISTENTES

El mercado de la ciberseguridad, dado que está fuertemente relacionado con los servicios cuenta con barreras de salida bajas, lo que lo hace muy atractivo para ingresar, el punto de dificultad es principalmente la captación de buenos profesionales especialistas, los que no serán baratos para iniciar y en ocasiones para conseguir contratos con los grandes fabricantes no será fácil ya que se debe contar con una serie de requisitos. La rivalidad de las empresas participantes de este mercado es moderada, dado que hay una amplia demanda, si bien las empresas que invierten fuertes sumas de dinero en ciberseguridad son menos, existe un gran número de empresas que podrían requerir de servicios de ciberseguridad.

Luego de analizar las 5 fuerzas, se puede observar que el mercado de la ciberseguridad en Chile es atractivo para la inversión, dado que es un escenario con bajo costo de salida y la rivalidad en el mercado es moderada, además de estar fragmentada lo que permite el ingreso de nuevos competidores en la escena.

11. PLAN ESTRATEGICO

Luego de analizar el micro y macro entono, se evalúan a través de un análisis FODA la situación en la que la consultora se encuentra dado el escenario descrito, en este contexto las situaciones observadas con las siguientes:

11.1. ANALISIS FODA

11.1.1. FORTALEZAS

Las fortalezas en el desarrollo de este plan de negocios están dadas por el conocimiento y la experiencia en el negocio del liderazgo del proyecto y la utilización de marcos de referencia de seguridad probados internacionalmente, esto ayuda a la consultora a generar una expectativa en los potenciales clientes. Por otra parte, el proceso de selección de los consultores debe ser robusto y exhaustivo para garantizar que los talentos del equipo sean un diferencial frente a la competencia.

11.1.2. OPORTUNIDADES

La nueva legislación chilena en torno a la materia de ciberseguridad y el aumento en el uso de tecnologías por las diferentes empresas genera oportunidades para el ingreso de nuevas empresas en el mercado de la ciberseguridad chilena. Por otra parte, las empresas requerirán de mayores controles que permitan asegurar la información de las personas, esto pasará de ser un diferenciador a ser una necesidad en el corto plazo, por otra parte la situación económica de Chile generará que muchas empresas busquen eficiencia en sus presupuestos, por ende se abran a la posibilidad de diversificar sus soluciones en ciberseguridad con el objetivo de abaratar costos pero mantener un ambiente de control adecuando en este aspecto, por lo que nuevas empresas podrán entrar en la escena aprovechando estas situaciones.

11.1.3. DEBILIDADES

Como debilidad, al ser una empresa nueva, esta no es conocida ni tiene un renombre en la industria, situación que debe ser revertida a través del plan de marketing. Por otra parte, la conexión con los grandes fabricantes de soluciones de ciberseguridad es compleja de conseguir sin los clientes existentes, por lo que hacer alianzas estratégicas con empresas fabricantes de diferentes tamaños es de suma importancia, de manera de diversificar el portafolio de soluciones a ofrecer.

11.1.4. AMENAZAS

Dado que es un mercado con bajas barreras de entrada y de salida, la aparición de nuevos competidores se puede tornar una amenaza ya que por ejemplo para una empresa de tecnología agregar el servicio de ciberseguridad es más fácil que iniciar un negocio desde cero, ya que tiene la ventaja de contar con un portafolio de clientes a los que solo debería ofrecer un nuevo servicio, esto se torna una amenaza dada la debilidad presente de no contar con el conocimiento de la empresa.

Por otra parte, el mundo de la ciberseguridad es un negocio complicado, ya que la credibilidad de las empresas se logra con los años de experiencia de las personas y de la compañía, por lo que en caso de contar con clientes y ocurrir situaciones como incidentes de ciberseguridad graves, podrían significar la pérdida de credibilidad y en consecuencia la de clientes. Es por esto que asegurar los estándares de calidad de los servicios y la calidad de los profesionales es un factor clave del éxito de la implementación de la consultora.

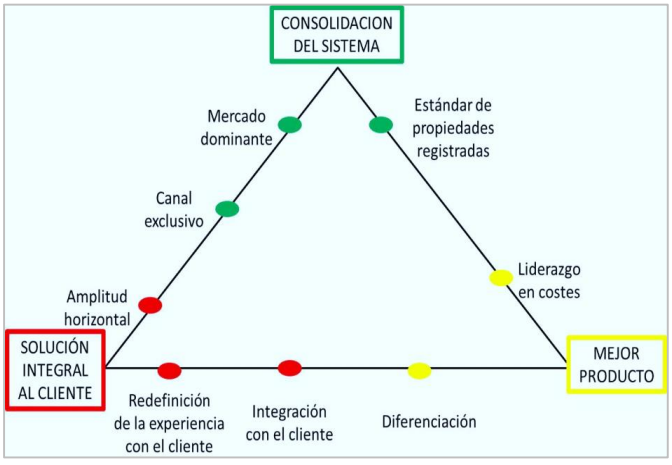
11.1.5. CONCLUSIONES FODA

En conclusión, se observa que, si bien existen amenazas de ingreso de nuevos competidores al mercado y el ser una nueva empresa que no es conocida en este rubro puede generar que el crecimiento inicial no sea rápido, se observan condiciones favorables para la implementación de la consultora, siempre y cuando se logre sensibilizar a las empresas y realizar una oferta de valor atractiva con un modelo de inversión para las ad hoc pymes.

11.2. ESTRATEGIA COMPETITIVA

Como fue definido en el capítulo de metodología, la definición del plan estratégico está basada en el modelo Delta de Arnoldo Hax, de acuerdo con la figura 18:

Figura 18. Tipo dificultades para contratar especialista TIC



Fuente: The Delta Model. Reinventing Your Business Strategy, Arnoldo C. Hax

Este plan de negocios está basado en una empresa que inicia sus actividades en un mercado emergente, por lo que la estrategia considera las condiciones del entorno más las dificultades propias de un emprendimiento en Chile. A continuación, se detallan los puntos relacionados con cada aspecto del modelo.

11.2.1. MEJOR PRODUCTO

Alineado con los objetivos específicos de este plan, esta es una de las estrategias a seguir por la consultora, principalmente relacionada con la entrega de servicios a precios accesibles y disruptivos para las pymes chilenas. A continuación, se detalla el enfoque por cada opción de “Mejor producto”.

Liderazgo en costo: De acuerdo con el análisis de los clientes (Pymes chilenas), el principal motivo de no inversión en ciberseguridad está relacionado con el costo de los servicios, por lo que es ahí donde entrará la consultora, con un modelo de suscripción mensual por empleado de la empresa con 2 servicios que serán detallados en el plan de marketing de este documento. La idea es apuntar a la masividad de clientes, con precios adaptables a la realidad de las pymes, pero con un modelo escalable que permita avanzar en los niveles de protección a medida de la necesidad.

Por otra parte, uno de los servicios de la consultora estará orientado a la autoevaluación de los riesgos de ciberseguridad de manera gratuita, entregando consejos a seguir dependiendo del nivel de seguridad que la empresa tenga, con esto se apunta a que incluso aquellos emprendedores que inician su negocio puedan hacerlo conscientes de los riesgos que enfrentan.

Diferenciación: De acuerdo con el análisis de las 5 fuerzas, se observa que están orientadas principalmente a aquellas empresas que ya cuentan con un nivel de madurez en seguridad y que por lo general cuentan con personal dedicado internamente para las labores de ciberseguridad. Por otra parte, las empresas objetivo de los principales competidores cuentan con grandes presupuestos asociados a ciberseguridad, por lo que las empresas más pequeñas quedan sin una oferta específica para estos servicios, es aquí donde pensar los servicios de manera diferente y conseguir economías de escala producto de un modelo de colaboración y cooperación es clave. En este sentido la consultora entregará un servicio diferente a los actuales simplificando el entendimiento de la ciberseguridad con un número reducido de servicios adaptados a la realidad de las pymes y alineados con las necesidades de protección.

11.2.2. SOLUCION INTEGRAL AL EL CLIENTE

En este punto es releva te mencionar que el mercado objetivo de la consultora no son las empresas que cuentan con la función de ciberseguridad internamente, pero que si estuvieran dispuestas a invertir en este ámbito. A continuación, se detalla el enfoque por cada opción de “Solución integral al cliente”.

Redefinición de la experiencia con el cliente: Como se pudo observar en el análisis de 5 fuerzas, existe una preferencia a invertir en el ámbito de la prevención de los riesgos relacionados a la ciberseguridad, es por esto por lo que es clave que los clientes de la consultora perciban que, al suscribir los servicios su nivel de protección aumenta cada día.

Es por esto por lo que el modelo operacional definido en capítulo 13 de este documento muestra en detalle el funcionamiento de cada servicio con entregables claros con diferentes periodos de envío, en donde el cliente sentirá que está protegido y hay un *socio* preocupado por la seguridad de su empresa.

Integración con el cliente. En este punto, la estrategia de la consultora es apoyar a los clientes en la mejora de los niveles de protección frente a los riesgos de ciberseguridad con el menor impacto en su operación diaria, para que de esta manera los clientes puedan dedicar los esfuerzos al *core* de su negocio.

Amplitud horizontal. Como parte fundamental de la estrategia debe ser la amplitud de la motivación de los clientes de adquirir servicios de ciberseguridad que de acuerdo con el análisis realizado está directamente relacionado con la concientización en estos temas, por lo que la estrategia de publicidad de la empresa debe estar fuertemente centrada en concientizar en la necesidad de contar con medidas de ciberseguridad más allá de solo promocionar los servicios en particular.

11.2.3. CONSOLIDACION DEL SISTEMA

Canal exclusivo. En este aspecto como se ha mencionado anteriormente, la estrategia de la consultora es ubicarse en un sector del mercado que no cuenta con una oferta especifica, con lo que se pretende colonizar nuevos puntos del mapa de esta forma, sin contar con una competencia directa inmediata ni con productos sustitutos que generen una amenaza inminente, de todas maneras se deben centrar los esfuerzos del plan de marketing en entrar fuertemente al mercado, con una estrategia de conocimiento de marca y sensibilización de las empresas, en este punto se debe pensar en modelos de suscripción mensual y anuales(a evaluar al cierre del primer año) para garantizar el *engagement* [18]de los clientes.

[18] Nivel de compromiso que tienen los consumidores y usuarios con una marca, y esto va más allá de la compra de sus productos o servicios

Mercado dominante. Apuntar a la masividad de clientes es clave en el éxito de la compañía por lo que generar alianzas con agrupaciones y asociaciones de emprendedores es una de las estrategias a evaluar para conseguir una mayor penetración en el mercado.

Estándar de propiedades registradas. En este punto lamentablemente al ser un modelo orientado a los servicios y de fácil replicabilidad de su construcción no es una opción inmediata el patentar el modelo operacional ni los servicios, los esfuerzos apuntarán posicionar la marca en el *top of mind* de las pymes chilenas, por lo que el foco en este aspecto será registrar la marca y contar con presencia en las diferentes redes sociales.

11.2.4. CONCLUSIÓN

Si bien al analizar los 3 puntos relacionados con el modelo de Arnoldo Hax se observa que en cada uno de ellos podría existir un potencial para encaminar el negocio, la estrategia definida para este plan es la de Mejor Producto, haciendo una fuerte diferenciación de la oferta actual adaptando las soluciones al segmento objetivo, por otra parte se buscará contar con precios acorde a las necesidades de los clientes, adaptándolos de acuerdo con el tamaño de estos.

11.3. VISIÓN

Ser una la compañía líder en soluciones de ciberseguridad para las pymes con el mejor nivel de satisfacción de clientes entregando soluciones sustentables y convenientes para los clientes.

11.4. MISIÓN

Ser la consultora de confianza en temas de ciberseguridad para las pymes chilenas, para lograrlo trabajaremos incansablemente para adaptar nuestros servicios a las necesidades de las pequeñas y medianas empresas.

12. PLAN DE MARKETING

Tomando como base los estudios analizados en este plan de negocios y las entrevistas realizadas para la profundización de resultados, se definen los siguientes objetivos del plan de marketing:

12.1. OBJETIVOS ESTRATÉGICOS

- Posicionarse en el *top of mind* de las pymes chilenas en el segmento objetivo en 1 año.
- Posicionarse como la principal consultora de ciberseguridad de las pymes chilenas en 5 años.

12.2. OBJETIVOS TÁCTICOS

- Conseguir captación de 180 clientes de suscripción mensual en el primer año de funcionamiento.
- Conseguir conexiones con asociaciones de emprendedores en Chile en el primer año de funcionamiento.

Para el cumplimiento de los objetivos se define el segmento objetivo, la declaración de posicionamiento y el análisis de las 4 Ps.

12.3. SEGMENTO OBJETIVO

Haciendo una proyeccion de los datos obtenidos de las entrevistas, más los analisis revisados en este plan se puede determinar que el segmento objetivo es:

Pymes chilenas que registran ventas anuales entre 25.000UF Y 75.000UF Anuales, que les preocuparía sufrir un incidente de ciberseguridad, con acceso a redes sociales, comercio electronico, ERP o servicios Cloud sin equipo de tecnología y/o ciberseguridad interno. Este segmento representa 17.604 pymes chilenas.

Por otra parte, tomando la media anual de las ventas de esta empresa(50.000UF), tomando como base la UF de junio de 2022($33.086,83), Este segmento de 17.604 empresas representa un total aproximado de ventas anuales de $31.315.083.619USD, por otro lado, de acuerdo con diferentes estudios analizados en este plan de negocios, se puede estimar que una empresa en promedio invierte en seguridad un 2% de sus ingresos anuales en este sentido se puede estimar un mercado potencial de $626.301.672USD anuales en Chile.

12.4. DECLARACION DE POSICIONAMIENTO

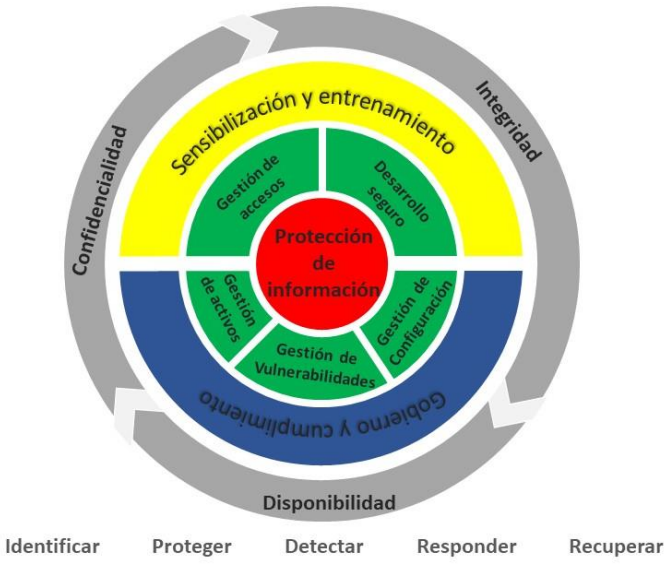
La declaración de posicionamiento busca apoyar la ejecución efectiva del plan de marketing, dada su principalidad, se declara posicionamiento lo siguiente:

“Para las Pymes chilenas que están interesadas en prevenir los incidentes de seguridad, es que esta es la consultora especialista que las acompañará en hacer sus operaciones seguras y con menos exposición a riesgos, porque somos emprendedores y conocemos el camino.”

12.5. PRODUCTO

Ya entendiendo el mercado en que se desenvolverá la consultora y conociendo el segmento objetivo y sus características, los esfuerzos apuntaron a desarrollar un framework de seguridad que pueda ser implementado en diferentes empresas con foco en la prevención de riesgos de ciberseguridad y la recuperación de incidentes, este framework es la base de los servicios que venderá la consultora y tomo como base los estándares internacionales NIST, controles CIS e ISO 27001, como se puede ver a continuación:

Figura 19. Framework de seguridad para PyMes



Fuente: Elaboración propia, basado en el Framework de ciberseguridad del NIST e ISO 27001

Con base en este modelo, se definen 3 servicios

- **Free**: Servicio gratuito orientado a sensibilizar a las empresas en temas de ciberseguridad, este servicio estará disponible a través del sitio web de la consultora y basado en un set de preguntas entregará el nivel de riesgo de la empresa autoevaluada acompañado de consejos a seguir para prevenir y protegerse de cada uno, es importante destacar que en estos consejos no habrá responsabilidad por parte de la consultora sobre la implementación de ellos, el seguirlos será de exclusiva responsabilidad de la persona que ingresa los datos. Por otra parte, los datos ingresados para la evaluación podrán ser utilizados como fuente de nuevos estudios y/o análisis comparativos de la industria chilena.

- **Conciencia**: Servicio suscripción mensual orientado a educar a los colaboradores de las empresas, este servicio consiste en la ejecución de ejercicios de Phishing, correos de sensibilización, cursos online, ejercicios de ingeniería social y reportes periódicos de ciberseguridad relacionados con la industria en la que se desenvuelve el cliente. Con el objetivo de mantener sensibilizados a los empleados y de esta manera prevenir incidentes de ciberseguridad. Este servicio es complementario a las herramientas de protección con que puede contar cada compañía y no asegura la no materialización de incidentes, pero busca prevenirlos y aminorar su impacto.

- **Virtual CISO:** Servicio de suscripción mensual orientado a acompañar en la estrategia de ciberseguridad a las empresas, este servicio apoya la gestión de riesgos e incidentes, el cumplimiento regulatorio, las campañas de concientización (pack conciencia adicional), gestión de los activos de información y la gestión del cumplimiento de los controles implementados. Una de las principales características de este servicio, es que permite a las empresas contar con personal certificado con amplio conocimiento y experiencia en temas de ciberseguridad a disposición de ellos, sin la necesidad de incurrir en los costos que conlleva tener un equipo completo dentro de la compañía.

Con estos 3 productos, se busca captar Pymes chilenas que están interesadas en prevenir los incidentes de seguridad, y acompañarlos en hacer más segura su operación.

12.6. PRECIO

En la definición del precio de los servicios se consideraron algunos datos estadísticos para la determinación del potencial presupuesto de ciberseguridad que podrían tener las pymes, en este contexto de acuerdo con diferentes estudios revisados, se puede obtener que las empresas podrían invertir hasta un 2% de su facturación anual en temas de ciberseguridad, entendiendo que esto es por el total de herramientas, se estima que para concientización el presupuesto rondaría el 30% de este valor. Por lo tanto, esto define el límite a cobrar por estos servicios, el que es de $10.673USD por año como para el segmento objetivo.

Si bien no se cuenta con un listado de precios detallados de los competidores, se pudo indagar que los valores por usuario para la ejecución de 1 ejercicio de concientización oscilan entre los 10 y 30 dólares, con algunos mínimos 50 usuarios, por otra parte, la oferta actual solo está definida como servicios puntuales y no como modelo de suscripción.

Es por esto por lo que la definición del precio para el servicio de concientización será de $24.990 con un mínimo de 10 suscriptores, con lo que se quiere avanzar con aquellas empresas con menos de 50 trabajadores como *target*.

Por el lado del servicio Virtual ciso, actualmente hay competencia en el mercado, y esta varía por la cantidad de personas de la empresa y el rubro en el que se encuentra, considerando la misma estimación anterior se definió el límite a cobrar y estimó el precio de $45.900 por suscripción mensual por este servicio, considerando un mínimo de 10 empleados.

Con estos precios, se espera ingresar al mercado objetivo con precios adaptables al tamaño y necesidades de las pymes.

12.7. CANALES DE VENTA O DISTRIBUCION

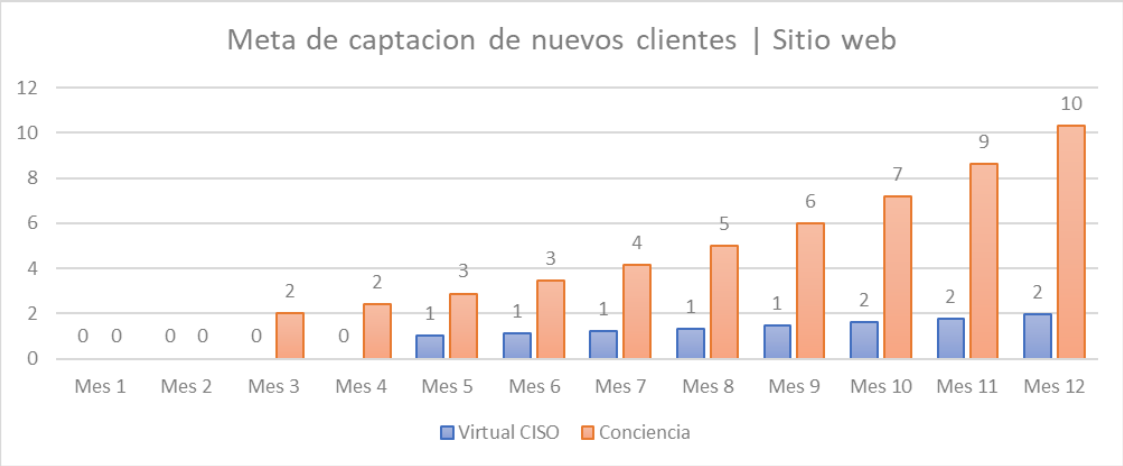
Dado que el modelo de venta es por suscripción mensual o anual, una vez que se consigue el cliente, la mantención de sus renovaciones estará dada principalmente por la calidad y percepción del servicio que entregue el modelo operativo. En cambio, la captación de nuevos clientes tendrá 2 canales de venta que se distribuyen de acuerdo con la figura 20.

Figura 20. Canales de distribución

Fuente: Elaboración propia

Si bien a través del sitio web se podrán contratar todos los servicios de la consultora, este tendrá el foco de distribuir los servicios Free y Conciencia, bajo la modalidad de suscripción mensual y anual, aquí la idea es que desde el modelo de autoatención del sistema free se genere la necesidad de contar con el servicio conciencia, las metas para el primer año en este canal son las siguientes:

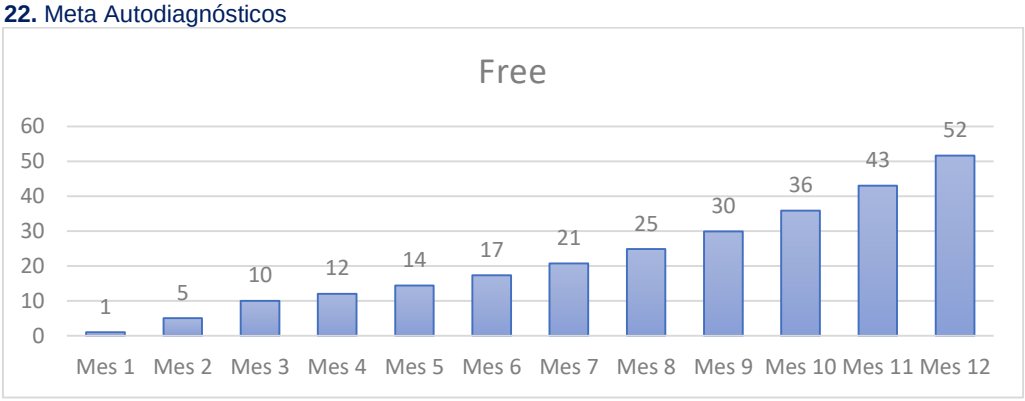
Figura 21. Meta captación suscriptores mensuales por canal web



Fuente: Elaboración propia

Con relación al servicio Free, el objetivo es conseguir el mayor número de autodiagnósticos en el primer año para realizar y publicar un estudio de ciberseguridad en el mundo pyme lo que será un instrumento de sensibilización para las empresas. El que será compartido con diferentes asociaciones de emprendedores y pymes para generar el vínculo, para esto se ha generado la meta de 266 autodiagnósticos realizados en los primeros 12 meses, de acuerdo con la siguiente figura:

Figura 22. Meta Autodiagnósticos

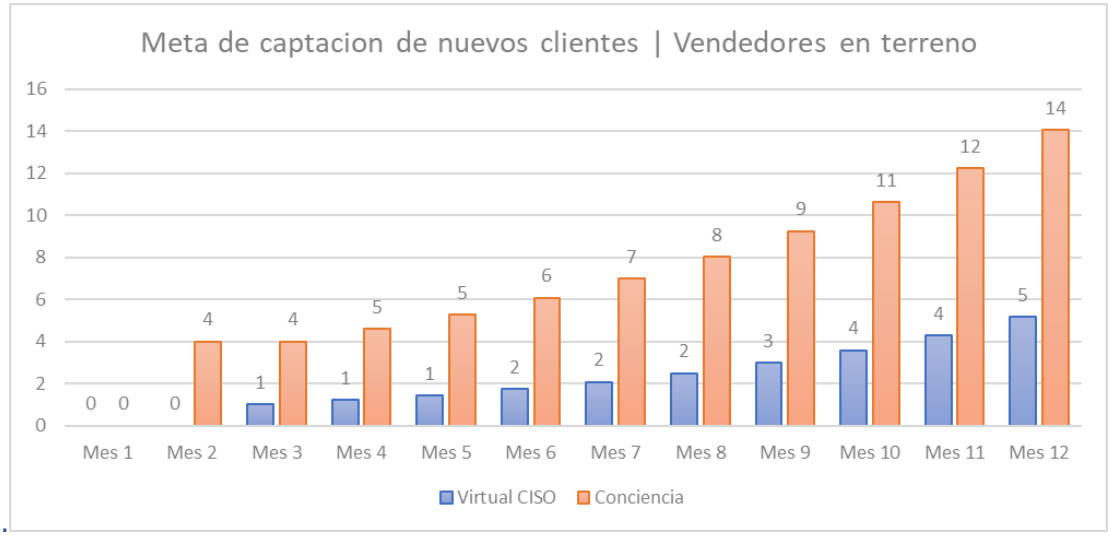


Fuente: Elaboración propia

Con relación a al canal presencial de vendedores en terreno, este tiene por objetivo vender principalmente los servicios de virtual ciso, si bien se generará una meta para el equipo de ventas relacionada con ambos servicios de suscripción mensual, se tendrán incentivos específicos en el primer año relacionados con el servicio virtual ciso, las metas relacionadas con este canal son definidas de acuerdo con el análisis de las entrevistas realizadas, donde se puede observar que al menos el 50% de los entrevistados mostró interés por comprar algún servicio, si se considera que el 20% de ese 50% podría concretarse como compra, y proyectarlo por la

cantidad de reuniones que podría conseguir un vendedor en un mes se realiza la siguiente proyección de metas para el canal presencial.

Figura 23. Meta vendedores en terreno



Fuente: Elaboración propia

Con estas metas, se busca conseguir el objetivo planteado del primer año de ventas, para los años subsiguientes se espera aumentar el número de suscriptores en un 20% anual.

12.8. PROMOCIÓN

Como se identificó en el análisis FODA, una de las debilidades de esta consultora es que no es conocida en el mercado, por lo que la campaña en los primeros meses de actividad debe ser con foco en el conocimiento de marca, para esto se deben realizar las siguientes actividades:

- Generar presencia en redes sociales, a través de campañas de sensibilización de ciberseguridad, para que las personas conozcan la marca y entiendan los riesgos a los que se podrían enfrentar.
- Realización de webinars gratuitos a emprendedores, para dar a conocer los riesgos y los servicios de la consultora
- Realizar reportaje en diarios de negocios, donde se dé a conocer la consultora y los riesgos relacionados con ciberseguridad
- Hacer conexiones con emprendedores reconocidos en Chile y conseguir embajadores de la marca.

Para esto se estima un presupuesto mensual de $2.000.000-. para los 6 primeros meses de funcionamiento de la consultora, luego se disminuirá a $1.000.000 para

los 6 meses restantes, llegando a un total de $18.000.000 anuales. En el segundo año el presupuesto se mantendrá.

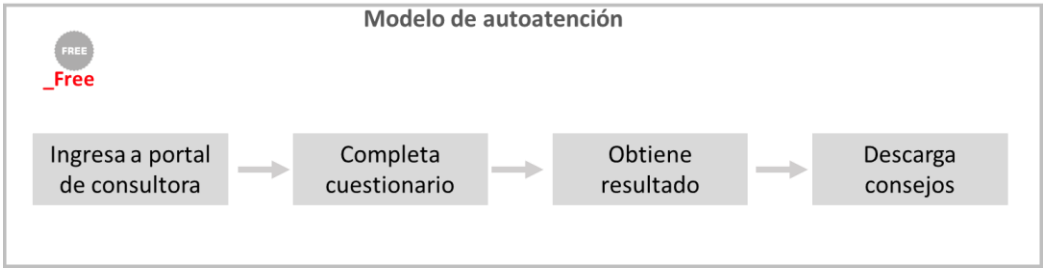
13. PLAN OPERACIONAL

13.1. OPERACIÓN DEL NEGOCIO

Para los 3 servicios definidos existe una cadena de valor en particular, las que se detallarán a continuación:

_**Free**: Este servicio estará disponible a través del portal de la consultora, las personas podrán ingresar l y autoevaluar su nivel de riesgo de ciberseguridad para los pilares del framework definido en este plan de negocios, con esto podrán obtener una guía gratuita de mejores prácticas dependiendo de su nivel de riesgo y madurez en temas de ciberseguridad, en este servicio los clientes solo interactuarán con el portal y no tendrán contacto con colaboradores de la consultora, a continuación se puede ver el flujo de autoatención:

Figura 24. Modelo de autoatención servicio _Free

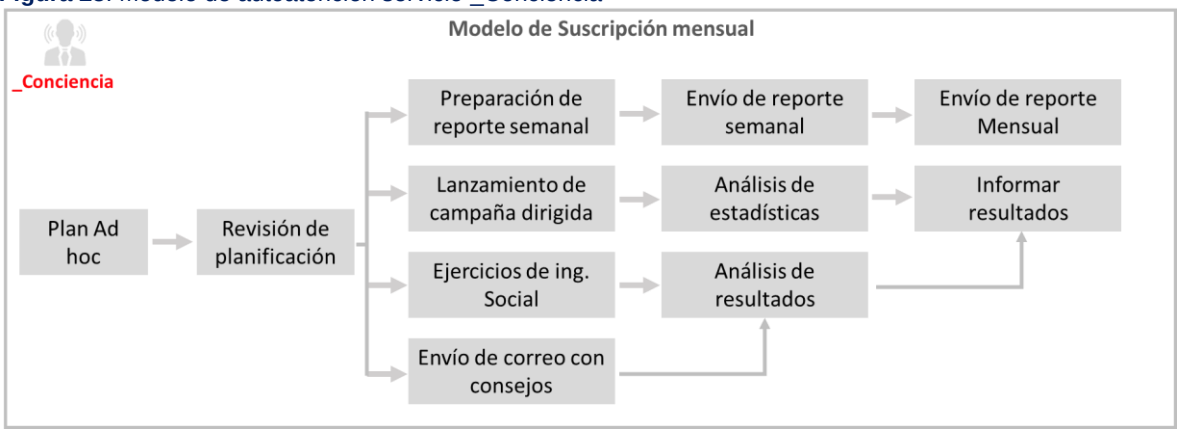


Fuente: Elaboración propia

_**Conciencia:** Este servicio puede ser operado por 1 analista cada 400 colaboradores o 50 empresas con suscripción mensual, dado que son servicios estandarizados que permitirán contar con mayor eficiencia en los ejercicios, este servicio inicia con la realización de un plan ad-hoc al cliente, dependiendo de la industria en que se desempeña, para esto debe completar un formulario a través del sitio y será contactado para una video llamada en la que se confirmarán y solicitarán algunos detalles, con lo que se realizará la planificación e iniciará el mes suscrito. Luego de la planificación el analista comienza el proceso de revisión y ejecución de los ejercicios, los ejercicios irán aumentando de nivel de complejidad con el tiempo ya que la idea es generar conciencia en las personas a través de la práctica, una vez se generen las campañas de envío de correo o ejecución de ejercicios de ingeniería social, se enviarán reportes semanales y mensuales con las informaciones y consejos para los colaboradores, en caso que sea necesario se pueden agendar charlas y cursos rápidos para mejorar la educación en estos aspectos, es importante que se mantenga el refuerzo de los conceptos y que las

personas logren identificar situaciones de riesgo, es por esto que también se enviarán campañas de correo con consejos de seguridad adaptados a cada empresa y/o industria, finalmente el analista preparará los reportes mensuales para ser enviados a cada cliente, en el tiempo se podrá ver la evolución de los colaboradores en estos aspectos. A continuación, se puede observar el modelo operacional.

Figura 25. Modelo de autoatención servicio _Conciencia



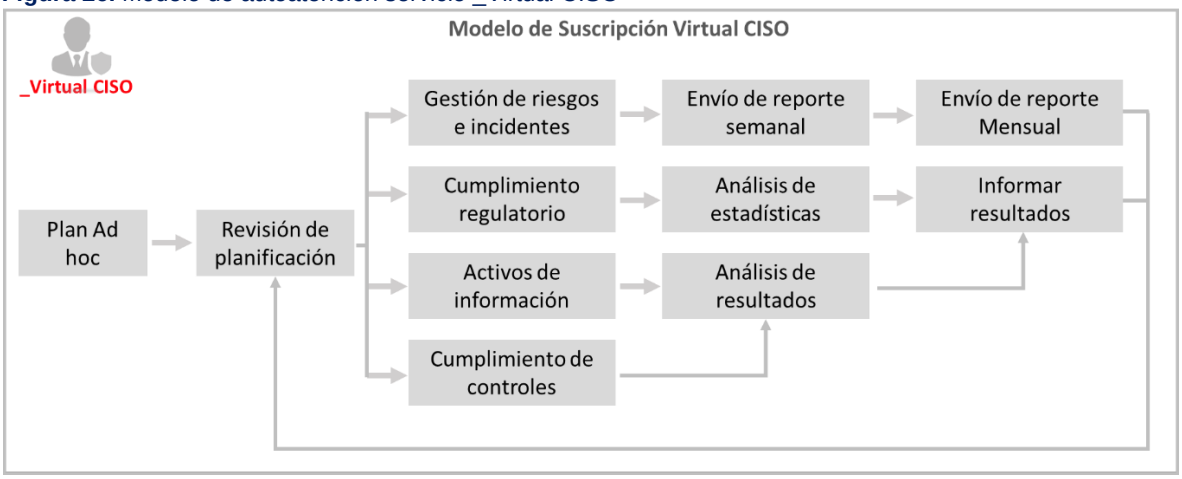
Fuente: Elaboración propia

_**Virtual CISO:** Para la realización de este servicio se requiere de al menos 2 personas, 1 supervisor y 1 analista, los que en su conjunto podrán atender hasta 30 empresas bajo la modalidad de suscripción mensual, estas células de trabajo estarán construidas por industria en la que se desarrollen los clientes, para de esta manera dar una atención más cercana al negocio. La operación de este servicio inicia con la definición del plan de ciberseguridad, el que debe estar alineado con la estrategia de la compañía cliente, luego de esto se comienza con la revisión del plan en detalle y priorización de reglas, actividades y/o proyectos (la implementación, compra o mantenimiento de herramientas de ciberseguridad especificas quedan fuera del precio de suscripción mensual y se debe revisar en detalle), con esto se podrá poner en marcha la implementación de la estrategia de ciberseguridad de la compañía, contando con un gobierno y marco normativo adaptado a su negocio sobre el cual se hará gestión constante, en caso de aumentar la cantidad de clientes suscritos a este modelo se puede aumentar en 1 analista la misma célula siempre y cuando se cumpla con la condición que los clientes pertenezcan a la misma industria o similar, en caso contrario, se debe evaluar la factibilidad de la creación de una nueva célula de virtual CISO.

El rol de virtual CISO, tendrá la responsabilidad de sensibilizar y comunicar la estrategia de ciberseguridad dentro de las compañías que contraten el servicio, para garantizar el éxito de esto, se deben comprender que esta labor requerirá apoyos de áreas o personas internas de la compañía, principalmente aquellas que se encuentren en labores de dirección, marketing, operaciones, administración y

personas. A continuación, se puede observar el modelo operacional de este servicio:

Figura 26. Modelo de autoatención servicio _Virtual CISO

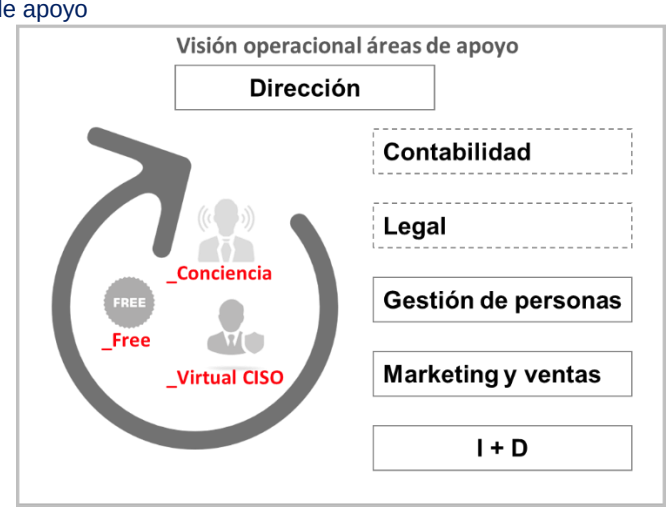


Fuente: Elaboración propia

13.2. ACTIVIDADES DE APOYO

Para el funcionamiento de la consultora se requiere de colaboradores que estén orientados a las actividades de dirección y administración, con el objetivo de garantizar la sustentabilidad de la compañía, estas funciones se pueden ver en la siguiente figura

Figura 27. Funciones de apoyo



Fuente: Elaboración propia

Contabilidad

Esta función tiene por objetivo registrar y clasificar las operaciones realizadas por la consultora, disponibilizando la información necesaria para realizar la correcta toma de decisiones, inicialmente esta función será externalizada con gestión directa sobre el gerente general de la compañía. La decisión de hacer esto de manera externa es para hacer más liviana la estructura inicialmente y permitir mayor eficiencia en el uso de los recursos de la compañía.

Legal

Esta función tiene por objetivo el supervisar y garantizar el cumplimiento de las leyes chilenas por parte de la consultora y de asesorar al gerente general en la toma de decisiones, esta función inicialmente será realizada de manera externa por lo que se contratarán servicios profesionales, se evaluará la modalidad y la posible internalización el cabo del segundo año de funcionamiento, siempre y cuando se cumpla con los objetivos financieros de la compañía.

Gestión de personas

Como se ha mencionado en este plan de negocios el contar con personal adecuado para las funciones es parte de los factores clave del negocio, por esto es una función que requiere evolución y que generará ventajas competitivas sobre los rivales en el mercado, por lo tanto, se realizará internamente, en el primer año esta función dependerá del gerente general de la consultora, apoyado por los gestores, a partir del segundo año iniciará este rol en la consultora tendrá las siguientes responsabilidades:

- Proceso de selección.
- Plan de capacitación de los colaboradores.
- Asegurar el cumplimiento de las leyes laborales.

Marketing y ventas

Este proceso tendrá la función captar los nuevos clientes para los servicios, generar las campañas necesarias para dar a conocer la consultora, por otro lado, serán los responsables de realizar las proyecciones de ventas para los próximos años y encargados de la gestión del portafolio de servicios

I+D

Este proceso tendrá por objetivo generar el material para realizar las campañas, investigar diferentes vectores de ataque y comportamiento humano para mejorar contantemente la calidad de los ejercicios prestados por la consultora, esta función debe desarrollar e incrementar las ventajas competitivas en el tiempo, garantizando el cumplimiento de los objetivos de la consultora, este proceso será liderado de forma interna por el gerente general de la compañía acompañado de los lideres y los analistas, en el tiempo esta composición irá variando a medida que sea necesario fijar personal dedicado a esta función. Al ser una función que requiere de

expertise, evolución y que generará ventajas competitivas sobre los rivales en el mercado, esta función se realizará internamente.

14. PLAN ORGANIZACIONAL

En este capítulo se definirán los aspectos principales que ayudarán a la consultora a cumplir con los objetivos estratégicos de la consultora. A continuación, se detalla cada uno de estos aspectos:

- **Estructura y proyección de dotación.** Si bien se ha definido una estructura funcional de acuerdo con el plan operacional, no todas las posiciones serán cubiertas en el inicio de las actividades de la consultora, este crecimiento será gradual y alineado con el crecimiento de las ventas de la compañía, para lo que se han definido los siguientes cargos:

Tabla 4. Cargos definidos para el funcionamiento de la consultora

Cargo	Responsabilidades
Gerente General	• Liderar el plan estratégico de la compañía • Liderar las funciones de gestión de personas, I+D, ventas y marketing, pudiendo contratar servicios ocasionales en caso sea necesario. • Coordinar las asesorías Legales y de Contabilidad. • Reportar el directorio los avances de la consultora • Informar periódicamente los indicadores financieros de la consultora
Líder de Operaciones	• Liderar la prestación de los servicios de la consultora • Coordinar el equipo de analistas a cargo • Garantizar el cumplimiento de los niveles de servicio • Mantener una tasa de fuga de clientes bajo el 10% anual. • Reportar oportunamente los resultados de la operación al gerente general • Medir y reportar la capacidad del equipo. • Participar de los procesos de I+D y gestión de personas
Analista Jr	• Ejecutar las tareas de los servicios (campañas y ejercicios de phishing) • Reportar oportunamente las situaciones de incumplimiento al líder de operaciones • Construir reportes de clientes
Vendedor	• Cumplir con la meta definida para el mes y año en curso • Identificar mejoras en la propuesta de servicios de la consultora.
Líder de Marketing y Ventas	• Monitorear el cumplimiento de la estrategia de marketing • Administrar el portafolio de productos • Posicionar la marca de acuerdo con la definición
Líder de I+D	• Generar el material para realizar las campañas. • Investigar diferentes vectores de ataque y comportamiento humano para mejorar contantemente la calidad de los ejercicios

	• Identificar nuevas líneas de negocio • Liderar la mejora continua de los procesos existentes
Gestor de RRHH	• Proceso de selección. • Definición de perfiles para cada cargo. • Plan de capacitación de los colaboradores. • Definición y mantención de modelo de incentivos basado en meritocracia. • Asegurar el cumplimiento de las leyes laborales. • Administrar el plan de beneficios de la consultora

Fuente: Elaboración propia

De acuerdo con las metas definidas para los canales de distribución y estresadas por las proyecciones de crecimiento de los escenarios pesimista y optimista, se puede estimar lo siguiente:

Tabla 5. Proyección en la dotación de analistas

Año	Pesimista	Probable	Optimista
1	3	4	5
2	4	5	6
3	4	6	8
4	5	8	11
5	5	9	14

Fuente: Elaboración propia

Cabe destacar que esta proyección es solo para los analistas, los siguientes roles no estarán en el inicio de la compañía y se incorporarán de acuerdo con la proyección realizada en el Anexo F de este documento:

- Líder de Marketing y Ventas
- Líder de I+D
- Gestor de RRHH

Durante el periodo que no se cuente con personal dedicado a estas funciones, la responsabilidad estará con el Gerente General.

- **Plan de capacitación:** El ámbito de la ciberseguridad está en constante evolución y movimiento por lo que mantenerse activo y actualizado con los nuevos vectores de ataque es clave para garantizar la correcta ejecución de los servicios, en este sentido se evaluará la contratación del servicio Udemy Business con el cual se podrá generar una ruta de aprendizaje para cada cargo de la consultora. Inicialmente este plan será liderado por el gerente general.

- **Plan de reclutamiento y selección:** El contar con personal calificado para los puestos es clave en el desarrollo de la estrategia y cumplimiento de los objetivos del negocio, por lo que este proceso se definirá de manera interna y se podrían contratar consultoras especializadas en caso de que sea

necesario, esta funciona inicialmente estará con el gerente general y dependiendo del escenario, se contará con un responsable del proceso completo.

15. PLAN FINANCIERO

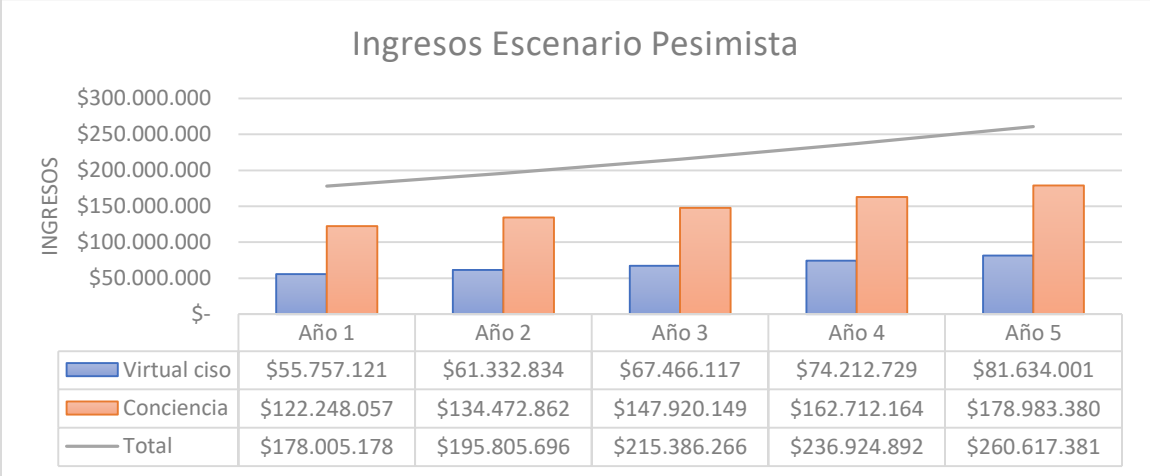
15.1. ESTIMACION DE INGRESOS

En el Anexo E, se muestra la proyección de captación de clientes para cada uno de los escenarios planteados, según los niveles de crecimiento desde el año 1 de la consultora, esta proyección se basa en las metas de ventas definidas en el plan de marketing, de acuerdo con esto se generan los escenarios de ingresos que se presentan a continuación.

Escenario pesimista

En este escenario se considera que en los 2 primeros meses de funcionamiento de la consultora solo se consiguen 3 ventas del servicio Conciencia, a partir del tercer mes se proyecta un crecimniento de un 20% por debajo de la meta de canales en clientes suscriptores, llegando al finalizar los primeros 12 meses a un total de 30 clientes en el servicio virtual CISO y 110 en Conciencia, luego se mantiene un 10% de crecimiento anual hasta el año 5, lo que genera los ingresos que se observan en la figura:

Figura 28. Ingresos escenario Pesimista



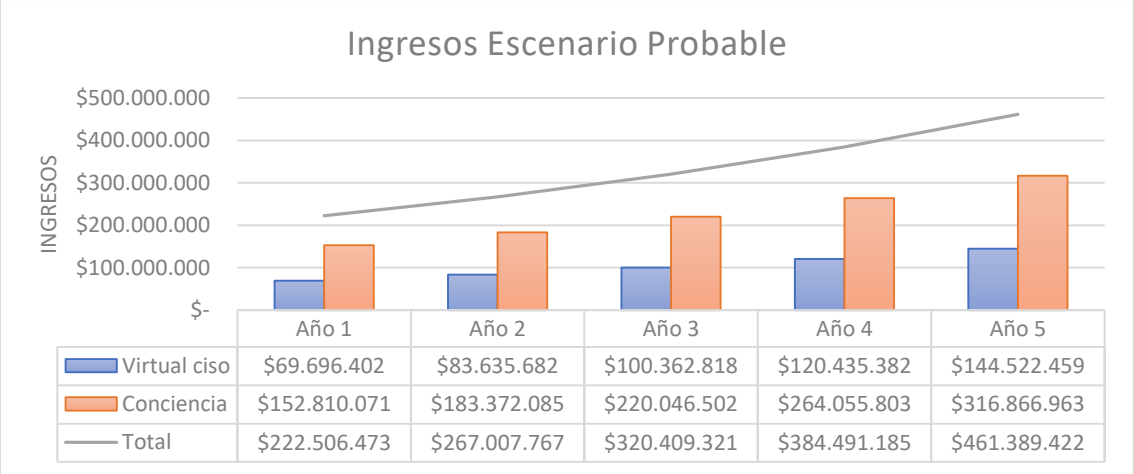
	Año 1	Año 2	Año 3	Año 4	Año 5
Virtual ciso	$55.757.121	$61.332.834	$67.466.117	$74.212.729	$81.634.001
Conciencia	$122.248.057	$134.472.862	$147.920.149	$162.712.164	$178.983.380
Total	$178.005.178	$195.805.696	$215.386.266	$236.924.892	$260.617.381

Fuente: Elaboración propia

Escenario Probable

En este escenario se considera como base de proyeccion la meta definida en el apartado de promocion del plan de marketing para los primeros 12 meses funcionamiento de la consultora por lo que se estima se tendría un cierre de año llegando a 137 clientes en el servicio Conciencia y 37 en el servicio virtual CISO luego se mantiene un 20% de crecimiento anual hasta el año 5, lo que genera los ingresos que se observan en la siguiente figura:

Figura 29. Ingresos escenario Probable



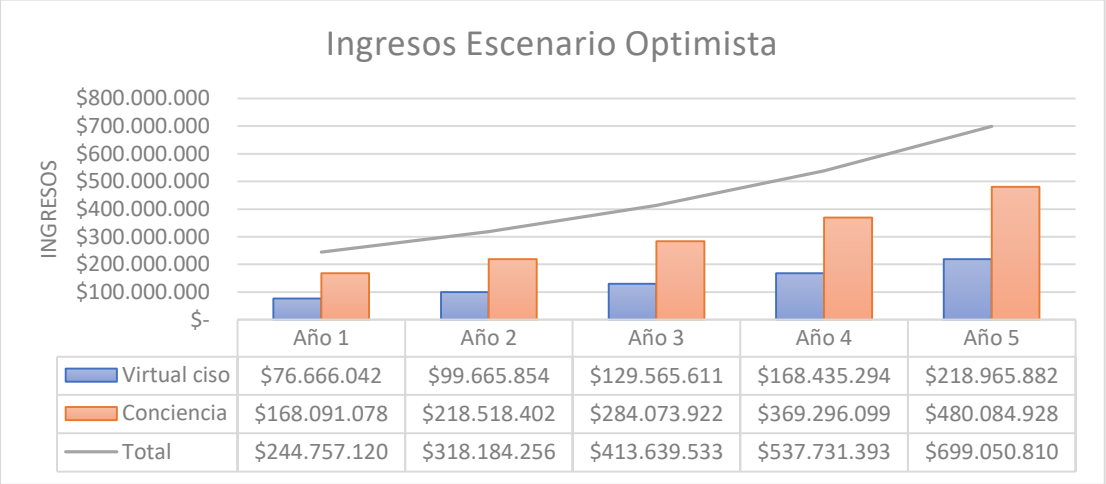
	Año 1	Año 2	Año 3	Año 4	Año 5
Virtual ciso	$69.696.402	$83.635.682	$100.362.818	$120.435.382	$144.522.459
Conciencia	$152.810.071	$183.372.085	$220.046.502	$264.055.803	$316.866.963
Total	$222.506.473	$267.007.767	$320.409.321	$384.491.185	$461.389.422

Fuente: Elaboración propia

Escenario Optimista

En este escenario se considera que en los 2 primeros meses de funcionamiento de la consultora solo se consiguen 4 ventas del servicio Conciencia, a partir del tercer mes se proyecta un crecimniento 10% en la cantidad de clientes suscriptores, por sobre la meta de canales llegando al finalizar los primeros 12 meses a un total de 41 clientes en el servicio virtual CISO y 151 en Conciencia, luego se mantiene un 30% de crecimiento anual hasta el año 5, lo que genera los ingresos que se observan en la siguiente figura:

Figura 30. Ingresos escenario Optimista



	Año 1	Año 2	Año 3	Año 4	Año 5
Virtual ciso	$76.666.042	$99.665.854	$129.565.611	$168.435.294	$218.965.882
Conciencia	$168.091.078	$218.518.402	$284.073.922	$369.296.099	$480.084.928
Total	$244.757.120	$318.184.256	$413.639.533	$537.731.393	$699.050.810

Fuente: Elaboración propia

15.2. ESTIMACION DE COSTOS

La estimación de los costos se realizó tomando en cuenta todos los aspectos mencionados anteriormente en este documento, la proyección de ventas y crecimiento de la consultora.

Por otra parte, los costos asociados a las remuneraciones del personal cuentan con un 43% de recargo por sobre la definición del sueldo liquido de los colaboradores, incluyendo:

- provisión por vacaciones
- provisión por años de servicio
- pagos previsionales

por otra parte, los costos están definidos de acuerdo con la proyección del plan organizacional, que se pueden ver en el anexo 06 de este documento y los costos mensuales relacionados con la operación, de acuerdo con la siguiente tabla:

Tabla 6. Gastos Mensuales

Gastos mensuales	Monto	Obs
Oficina virtual	$ 60.000	
Asesorías legales	$ 200.000	
Servicio de contabilidad	$ 100.000	
Udemy	$ 243.000	
Servicio Cloud	$ 357.000	Costo mensual por 9 usuarios
Servicio de correo	$ 150.000	
Publicidad y Ventas	$ 2.000.000	Incluye pago de comisiones.

Por otra parte, la inversión inicial, está relacionada con la adquisición de los siguientes elementos:

Tabla 7. Inversión en Activos

Inversión en activos	Monto	Obs
Celulares y periféricos	$ 1.500.000	
Computadores	$ 4.900.000	Compra inicial de 7
Sitio Web	$ 1.000.000	
Total	**$ 8.800.000**	

15.3. CALCULO TASA DE DESCUENTO

La tasa de descuento fue calculada de acuerdo con el modelo CAPM, utilizando la siguiente formula:

$$K_0 = R_f + \beta_u(R_m - R_f)$$

Donde:

K_0 Costo de capital, esto es la tasa de descuento aplicada para traer los flujos al valor presente.

R_f Tasa libre de riesgo, se consideró la tasa de rentabilidad de los bonos del Banco Central de Chile a 5 años, de acuerdo con el valor publicado para el 30 de junio de 2022, 6.42%.

R_m Tasa de mercado. Se utilizó el promedio de S&P/CLX IPSA, según el rendimiento anualizado en el último año, 23.75%

β_u Beta sin apalancamiento 1.06, promedio de las industrias de servicios computacionales de acuerdo con Damodaran.

Por lo tanto, la tasa de descuento a calculada es K_0 = 24.79%

15.4. WACC

Considerando que el inicio de la consultora será realizado con financiamiento (ver cuadro de pagos en Anexo G), se presenta el cálculo del WACC.

$$WACC = K_e\left[\frac{E}{E+D}\right] + K_d(1-T)\left[\frac{D}{E+D}\right]$$

Donde:

K_e representa el costo de capital, es decir la tasa de descuento para traer los flujos a valor presente

K_d Costo de la deuda

E Fondos propios

D Total de la deuda financiera

T Tasa de impositiva

A continuación, el cálculo del valor del WACC por cada uno de los escenarios planteados.

15.4.1. ESCENARIO PESIMISTA

Tabla 8. WACC Escenario Pesimista

Kd	20,04%
E	$ 5.672.487
D	$ 30.000.000
T	0,25%
WACC	**20,75%**

Fuente: Elaboración propia

15.4.2. ESCENARIO PROBABLE

Tabla 9. WACC Escenario Probable

Kd	20,04%
E	$ 4.020.431
D	$ 30.000.000
T	0,25%
WACC	**20,56%**

Fuente: Elaboración propia

15.4.3. ESCENARIO OPTIMISTA

Tabla 10. WACC Escenario Optimista

Kd	1,70%
E	$ 6.420.431
D	$ 30.000.000
T	0,25%
WACC	**5,77%**

Fuente: Elaboración propia

16. ANALISIS DE ESCENARIOS

En este capítulo se analizarán los 3 escenarios planteados en este plan de negocios, presentando los flujos de caja para cada uno e indicando el cálculo del VAN, TIR y otros indicadores, para efectos de las conclusiones del trabajo se toma el escenario más probable.

16.1. FLUJO DE CAJA

16.1.1. ESCENARIO PESIMISTA

Tabla 11. Flujo de Caja Pesimista

	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
Ingresos por ventas		$ 178.005.178	$ 195.805.696	$ 215.386.266	$ 236.924.892	$ 260.617.381
Costos Operacionales		$ -13.320.000	$ -13.320.000	$ -13.320.000	$ -13.320.000	$ -13.320.000
Utilidad Bruta	**$ -**	**$ 164.685.178**	**$ 182.485.696**	**$ 202.066.266**	**$ 223.604.892**	**$ 247.297.381**
Margen Bruto		93%	93%	94%	94%	95%
Remuneraciones		$-169.884.000	$-169.884.000	$ -169.884.000	$-169.884.000	$-195.624.000
Publicidad y ventas		$ -18.000.000	$ -9.000.000	$ -9.000.000	$ -9.000.000	$ -9.000.000
Utilidad Operacional	**$ -**	**$ -23.198.822**	**$ 3.601.696**	**$ 23.182.266**	**$ 44.720.892**	**$ 42.673.381**
Margen Operacional		-13,03%	1,84%	10,76%	18,88%	16,37%
Depreciación		$ -1.675.000	$ -1.675.000	$ -1.675.000	$ -1.675.000	$ -
Intereses de crédito		$ -5.773.665	$ -4.911.753	$ -3.856.603	$ -2.564.891	-983.581
Ganancias/Pérdidas de Capital						
Perdidas del ejercicio anterior		$ -	$ -30.647.487	$ -33.632.544	$ -15.981.882	$ -
Utilidad Antes de Impuesto	**$ -**	**$ -30.647.487**	**$ -33.632.544**	**$ -15.981.882**	**$ 24.499.119**	**$ 41.689.801**
Impuesto a la renta (25%)		$ -	$ -	$ -	$ -6.124.780	$ -10.422.450
Utilidad después de impuesto		$ -30.647.487	$ -33.632.544	$ -15.981.882	$ 18.374.340	$ 31.267.351
depreciación		$ 1.675.000	$ 1.675.000	$ 1.675.000	$ 1.675.000	$ -
Perdidas del ejercicio anterior		$ -	$ 30.647.487	$ 33.632.544	$ 15.981.882	$ -
Flujo de Caja Operacional	**$ -**	**$ -28.972.487**	**$ -1.310.057**	**$ 19.325.662**	**$ 36.031.221**	**$ 31.267.351**
Inversión Activo Fijo	$ -6.700.000					
Inversión en Capital de Trabajo	$ -28.972.487					
Préstamo	$ 30.000.000					
Amortización Préstamo		$ -3.844.434	$ -4.706.345	$ -5.761.496	$ -7.053.208	$ -8.634.518
Valor Mercado Activo Fijo						
Recuperación de Capital de Trabajo						$ 28.972.487
Flujo de Capitales	$ -5.672.487	$ -3.844.434	$ -4.706.345	$ -5.761.496	$ -7.053.208	$ 20.337.969
Flujo de Caja Privado	**$ -5.672.487**	**$ -32.816.920**	**$ -6.016.403**	**$ 13.564.167**	**$ 28.978.014**	$ 51.605.319

Fuente: Elaboración propia

Tabla 12. VPN, TIR y Payback, Pesimista

VPN	$148.781
TIR anual	25%
Tasa de Descuento	24,79%
Payback	3
Total, Inversión inicial	$35.672.487

Rf (tasa libre de riesgo)	6,42%
Rm (tasa de mercado)	23,75%
Beta desapalancado	1,06

16.1.1.1. CONCLUSIONES ESCENARIO PESIMISTA

Si bien el VAN es positivo, la TIR es casi igual que la tasa de descuento, por lo que hacer este negocio sería indiferente de cara a los inversionistas, en este escenario, no se cumple con el objetivo de obtener un 50% de utilidad en 5 años, por lo que, si al iniciar las actividades de la consultora los números se acercan a esto, se deben tomar medidas para remediar, ya que con esta proyección no sería atractivo el plan.

Por otra parte, para el cálculo de este escenario se castigó en un 20% la meta de clientes mensuales del primer año, por lo que en caso de implementar el plan de negocios la meta no debe estar por menos de un 5%.

16.1.2. ESCENARIO PROBABLE

Tabla 13. Fujo de caja, Probable

	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
Ingresos por ventas		$ 222.506.473	$ 267.007.767	$ 320.409.321	$ 384.491.185	$ 461.389.422
Costos Operacionales		$ -13.320.000	$ -13.320.000	$ -13.320.000	$ -13.320.000	$ -13.320.000
Utilidad Bruta	**$ -**	**$ 209.186.473**	**$ 253.687.767**	**$ 307.089.321**	**$ 371.171.185**	**$ 448.069.422**
Margen Bruto		94%	95%	96%	97%	97%
Remuneraciones		$-195.624.000	$-221.364.000	$-252.252.000	$-360.360.000	$-411.840.000
Publicidad y ventas		$ -18.000.000	$ -9.000.000	$ -9.000.000	$ -9.000.000	$ -9.000.000
Utilidad Operacional	**$ -**	**$ -4.437.527**	**$ 23.323.767**	**$ 45.837.321**	**$ 1.811.185**	**$ 27.229.422**
Margen Operacional		-1,99%	8,74%	14,31%	0,47%	5,90%
Depreciación		$ -1.600.000	$ -1.600.000	$ -1.600.000	$ -1.950.000	$ -350.000
Intereses de crédito		$ -5.773.665	$ -4.911.753	$ -3.856.603	$ -2.564.891	-983.581
Ganancias/Pérdidas de Capital						
Perdidas del ejercicio anterior		$ -	$ -11.811.192	$ -	$ -	$ -2.703.706
Utilidad Antes de Impuesto	**$ -**	**$ -11.811.192**	**$ 5.000.822**	**$ 40.380.718**	**$ -2.703.706**	**$ 23.192.135**
Impuesto a la renta (25%)		$ -	$ -1.250.205	$ -10.095.179	$ -	$ -5.798.034
Utilidad después de impuesto		$ -11.811.192	$ 3.750.616	$ 30.285.538	$ -2.703.706	$ 17.394.101
Depreciación		$ 1.600.000	$ 1.600.000	$ 1.600.000	$ 1.950.000	$ 350.000
Perdidas del ejercicio anterior		$ -	$ 11.811.192	$ -	$ -	$ 2.703.706
Flujo de Caja Operacional	**$ -**	**$ -10.211.192**	**$ 17.161.809**	**$ 31.885.538**	**$ -753.706**	**$ 20.447.807**
Inversión Activo Fijo	$ -6.400.000		-2800000	$ -1.400.000	-2100000	700000
Inversión en Capital de Trabajo	$ -27.620.431					
Préstamo	$ 30.000.000					
Amortización Préstamo		$ -3.844.434	$ -4.706.345	$ -5.761.496	$ -7.053.208	$ -8.634.518
Valor Mercado Activo Fijo						
Recuperación de Capital de Trabajo						$ 27.620.431
Flujo de Capitales	**$ -4.020.431**	**$ -3.844.434**	**$ -7.506.345**	**$ -7.161.496**	**$ -9.153.208**	**$ 19.685.913**
Flujo de Caja Privado	**$ -4.020.431**	**$ -14.055.626**	**$ 9.655.463**	**$ 24.724.043**	**$ -9.906.914**	**$ 40.133.721**

Fuente: Elaboración propia

Tabla 14. VPN, TIR y Payback, Probable

VPN	$12.816.115
TIR anual	57%
Tasa de Descuento	24,79%
Payback	2
Total, Inversión inicial	$34.020.431

Rf (tasa libre de riesgo)	6,42%
Rm (tasa de mercado)	23,75%
Beta desapalancado	1,06

16.1.2.1. CONCLUSIONES ESCENARIO PROBABLE

En este escenario se cumple el objetivo principal, consiguiendo una rentabilidad de un 50% en el plazo de 5 años, con una VAN positivo y un retorno de la inversión de 2 años. Por otra parte, la TIR es casi el doble de la tasa de descuento, al igual que la tasa de mercado, por lo que sería un buen negocio invertir en este plan si ocurre como lo proyectado.

Por otra parte, es importante mencionar que el crecimiento proyectado desde el año 2 es de un 20% anual en la cantidad de clientes, sin considerar una tasa de fuga de clientes. Dado que no se cuenta con un modelo de referencia de fuga para este tipo de servicios, se debe definir un indicador durante el primer año de operación, para estimar umbrales y ajustar las proyecciones.

16.1.3. ESCENARIO OPTIMISTA

Tabla 15. Fujo de caja, Optimista

	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
Ingresos por ventas		$ 244.757.120	$ 318.184.256	$ 413.639.533	$ 537.731.393	$ 699.050.810
Costos Operacionales		$ 13.320.000	$ 13.320.000	$ 13.320.000	$ 13.320.000	$ 13.320.000
Utilidad Bruta	**$ -**	**$ 258.077.120**	**$ 331.504.256**	**$ 426.959.533**	**$ 551.051.393**	**$ 712.370.810**
Margen Bruto		105%	104%	103%	102%	102%
Remuneraciones		$-247.104.000	$-303.732.000	$-386.100.000	$-463.320.000	$-540.540.000
Publicidad y ventas		$ -18.000.000	$ -9.000.000	$ -9.000.000	$ -9.000.000	$ -9.000.000
Utilidad Operacional	**$ -**	**$ -7.026.880**	**$ 18.772.256**	**$ 31.859.533**	**$ 78.731.393**	**$ 162.830.810**
Margen Operacional		-2,87%	5,90%	7,70%	14,64%	23,29%
Depreciacion		$ -2.200.000	$ -2.900.000	$ -2.550.000	$ -2.725.000	$ -2.375.000
Intereses de credito		$ -5.773.665	$ -4.911.753	$ -3.856.603	$ -2.564.891	-983.581
Ganacias/Pérdidas de Capital						
Perdidas del ejercicio anterior		$ -	$ -15.000.545	$ -4.040.042	$ -	$ -
Utilidad Antes de Impuesto	**$ -**	**$ -15.000.545**	**$ -4.040.042**	**$ 21.412.887**	**$ 73.441.502**	**$ 159.472.230**
Impuesto a la renta (25%)		$ -	$ -	$ -5.353.222	$ -18.360.375	$ -39.868.057
Utilidad después de impuesto		$ -15.000.545	$ -4.040.042	$ 16.059.666	$ 55.081.126	$ 119.604.172
Depreciacion		$ 2.200.000	$ 2.900.000	$ 2.550.000	$ 2.725.000	$ 2.375.000
Perdidas del ejercicio anterior		$ -	$ 15.000.545	$ 4.040.042	$ -	$ -
Flujo de Caja Operacional	**$ -**	**$ -12.800.545**	**$ 13.860.503**	**$ 22.649.708**	**$ 57.806.126**	**$ 121.979.172**
Inversión Activo Fijo	$ -8.800.000		$ -2.800.000	$ -1.400.000	$ -2.100.000	$ -700.000
Inversión en Capital de Trabajo	$ -27.620.431					
Préstamo	$ 30.000.000					
Amortización Préstamo		$ -3.844.434	$ -4.706.345	$ -5.761.496	$ -7.053.208	$ -8.634.518
Valor Mercado Activo Fijo						
Recuperación de Capital de Trabajo						$ 27.620.431
Flujo de Capitales	**$ -6.420.431**	**$ -3.844.434**	**$ -7.506.345**	**$ -7.161.496**	**$ -9.153.208**	**$ 18.285.913**
Flujo de Caja Privado	**$ -6.420.431**	**$ -16.644.979**	**$ 6.354.157**	**$ 15.488.212**	**$ 48.652.919**	**$ 140.265.086**

Fuente: Elaboración propia

Tabla 16. VPN, TIR y Payback, Optimista

VPN	$58.704.949
TIR anual	83%
Tasa de Descuento	24,79%
Payback	2
Total, Inversión inicial	$36.420.431

Rf (tasa libre de riesgo)	6,42%
Rm (tasa de mercado)	23,75%
Beta desapalancado	1,06

16.1.3.1. CONCLUSIONES ESCENARIO OPTIMISTA

En este escenario se obtiene un pronóstico muy favorable, que sobrepasa los objetivos planteados en el plan de negocios, con un VAN positivo y una TIR de 83%, más de 3 veces la tasa de descuento, lo que muestra un negocio muy rentable.

Es importante mencionar que conseguir estos resultados implicaría captar el doble de clientes mensuales aproximadamente y crecer en un 30% anual, si bien no es un escenario imposible se debe determinar cuál es el horizonte de crecimiento que tendrá la consultora en el mercado chileno y determinar cuándo será el momento de mirar a otros países de la región.

16.2. CONCLUSIONES EVALUACION ECONOMICA

En conclusión, al revisar los resultados de los 3 escenarios se puede observar que la meta de captación definida para los canales permite conseguir los objetivos planteados en este documento, de todas maneras, es importante monitorear constantemente el cumplimiento de la meta de captación dado que en el escenario pesimista no se cumplirá el objetivo, y sería más atractivo para los inversionistas invertir en otro proyecto. Por otra parte el valor residual al final de 5 años no fue considerado en el análisis económico debido a que es un negocio intensivo en mano de obra.

Por lo tanto, se deben seguir las siguientes recomendaciones:

- El cumplimiento de la meta de captación de clientes no debe ser inferior al 80% Anual.
- Optimizar el proceso de administración de clientes y evaluar eficiencias en la operación mediante automatización y robotización de procesos.
- Tener una tasa de fuga de clientes y monitorearla diariamente.

.

17. CONCLUSIONES

Día a día los riesgos de ciberseguridad aumentan producto del constante uso de tecnologías, hace no muchos años atrás el porcentaje de personas y empresas con acceso a internet era muy diferente a la realidad actual. Por otro lado, las empresas producto de la pandemia tuvieron que adaptarse en su funcionamiento, ya sea por eficiencia o simplemente para garantizar la operación, por lo que se generó un aumento en la transformación digital de las empresas de todo tamaño y una adopción explosiva del teletrabajo.

Pese a ello y a las constantes noticias relacionadas con los ataques de ciberseguridad, las pymes chilenas aún están al debe en términos de sensibilización y acción frente a estos riesgos, como lo demuestran diferentes estudios que fueron analizados en este plan de negocios, pero no solamente son las pymes las que están al debe sino también la oferta de servicios para este tipo de empresa, se debe replantear el negocio y no sólo pensar en la implementación de herramientas y servicios estándar, debe existir una oferta adaptada escalable que permita a los lideres de estas empresas preocuparse de su negocio mientras delegan la seguridad en expertos, no se puede ofrecer servicios con mega soluciones que requieran un alto conocimiento de utilización, por lo que se debe apoyar a las empresas con soluciones de fácil implementación y mantención.

Por otra parte, estamos en presencia de un escenario favorable para emprender negocios relacionados a la ciberseguridad en las pymes chilenas, el marco regulatorio en Chile ha implementado una serie de requerimientos relacionados a esto y con el tiempo cada vez serán más rigurosos, por otra parte muchas grandes empresas han comenzado a solicitar la implementación de medidas de este ámbito en sus proveedores, por ejemplo planes de concientización, estrategias de protección entre otras, requerimientos para los que este tipo de empresas no está preparado.

Por otra parte, el aumento del cibercrimen y la facilidad de acceder a herramientas para realizar ataques por parte de los cibercriminales genera una proyección no muy alentadora por este aspecto para las empresas, pero si muy positiva para aquellos que venden servicios relacionados a la prevención y protección de ciberataques.

Con respecto al entorno económico y político, si bien se observan años complejos y con bastante incertidumbre, se pueden convertir en años llenos de oportunidades para el ingreso de nuevas empresas prestadoras de servicios que sean capaces de repensar la cadena y mantener un alto nivel de calidad a mejores precios.

Sin embargo, se debe incentivar a las pymes al uso e implementación de soluciones de ciberseguridad, ya que como se pudo observar que principalmente el desinterés en los temas de ciberseguridad está relacionado con el desconocimiento de las amenazas a las que se enfrentan las empresas, es por esto que la generación de eventos, webinars charlas y visitas presenciales a las empresas es clave en este aspecto. Por esta razón es que dentro de los servicios de la consultora se definió uno sin costo, principalmente pensado en las empresas que están iniciando sus actividades y quieren saber cómo avanzar en temas de prevención y protección.

Por otra parte, dado que la principal barrera de entrada de los servicios de ciberseguridad para las pymes es el costo, no sólo se debe solucionar con bajos precios, si no también buscar alianzas con las redes de emprendedores que permitan a más personas acceder a este tipo de servicios y así prevenir los posibles incidentes que podrían sufrir y poner en riesgo su negocio.

Muchos pueden pensar que las herramientas de ciberseguridad son limitadas o solo se debe contar con las mejores para estar protegidos, la verdad es que esto es relativo, dependerá del escenario en que se quiera jugar, por lo que contar con un framework que sea modular y permita integrar diferentes soluciones para dar prevención y protección a medida es la clave. En resumen, se puede diseñar, se puede crear y por supuesto implementar, sin duda en los próximos años quienes logren repensar los servicios serán los que tengan la ventaja competitiva frente al resto.

En este plan de negocios se consiguió evaluar 2 escenarios favorables con retornos de la inversión atractivos para la inversión y con VAN positivo, lo que demuestra que apuntar como segmento objetivo un gran número de pequeños clientes puede ser tan atractivo como mirar pocos pero grandes, es por esto que el mercado de las pymes tiene un gran atractivo y potencial de crecimiento.

18. BIBLIOGRAFÍA

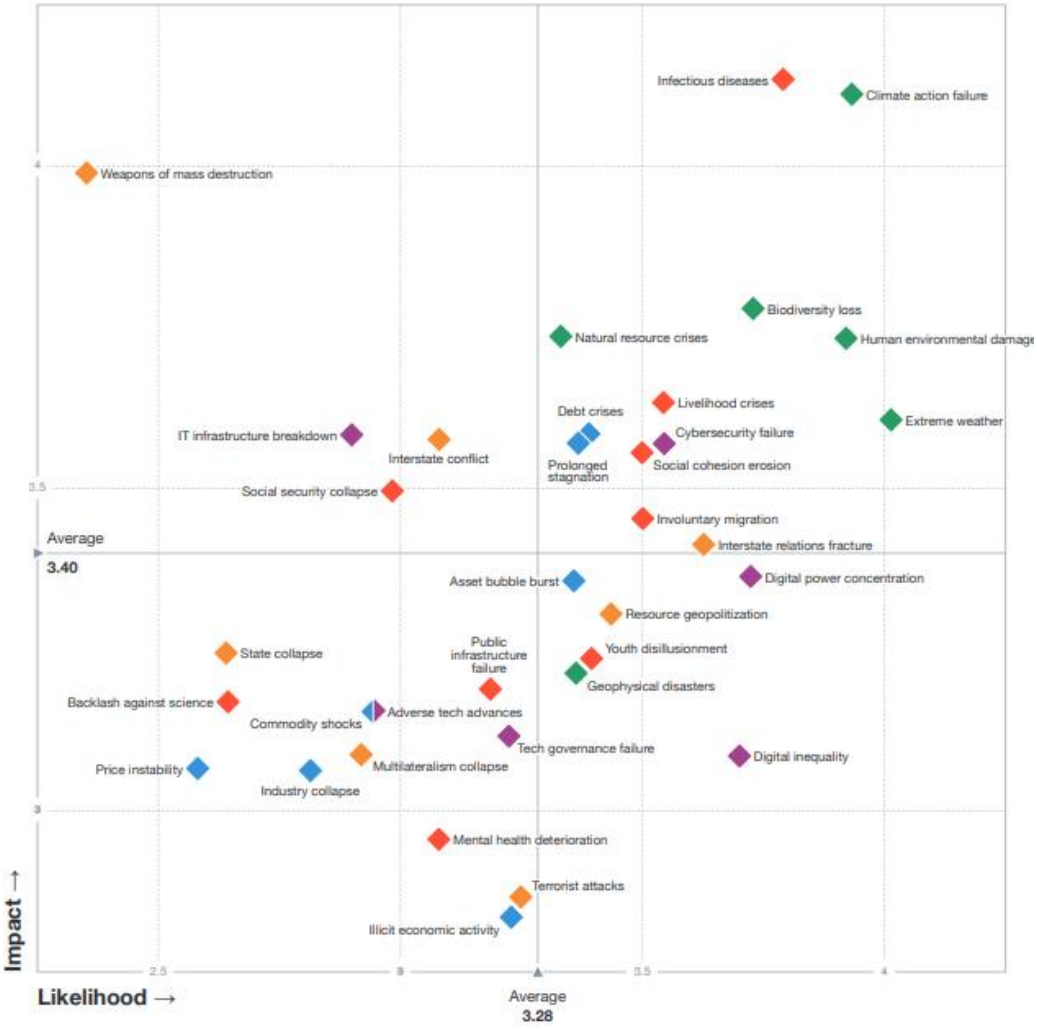
- World Economic Forum. 2022. The Global Risks Report 2020. [online] Disponible en: https://www.weforum.org/reports/the-global-risks-report-2020
- Corporativa, I., 2021. *Entel: Líder en Tecnología y Telecomunicaciones*. [online] Informacioncorporativa.entel.cl. Disponible en: https://informacioncorporativa.entel.cl/estado-de-la-ciberseguridad.
- Nacional, B., 2022. LEY 19628 SOBRE PROTECCION DE LA VIDA PRIVADA. [online] www.bcn.cl/leychile. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=141599
- Sii.cl. 2022. Estadísticas de Empresa. [online] Disponible en: https://www.sii.cl/sobre_el_sii/estadisticas_de_empresas.html
- NIST. 2021. *Cybersecurity Framework*. [online] Disponible en: https://www.nist.gov/cyberframework.
- CIS. 2021. *CIS Controls*. [en linea] Disponible en: https://www.cisecurity.org/controls.
- Hax, Arnoldo. The Delta Model. 2010th ed.
- ISACA. 2021. *COBIT | Control Objectives for Information Technologies | ISACA*. [online] Disponible en: https://www.isaca.org/resources/cobit.
- Quijano, S., 2006. *Dirección de Recursos Humanos y Consultoría en las organizaciones*. Barcelona: Icaria.
- ITU. 2022. *Global Cybersecurity Index.* [online] Disponible en: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
- Kaspersky. 2021. 2020 IT spending: cybersecurity remains investment priority despite overall IT budget cuts, *Kaspersky found.* [online] Disponible en: https://www.kaspersky.com/about/press-releases/2020_2020-it-spending-cybersecurity-remains-investment-priority-despite-overall-it-budget-cuts-kaspersky-found
- Financiero, D., 2022. Cinco tecnologías que marcarán la ruta de las industrias en 2022 | Diario Financiero. [en linea] Df.cl. Disponible en: https://www.df.cl/df-lab/transformacion-digital/cinco-tecnologias-que-marcaran-la-ruta-de-las-industrias-en-2022
- Nacional, B., 2022. DFL 3 FIJA TEXTO REFUNDIDO, COORDINADO Y SISTEMATIZADO DE LA LEY N° 19.496, QUE ESTABLECE NORMAS SOBRE PROTECCIÓN DE LOS DERECHOS DE LOS CONSUMIDORES. [en línea] Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1160403
- Política Nacional de Ciberseguridad. [en línea] Disponible en: https://cms-dgd-prod.s3-us-west-

2.amazonaws.com/uploads/pdf/Politica_Nacional_de_Ciberseguridad_2017.pdf

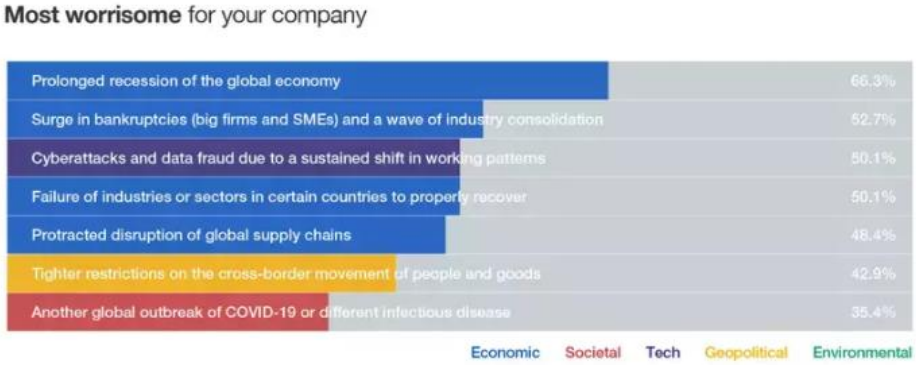
- Statista. 2022. Cybersecurity Software Report 2021 | Statista. [En línea] Disponible en: https://de.statista.com/statistik/studie/id/104227/dokument/software-report/
- Gartner. 2022. Gartner Identifies Top Security and Risk Management Trends for 2022. [En linea] Disponible en: https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022
- Cetiuc.com. 2022. CETIUC – Centro de Estudios de Tecnologías de Información de la Pontificia Universidad Católica de Chile – Centro de Estudios de Tecnologías de Información de la UC. [En linea] Disponible en: https://cetiuc.com/
- Pages.stern.nyu.edu. 2022. Damodaran Online: Home Page for Aswath Damodaran. [En linea] Disponible en: https://pages.stern.nyu.edu/~adamodar/ .
- Economia.gob.cl. 2020. [En Linea] Disponible en: https://www.economia.gob.cl/wp-content/uploads/2020/07/Informe-de-Resultados-Encuesta-TIC.pdf

ANEXOS

ANEXO A: Panorama de riesgos globales 2021 del Foro Económico Mundial (WEF)



¿Cuáles son, según los líderes empresariales, los riesgos más preocupantes para las empresas debido al coronavirus?



Fuente: Foro Económico Mundial https://es.weforum.org/reports/the-global-risks-report-2021

ANEXO B: Resultado 2021 índice Global de ciberseguridad- Chile

Chile

Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
68.83	17.20	9.39	15.84	11.07	15.33

Source: ITU Global Cybersecurity Index v4, 2021

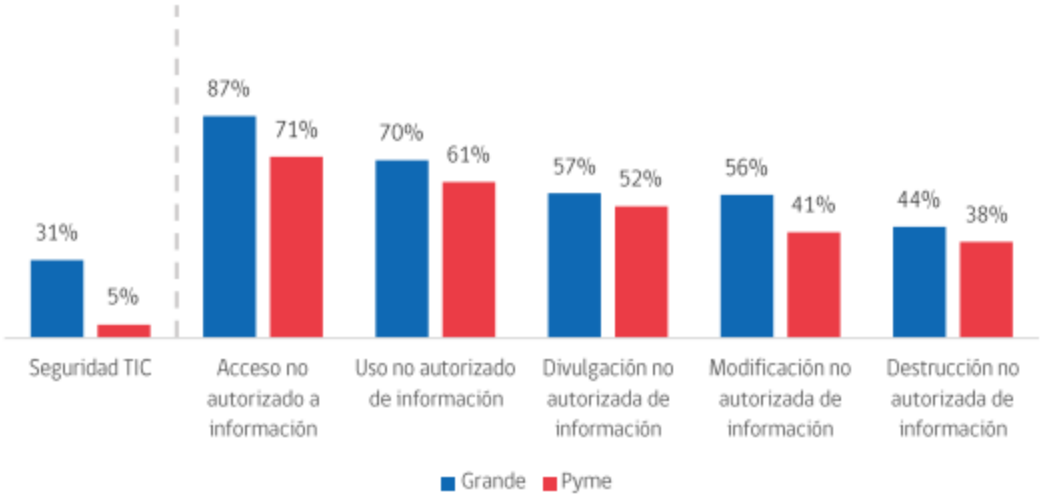
ANEXO C: Análisis de competidores directos

					modalidad de contacto				Servicios de ciberseguridad prestados				
#	Empresa	Servicios Adicionales a Ciberseguridad	Suscripcion Online	Precios	Formulario	Correo	Telefono	Sitio web	Hacking etico	Implementacion de herramientas	Concientización de usuarios	Asesorías/ consultoria	Otros
1	GREP	Si	No	No	Si	Si	Si	grep.cl	Si	Si	Si	Si	Si
2	STEGA	No	No	No	Si	Si	No	stega.cl	Si	No	No	Si	Si
3	IIA	Si	No	No	Si	Si	Si	iia.cl	Si	Si	No	Si	Si
4	LUMEN	Si	No	No	Si	Si	Si	https://www.lumen.com/	Si	Si	No	Si	Si
5	Movistar	Si	Si	Si	Si	Si	Si	negociosdigitalesmovistar.com/	No	Si	No	No	Si
6	redvoiss	Si	No	No	Si	Si	No	negociosdigitalesmovistar.com/	No	No	No	No	Si
7	hackmetrix	no	No	No	Si	Si	no	https://www.hackmetrix.com/	Si	no	no	no	Si
8	Ciberseguridad humana	si	No	No	Si	Si	si	https://ciberseguridadhumana.cl/	No	No	Si	No	No
9	OCP.TECH	Si	No	No	Si	Si	No	ocp.tech/	No	Si	No	No	No
10	Kepler	Si	No	No	Si	Si	No	https://kepler.cl/	No	Si	Si	Si	Si

ANEXO D: Preguntas realizadas en las entrevistas a lideres de pymes chilenas

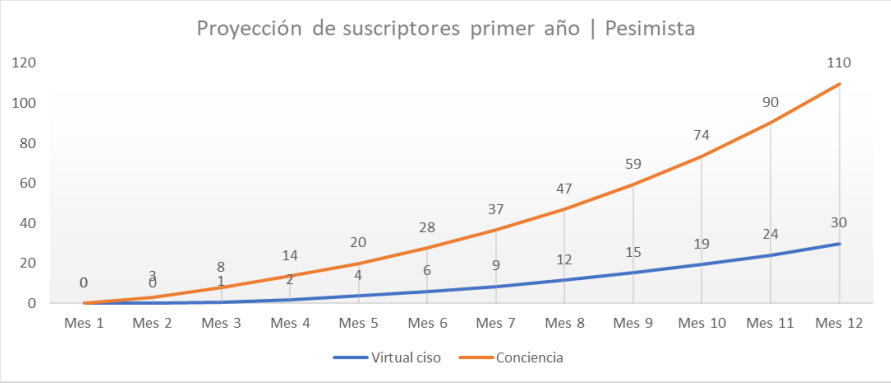
N°	Preguntas
1	¿Qué conoces de la ciberseguridad en chile?
2	¿Has tenido algún incidente de ciberseguridad?
3	¿Has sabido de algún incidente de ciberseguridad en tu industria?
4	¿Tu o algún familiar se han visto enfrentados a algún incidente de ciberseguridad?
5	¿Qué tan probable ves que tu empresa tenga un incidente en los próximos años?
6	¿Qué medidas de prevención de seguridad utilizas en tu empresa?
7	¿Tienes categorizada la información de tu empresa?
8	¿Sabes dónde está la información relevante de tu empresa?
9	¿Qué harías si te vieras enfrentado a una fuga masiva de informaciones?
10	¿Qué pasaría si producto de un ciberataque mañana no pudieras acceder a las informaciones de la empresa?
11	¿Tienes respaldos de tus informaciones, proyectos o sistemas?
12	Crees que las personas que trabajan contigo, ¿conocen los riesgos de la ciberseguridad?
13	¿Algún cliente te ha preguntado por el resguardo de sus datos?
14	¿Trabajas con proyectos o informaciones confidenciales?
15	¿Qué crees que es lo peor que te podría ocurrir en términos de ciberseguridad?
16	¿Gastas o inviertes en seguridad hoy?, podrías mencionar cuánto?

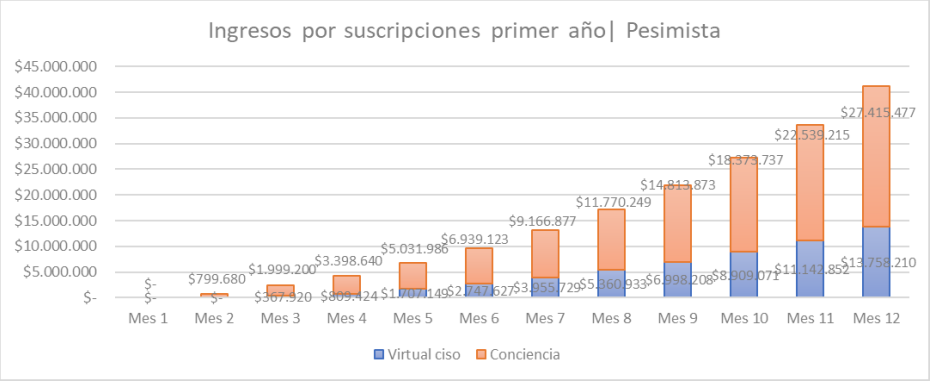
ANEXO E: Gráfico, Porcentaje de empresas que utilizan nuevas tecnologías: Seguridad TIC

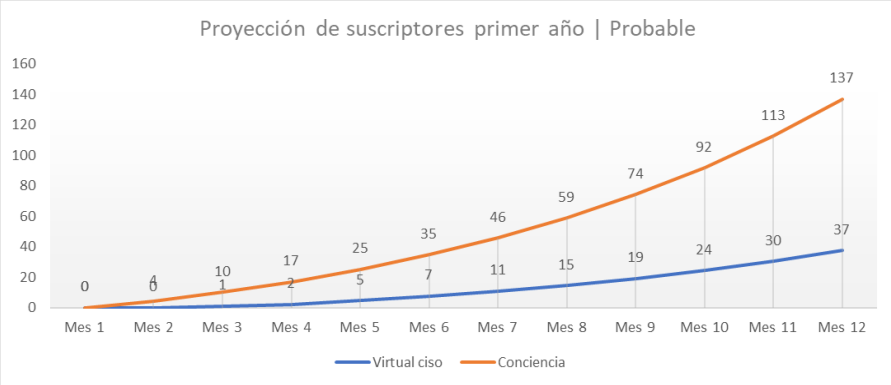


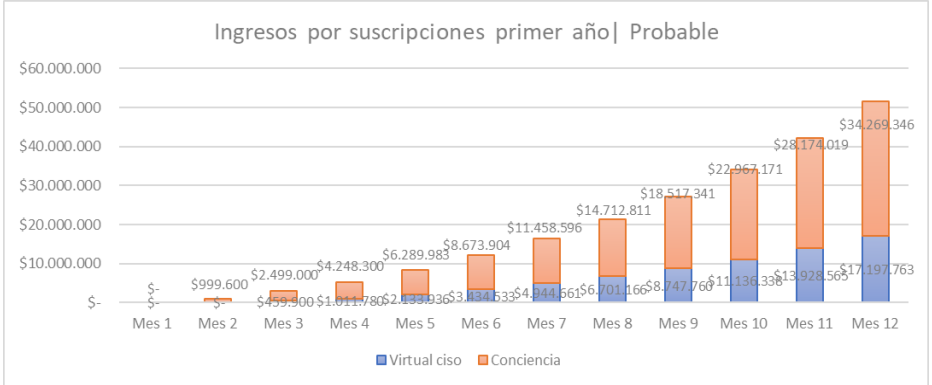
Fuente: Encuesta TIC, Ministerio de economía de Chile

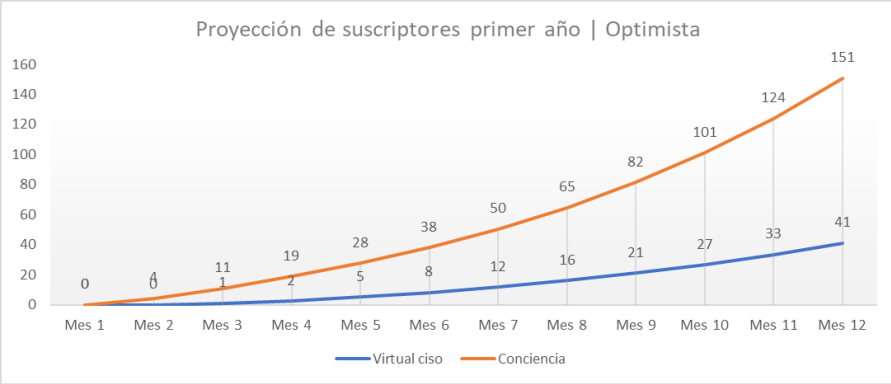
ANEXO F: Proyección de los primeros 12 meses de crecimiento de clientes por escenario e ingreso por productos.

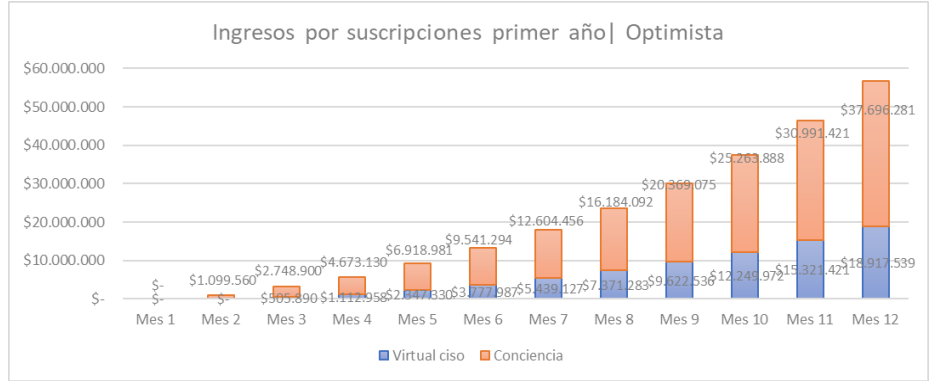












ANEXO G: Proyección de dotación con renta y costo empresa

Escenario Pesimista

			Año 1		Año 2		Año 3		Año 4		Año 5	
Personas	**Sueldo Liquido**	**Costo empresa**	**Q**	**Monto**	**Q**	**Monto**	**Q**	**Monto**	**Q**	**Monto**	**Q**	**Monto**
Gerente General	$ 3.000.000	$ 4.290.000	1	$ 4.290.000	1	$ 4.290.000	1	$ 4.290.000	1	$ 4.290.000	1	$ 4.290.000
Gestor de RRHH	$ 1.500.000	$ 2.145.000		$ -	0	$ -	0	$ -	0	$ -	0	$ -
Lider de Mkt y Ventas	$ 1.800.000	$ 2.574.000		$ -	0	$ -	0		0	$ -	0	$ -
Lider de I+D	$ 1.800.000	$ 2.574.000		$ -	0	$ -	0		0	$ -	0	$ -
Lider de Operaciones	$ 1.800.000	$ 2.574.000	1	$ 2.574.000	1	$ 2.574.000	1	$ 2.574.000	1	$ 2.574.000	1	$ 2.574.000
Analista	$ 1.500.000	$ 2.145.000	3	$ 6.435.000	3	$ 6.435.000	3	$ 6.435.000	3	$ 6.435.000	4	$ 8.580.000
Vendedor	$ 600.000	$ 858.000	1	$ 858.000	1	$ 858.000	1	$ 858.000	1	$ 858.000	1	$ 858.000
		Mensual		**$ 14.157.000**		**$ 14.157.000**		**$ 14.157.000**		**$ 14.157.000**		**$ 16.302.000**
		Anual		**$169.884.000**		**$169.884.000**		**$169.884.000**		**$169.884.000**		**$195.624.000**

Escenario Probable

			Año 1		Año 2		Año 3		Año 4		Año 5	
Personas	**Sueldo Liquido**	**Costo empresa**	**Q**	**Monto**	**Q**	**Monto**	**Q**	**Monto**	**Q**	**Monto**	**Q**	**Monto**
Gerente General	$ 3.000.000	$ 4.290.000	1	$ 4.290.000	1	$ 4.290.000	1	$ 4.290.000	1	$ 4.290.000	1	$ 4.290.000
Gestor de RRHH	$ 1.500.000	$ 2.145.000	0	$ -	0	$ -	0	$ -	0	$ -	1	$ 2.145.000
Lider de Mkt y Ventas	$ 1.800.000	$ 2.574.000		$ -	0	$ -	0	$ -	1	$ 2.574.000	1	$ 2.574.000
Lider de I+D	$ 1.800.000	$ 2.574.000		$ -	0	$ -	1	$ 2.574.000	1	$ 2.574.000	1	$ 2.574.000
Lider de Operaciones	$ 1.800.000	$ 2.574.000	1	$ 2.574.000	1	$ 2.574.000	1	$ 2.574.000	1	$ 2.574.000	1	$ 2.574.000
Analista	$ 1.500.000	$ 2.145.000	4	$ 8.580.000	5	$ 10.725.000	5	$ 10.725.000	8	$ 17.160.000	9	$ 19.305.000
Vendedor	$ 600.000	$ 858.000	1	$ 858.000	1	$ 858.000	1	$ 858.000	1	$ 858.000	1	$ 858.000
		Mensual		**$ 16.302.000**		**$ 18.447.000**		**$ 21.021.000**		**$ 30.030.000**		**$ 34.320.000**
		Anual		**$195.624.000**		**$221.364.000**		**$252.252.000**		**$360.360.000**		**$411.840.000**

Escenario Optimista

			Año 1		Año 2		Año 3		Año 4		Año 5	
Personas	**Sueldo Liquido**	**Costo empresa**	**Q**	**Monto**	**Q**	**Monto**	**Q**	**Monto**	**Q**	**Monto**	**Q**	**Monto**
Gerente General	$ 3.000.000	$ 4.290.000	1	$ 4.290.000	1	$ 4.290.000	1	$ 4.290.000	1	$ 4.290.000	1	$ 4.290.000
Gestor de RRHH	$ 1.500.000	$ 2.145.000	1	$ 2.145.000	1	$ 2.145.000	1	$ 2.145.000	1	$ 2.145.000	1	$ 2.145.000
Lider de Mkt y Ventas	$ 1.800.000	$ 2.574.000		$ -	0	$ -	1	$ 2.574.000	1	$ 2.574.000	1	$ 2.574.000
Lider de I+D	$ 1.800.000	$ 2.574.000		$ -	1	$ 2.574.000	1	$ 2.574.000	1	$ 2.574.000	1	$ 2.574.000
Lider de Operaciones	$ 1.800.000	$ 2.574.000	1	$ 2.574.000	1	$ 2.574.000	1	$ 2.574.000	1	$ 2.574.000	1	$ 2.574.000
Analista	$ 1.500.000	$ 2.145.000	5	$ 10.725.000	6	$ 12.870.000	8	$ 17.160.000	11	$ 23.595.000	14	$ 30.030.000
Vendedor	$ 600.000	$ 858.000	1	$ 858.000	1	$ 858.000	1	$ 858.000	1	$ 858.000	1	$ 858.000
		Mensual		**$ 20.592.000**		**$ 25.311.000**		**$ 32.175.000**		**$ 38.610.000**		**$ 45.045.000**
		Anual		**$247.104.000**		**$303.732.000**		**$386.100.000**		**$463.320.000**		**$540.540.000**

ANEXO H: Cuadro de Pagos de Crédito

Préstamo	$ 30.000.000
Tasa Mensual	1,7%
Tasa Anual	20,04%
Períodos	60
Cuota	-801.508

	Deuda inicial	Cuota	Amortización	Intereses
1	-30.000.000	-801.508	-291.508	-510.000
2	-29.708.492	-801.508	-296.464	-505.044
3	-29.412.028	-801.508	-301.504	-500.004
4	-29.110.524	-801.508	-306.629	-494.879
5	-28.803.895	-801.508	-311.842	-489.666
6	-28.492.053	-801.508	-317.143	-484.365
7	-28.174.910	-801.508	-322.535	-478.973
8	-27.852.375	-801.508	-328.018	-473.490
9	-27.524.357	-801.508	-333.594	-467.914
10	-27.190.763	-801.508	-339.265	-462.243
11	-26.851.498	-801.508	-345.033	-456.475
12	-26.506.465	-801.508	-350.898	-450.610
13	-26.155.566	-801.508	-356.864	-444.645
14	-25.798.703	-801.508	-362.930	-438.578
15	-25.435.773	-801.508	-369.100	-432.408
16	-25.066.673	-801.508	-375.375	-426.133
17	-24.691.298	-801.508	-381.756	-419.752
18	-24.309.542	-801.508	-388.246	-413.262
19	-23.921.296	-801.508	-394.846	-406.662
20	-23.526.449	-801.508	-401.559	-399.950
21	-23.124.891	-801.508	-408.385	-393.123
22	-22.716.506	-801.508	-415.328	-386.181
23	-22.301.178	-801.508	-422.388	-379.120
24	-21.878.790	-801.508	-429.569	-371.939
25	-21.449.221	-801.508	-436.871	-364.637
26	-21.012.350	-801.508	-444.298	-357.210
27	-20.568.051	-801.508	-451.851	-349.657
28	-20.116.200	-801.508	-459.533	-341.975
29	-19.656.667	-801.508	-467.345	-334.163
30	-19.189.322	-801.508	-475.290	-326.218
31	-18.714.033	-801.508	-483.370	-318.139
32	-18.230.663	-801.508	-491.587	-309.921
33	-17.739.076	-801.508	-499.944	-301.564
34	-17.239.132	-801.508	-508.443	-293.065
35	-16.730.689	-801.508	-517.087	-284.422
36	-16.213.603	-801.508	-525.877	-275.631
37	-15.687.726	-801.508	-534.817	-266.691
38	-15.152.909	-801.508	-543.909	-257.599
39	-14.609.000	-801.508	-553.155	-248.353

40	-14.055.845	-801.508	-562.559	-238.949
41	-13.493.286	-801.508	-572.122	-229.386
42	-12.921.163	-801.508	-581.848	-219.660
43	-12.339.315	-801.508	-591.740	-209.768
44	-11.747.575	-801.508	-601.799	-199.709
45	-11.145.776	-801.508	-612.030	-189.478
46	-10.533.746	-801.508	-622.435	-179.074
47	-9.911.311	-801.508	-633.016	-168.492
48	-9.278.295	-801.508	-643.777	-157.731
49	-8.634.518	-801.508	-654.721	-146.787
50	-7.979.797	-801.508	-665.852	-135.657
51	-7.313.945	-801.508	-677.171	-124.337
52	-6.636.774	-801.508	-688.683	-112.825
53	-5.948.091	-801.508	-700.391	-101.118
54	-5.247.700	-801.508	-712.297	-89.211
55	-4.535.403	-801.508	-724.406	-77.102
56	-3.810.996	-801.508	-736.721	-64.787
57	-3.074.275	-801.508	-749.246	-52.263
58	-2.325.029	-801.508	-761.983	-39.526
59	-1.563.047	-801.508	-774.936	-26.572
60	-788.110	-801.508	-788.110	-13.398
61	0	-801.508	-801.508	0