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

ESTRATEGIA DE NEGOCIO PARA EL SERVICIO DE CIBERSEGURIDAD ENTEL S.A.

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

VÍCTOR MANUEL ALFARO GÓMEZ

PROFESOR GUÍA:
CLAUDIO ENRIQUE PIZARRO TORRES

MIEMBROS DE LA COMISIÓN:
ANTONIO AGUSTÍN HOLGADO SAN MARTÍN
EDUARDO ENRIQUE DÍAZ LY

SANTIAGO DE CHILE
2020

RESUMEN

ESTRATEGIA DE NEGOCIO PARA EL SERVICIOS DE CIBERSEGURIDAD ENTEL S.A

El objetivo de presente trabajo es formular una estrategia de negocio para el servicio de CiberSeguridad de ENTEL S.A., que permita incrementar los ingresos y su participación de mercado en Chile, y con ello, maximizar el valor del negocio.

El mercado global de la ciberseguridad tiene alto potencial de crecimiento (cagr 11% al 2021), producto del incremento de la inversión en las TIC en el desarrollo de estrategias digitales, a la preocupación para mitigar riesgos de ciberataques, y además por el cumplimiento de normativas gubernamentales exigidas por los estados. Por lo anterior, las organizaciones consideran a la CiberSeguridad como un elemento clave dentro de su planificación estratégica. Sin embargo, existen obstáculos para su implementación con recursos internos, limitaciones en la inversión, alta demanda de personal calificado, aspectos culturales, entre otros. Lo anterior puede ser desfavorable para muchas organizaciones, pero en la industria de CiberSeguridad y en Chile esto representa una oportunidad de crecimiento de mercado (cagr 7,6% al 2023).

En Chile la industria de CiberSeguridad, está inserta en un entorno con alto nivel de competitividad e inversiones, y constantes cambios tecnológicos, además de la aplicación de marcos regulatorios. ENTEL S.A. al ser parte de esta industria, desde la distribución hasta la entrega de servicios, está expuesta a diversos factores que representan un desafío constante. Por lo anterior, contar con una estrategia para el servicio de CiberSeguridad es clave para mejorar su posición competitiva e incrementar la participación de mercado. Como resultado de la implementación de la estrategia formulada en este trabajo, se estima que ENTEL S.A. al cuarto año, podría duplicar los ingresos del servicio de CiberSeguridad, pasando de 6,2 miles de millones de pesos en el año 2018 a 19,1 miles de millones de peso al 2023. Además, podría aumentar la participación de mercado: 7,5% en el año 2019 a un 21,4% en el 2023. En relación al margen operacional del servicio, en este mismo periodo; este podría mejorar en un 28%.

El desarrollo de la estrategia se fundamentó en un diagnóstico de la industria a nivel global, y las particularidades del mercado en Chile. Para luego analizar, la propuesta de valor de ENTEL S.A del servicio de CiberSeguridad, y con ello establecer líneas de acción que mejoren la propuesta actual. Las líneas de acción se elaboraron de acuerdo con la metodología Modelo Delta, Arnoldo C. Hax, permitiendo responder rápidamente al mercado, en el marco de una cultura de alta competencia y confianza.

Tabla de Contenido

1 Introducción 1

2 Objetivos y resultados esperados 2

2.1 Objetivo general 2

2.2 Objetivos específicos 2

2.3 Resultados esperados 2

3 Marco conceptual 3

3.1 CiberSeguridad 3

3.2 Gestión Estratégica 5

4 Mercado de ciberseguridad 9

4.1 Mercado Global 9

4.2 Mercado Latinoamérica y Chile 11

4.3 Cadena de Valor Servicios Ciberseguridad 13

5 Clientes de ciberseguridad 14

5.1 Clasificación de Clientes 14

5.1.1 Administraciones Públicas 14

5.1.2 Corporaciones y Empresas 15

5.1.3 Pymes y Particulares 15

5.2 Marco normativo en Chile 15

5.2.1 Agenda Digital 2020 15

5.2.2 Política Nacional de Ciberseguridad (PNCS) 16

5.2.3 Normas en materia de ciberseguridad 16

5.2.4 Tratado de Budapest 17

5.2.5 Ley de Protección de Datos Personales 17

6 Proveedores de ciberseguridad 18

6.1 Clasificación de Proveedores 18

6.1.1 Fabricación de hardware y desarrollo de software 18

6.1.2 Distribución de productos de ciberseguridad 18

6.1.3 Prestación de servicios de ciberseguridad 18

6.1.4 Proveedores de servicios gestionados de seguridad (MSSP) 19

6.2 Soluciones de CiberSeguridad 21

6.2.1 Soluciones de Prevención 21

6.2.2 Soluciones de Control 21

6.2.3 Soluciones de Mitigación 22
7 Servicios de Entel CyberSecure 23
7.1 Descripción de la Organización 23
7.1.1 Estrategia Corporativa 24
7.1.2 Participación de Mercado en Chile 25
7.1.3 Mercado Corporaciones 26
7.1.4 Entel CyberSecure 28
7.1.4.1 Servicios 28
7.1.4.2 Cadena de Valor 29
7.1.4.3 Empresa Extendida 30
7.1.4.4 Estructura Organizacional 33
7.1.4.5 Competencias Actuales y Deseadas 38
7.1.4.6 Resultados Financieros Actuales 40
8 Estrategia de Negocio para el Servicio de Ciberseguridad 40
8.1 Propuesta de Líneas de acción 41
8.2 Resultados esperados 43
9 Conclusiones y Recomendaciones 46
10 Bibliografía 47

1 Introducción

En Chile la industria de las Telecomunicaciones y CiberSeguridad, está inserta en un entorno económico débil, con alto nivel de competitividad e inversiones, y constantes cambios tecnológicos, además de la aplicación de marcos regulatorios.

En este contexto, Empresa Nacional de Telecomunicaciones (ENTEL S.A) es un operador líder de telecomunicaciones en Chile, con 50 años de presencia en el país y desde el 2013 cuenta con una creciente operación en Perú. Ofrece una completa gama de servicios para sus clientes, que se dividen en los segmentos de personas, empresas y corporaciones. La propuesta de valor de ENTEL S.A. consiste en entregar experiencias de servicio simples y eficientes, a través de una infraestructura de primer nivel para comunicaciones móviles, fijas, y tecnologías de la información digitales, abriendo a sus clientes posibilidades infinitas.

En los negocios de Entel en Chile, debido al alto nivel de intensidad competitiva y un ambiente económico débil, el EBITDA mostró una baja el año 2018. Por otra parte, Entel ha presentado exceso de foco en crecimiento en los 6 últimos años, para potenciar el negocio en Perú y además la mantención de infraestructura en Chile con inversiones en redes, plataformas y data center. Por todos estos factores, la compañía se ve enfrentada al desafío de mejorar sus márgenes operacionales, disminuir el nivel de endeudamiento y rentabilizar las inversiones tanto en Chile como en Perú.

Las líneas de acción definidas por la Vicepresidencia del Mercado Corporaciones de Entel, para apoyar este desafío, ponen foco en lo siguiente: Incrementar ingresos a través de nuevos servicios digitales. Defender y evolucionar negocio tradicional. Incrementar rentabilidad, eficiencia y control de inversiones.

El presente proyecto, se enmarca en la dirección indicada por la Vicepresidencia del Mercado Corporaciones y tiene por objetivo formular una estrategia de negocio para el Servicio de Ciberseguridad que permita incrementar los ingresos y su participación de mercado en Chile, y con ello, maximizar el valor del negocio.

2 Objetivos y resultados esperados

2.1 Objetivo general

Formular una estrategia de negocio para el servicio de CiberSeguridad de ENTEL S.A., que permita incrementar los ingresos y su participación de mercado en Chile, y con ello, maximizar el valor del negocio.

2.2 Objetivos específicos

1. Analizar la situación actual del Servicio de CiberSeguridad, en los aspectos que afectan de forma positiva y negativa el valor al negocio.

2. Determinar oportunidades y desafíos de transformación en base al diagnóstico anterior, y a la comparación de mejores prácticas e indicadores de la industria y mercado.

3. Formular líneas de acción estratégicas, respondiendo a oportunidades y brechas, en el contexto de la creación de valor de la empresa.

4. Estimar el impacto económico y estratégico de las líneas de acción formuladas.

2.3 Resultados esperados

Estrategia de negocio valorizada para el Servicio de CiberSeguridad.

3 Marco conceptual

A continuación, se especifican los conceptos claves que forman parte del marco conceptual del desarrollo de este proyecto y que permitirán formular una estrategia de negocio para el Servicio CiberSeguridad.

3.1 CiberSeguridad

En la era de la globalización digital, los flujos de datos están creciendo de forma exponencial. Las tecnologías digitales están cambiando la forma de hacer de los negocios y ampliando la participación más allá de las fronteras. Los datos gobiernan y las personas tienen cada vez más acceso a la información. Por estas razones el proteger la información, y con ello la reputación de las empresas y organizaciones públicas o privadas, será un aspecto crucial en la planificación estratégica de las empresas. Con los ciberataques aumentando día a día, preparar a una organización para establecer políticas, procesos, tecnologías y desarrollar una cultura de seguridad digital *"**Ciberseguridad**"*, es clave para disminuir los riegos a la velocidad que demandan los negocios digitales.

El desarrollo de las Tecnologías de la información y la comunicación (TIC) ha generado un nuevo espacio de relación, denominado "Ciberespacio" (ver Figura 1), lugar donde no existen fronteras y donde se generan muchas oportunidades, pero también riesgos y amenazas en un entorno dinámico.

Figura 1. Vulnerabilidad del Ciberespacio.

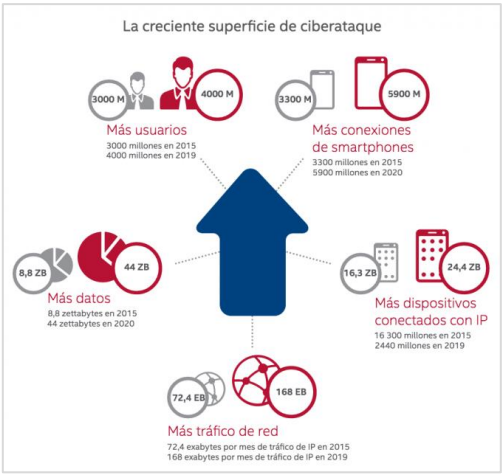
Fuente: Estrategia de Seguridad Nacional Española 2017

La transformación digital incrementa la dependencia de las tecnologías de la información, y por tanto genera mayor cantidad de datos, que a su vez aumenta el riesgo de ciberataques, en un entorno donde el derecho a la protección de datos personales es un requisito esencial en la relación del cliente y los negocios digitales. Por otra parte, el ciberespacio es un escenario de fácil accesibilidad, anonimidad, alta conexión y dinamismo.

En los últimos tiempos, los ciberataques han aumentado número, alcance y nivel de complejidad de las acciones. Esto implica un aumento en la demanda de servicios y soluciones de ciberseguridad orientadas a mitigar los riesgos. Estas acciones han adquirido mayor relevancia en Chile, un país altamente interconectado y que ocupa una posición de liderazgo en la región en materia de redes digitales.

En la figura 2 se visualiza el grado de dependencia de una sociedad digitalizada y cómo el ciberespacio crece día a día. Conocer las amenazas del ciberespacio, gestionar los riesgos y una adecuada capacidad de prevención, defensa, detección, análisis, investigación, recuperación y respuesta constituyen elementos esenciales en una Estrategia de CiberSeguridad.

Figura 2. La creciente superficie de ciberataque.



Fuente: McAfee Labs 2015

El patrón de amenazas dado por: Ciberespinonaje, Intrusiones en POS y Ataque a Aplicaciones WEB, revela que la Estrategia de Defensa para hacer frente a las amenazas es transversal a cualquier industria y las soluciones que mitigan los riesgos son multi-sectoriales (ver Figura 3).

Figura 3. Amenazas de Crimen Organizado.

Fuente: Verizon 2014

Fuente: IBM Threat Intelligence Quarterly, 2015

De acuerdo con los antecedentes descritos anteriormente podemos concluir lo siguiente:

- El mayor uso de las TIC y el ritmo acelerado de crecimiento que demandan los Negocios Digitales han generado riesgos y oportunidades en un entorno dinámico, los datos gobiernan y las personas tienen cada vez más acceso a la información.

- La Planificación Estratégica de las empresas, organizaciones públicas o privadas deben considerar la protección de la información, y con ello la reputación de las empresas y evitar impactos negativos al negocio.

- Las organizaciones deben establecer políticas, procesos, tecnologías y desarrollar una cultura de seguridad digital “Ciberseguridad” basada en la gestión de riesgos, que mitigue las vulnerabilidades presentes del Ciberespacio.

- Las amenazas y riesgos de los ciberataques son transversales a cualquier industria, y con mayor presencia en las industrias asociadas a Servicios Digitales, Comercio, Gobierno y Mercados Financieros.

3.2 Gestión Estratégica

Las empresas utilizan el proceso de Gestión Estratégica para lograr una posición competitividad y obtener rendimientos superiores al promedio. Las empresas logran una posición competitividad cuando ha creado una estrategia que crea valor y ha aprendido a implementarla.

De acuerdo con lo anterior, podemos identificar diversos modelos para establecer una estrategia de negocios que permita tomar posición frente al mercado, en especial sobre la competencia.

Sera parte de este trabajo el análisis de modelos de posicionamiento estratégico, que permitan identificar elementos que contribuyan a la formulación de las líneas de acción para mejorar la actual estrategia de ENTEL S.A para el servicio de CiberSeguridad.

A continuación se detallan modelos de posicionamiento estratégico que servirán como base para la definición de las líneas de acción estratégicas:

- **El Modelo de Porter para Posicionamiento Competitivo**, sitúa a la industria como el foco de la atención de la estrategia. Porter establece que las características estructurales de la organización son las que mejor explican el desempeño de una empresa. Desde la perspectiva de Porter sólo existen dos formas de competir, con bajos precios o diferenciación de productos.

    - El liderazgo en precio se obtiene con una agresiva búsqueda de economías de escalas, optimización de productos y procesos y una cuota de mercado de producto significativa que permite a las compañías explotar la experiencia de otros.

    - La diferenciación apunta a crear productos que los consumidores perciben como únicos y con un alto valor agregado para ellos. Esta estrategia puede manifestarse de varias formas: diseño de la imagen de una marca, con tecnología, servicio al consumidor, y redes de distribución, entre otras.

- **El Modelo Basado en Recursos**, en vez de mirar la industria como una fuente de beneficios, postula que la atención debe focalizarse en los recursos propios de la empresa. Este modelo busca valor derivado de los recursos, competencias y capacidades. En este modelo lo que hace a una empresa diferente de otra es la habilidad para apropiarse de recursos que son valorados, escasos y difíciles de sustituir o copiar.

Ambos modelos perciben como rol primario de la estrategia el alcanzar una ventaja competitiva única. En estos modelos, el objetivo de la estrategia es ganarle al competidor, ya sea por sobresalir en las actividades de la cadena de valor, lo que permite establecer una posición de liderazgo en la industria o por la movilización de recursos y capacidades únicas (ver Figura 4).

Figura 4. Posiciones estratégicas: Mejor Producto.

Posición estratégica	Definición	Comentarios
Bajo Costo	Foco es ser el proveedor con menor costo en una categoría no diferenciada de producto	Esta estrategia permite poco espacio para una posición competitiva. Estandariza la oferta, comoditiza al cliente e intensifica la rivalidad
Diferenciación	Desarrollo de características y funcionalidades que hagan único al producto a un precio más alto	Tan pronto el producto diferenciado emerge, los competidores tienden a imitarlo. Es una ventaja no sustentable.

Fuente: Modelo Delta Arnoldo Hax.

Estos modelos se pueden complementar perfectamente. Sin embargo, ambos pueden enriquecerse si se les agrega la perspectiva del "Cliente". Desde esta perspectiva el cliente es un elemento más de competitividad. El Modelo Delta es un nuevo marco estratégico que sitúa al cliente al centro de la gestión. Examina las opciones primarias disponibles para establecer una vinculación con el cliente.

- **El Modelo Delta:** Establece que el centro de la estrategia debe considerar que debe ser el cliente. Es necesario servir a los clientes en forma distintiva si queremos obtener un buen desempeño. La estrategia se sustenta en atraer, satisfacer, y retener al cliente. Las estrategias clásicas están orientadas al producto. Muchas empresas tienden a entregar al cliente productos estandarizados, con canales masivos de distribución, haciendo pocos esfuerzos por satisfacer las necesidades individuales de sus clientes. Para lograr lo anterior, el modelo Delta establece lo siguiente:

    - La esencia de la estrategia radica no solo en lograr una ventaja competitiva permanente con los competidores, sino en lograr establecer lazos irrompibles, un conocimiento profundo y una vinculación afectiva con el cliente.
    - Identificar el sistema donde se encuentra inserta la empresa, "Empresa Extendida", para establecer la colaboración con clientes y proveedores, e integrar en la estrategia de negocio todos los elementos que forman parte de la cadena de valor
    - Examinar las competencias existentes y las que se necesitan adquirir para desarrollar una Estrategia ganadora.

Además de los modelos anteriores, como complemento se analizará como los Ecosistemas Digitales proporcionan a las empresas nuevas fuentes de valor y nuevas vías de crecimiento, que en su conjunto permiten responder rápidamente al mercado, en el marco de una cultura de alta competencia y confianza

- **Ecosistema Empresarial o Digital:** Las tecnologías digitales están revolucionando las interdependencias tradicionales entre las empresas. Como resultado, los gerentes han comenzado a reconocer sus entornos empresariales como ecosistemas digitales. Para las empresas acostumbradas a enmarcar sus entornos a través de diferentes modelos de cadena de suministro y nuevas estructuras de cooperación. Esto representa un cambio significativo en la perspectiva, que requiere una comprensión de las nuevas iniciativas estratégicas necesarias para competir en la era digital. Este ecosistema es el espacio donde los miembros que la integran pueden competir o colaborar entre ellos, pero coexistiendo y progresando juntos hacia un mejor servicio al cliente.

    - Velocidad: las empresas ahora pueden llevar productos al mercado en meses frente a años en función de la dinámica del ecosistema.
    - Competencia: un movimiento competitivo puede alterar la dinámica de toda una industria, aparentemente de la noche a la mañana.
    - Influencia: las citas basadas en la influencia están reemplazando las dictaduras de mando y control.
    - Unidades negociables: cuando cualquier cosa se puede digitalizar en una unidad comerciable, todo se convierte en una oportunidad.

    Para que una empresa tenga éxito, ésta no debe enfocarse solo en lo que hace como modelo de negocio, sino en expandirse y unirse a otras organizaciones para liderar el emprendimiento. El reto de las organizaciones no solo será velar por su cadena de valor, sino cómo la conecta con sus diversos grupos de interés y aliados, y en cómo gestiona el ecosistema.

    Un punto importante es que la consolidación de alianzas será el nuevo reto de las organizaciones. La idea es formar una red de colaboración, tener relaciones de confianza y reglas claras en el que todos ganen, siempre de una manera justa.

De acuerdo con los antecedentes descritos anteriormente podemos concluir lo siguiente:

- Para la Industria de Ciberseguridad no es una estrategia adecuada establecer un Posicionamiento solo basado en Costo o Diferenciación, debido a que esta industria posee una cantidad acotada de proveedores y de alta competitividad.
- Un Modelo Basado en Recursos, por si sólo tampoco es una estrategia adecuada, debido a la estandarización de las soluciones y servicios de CiberSeguridad, dificultad de retención de los clientes y la alta demanda de personal.
- Para lograr establecer una Estrategia Competitiva se requiere complementar ambos modelos con las competencias necesarias para lograr una vinculación afectiva (Atraer, Satisfacer y Retener) con el Cliente.
- En un entorno donde los nuevos negocios digitales crecen de forma acelerada, requieren que las empresas establezcan una Ecosistema Empresarial para trabajar de forma colaborativa y bajo el concepto de innovación abierta, siendo más ágiles para responder rápidamente al mercado, en el marco de una cultura de alta competencia y confianza.

4 Mercado de ciberseguridad

Se entiende como mercado de ciberseguridad la demanda de productos y soluciones para la protección de las infraestructuras TIC, las comunicaciones e información, tanto de las personas como de las empresas y administraciones públicas. Para el análisis de mercado y su desarrollo, a continuación, se describirá el sector a nivel Global, de Latinoamérica y en particular Chile.

4.1 Mercado Global

Se ha mencionado anteriormente la importancia de las tecnologías en el desarrollo de la industria tanto el sector público como el privado. Las empresas optan por invertir y fomentar el uso de las TIC. Según el informe Global Connnectivity Index 2015, el aumento de un 20% en la inversión en tecnologías de la información con lleva un crecimiento del PIB en un punto porcentual. Este crecimiento de la inversión ha traído consigo nuevos riesgos y amenazas que cada vez adquieren un mayor peso a nivel mundial. Así lo muestra el estudio elaborado por el Word Economic Forum que indica a los ciberataques como una de las amenazas a nivel global más significativas, de igual trascendencia que el desempleo o las inestabilidades sociales.

Ante esta situación, las empresas a nivel mundial han tendido a adoptar medidas de protección de sus sistemas, redes y en particular de la seguridad de la información. Adicionalmente a lo anterior, los Gobiernos a nivel mundial han hecho esfuerzos por establecer políticas públicas que regulen los aspectos asociados a la ciberseguridad.

Según Gartner, el mercado de la ciberseguridad se presenta como una actividad económica en auge (ver Figura 5), el gasto mundial en productos y servicios de seguridad de la información alcanzará más de 114.000 millones de dólares en 2018, un aumento del 12,4% respecto del año pasado y en el 2019, se espera que el mercado crecerá un 8,7% 124.000 millones.

Figura 5. Worldwide Security Spending by Segment, 2017 – 2019

Market Segment	2017	2018	2019
Application Security	2,434	2,742	3,003
Cloud Security	185	304	459
Data Security	2,563	3,063	3,524
Identity Access Management	8,823	9,768	10,578
Infrastructure Protection	12,583	14,106	15,337
Integrated Risk Management	3,949	4,347	4,712
Network Security Equipment	10,911	12,427	13,321
Other Information Security Software	1,832	2,079	2,285
Security Services	52,315	58,920	64,237
Consumer Security Software	5,948	6,395	6,661
Total	101,544	114,152	124,116

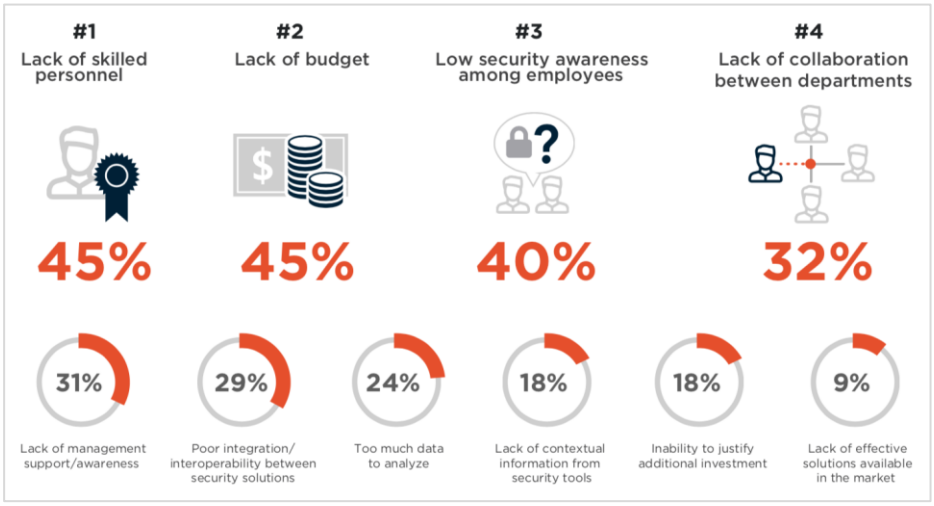
Fuente: Gartner Agosto 2018

Además, Gartner en su estudio del 2017 enfatiza en que “la persistente escasez de habilidades”, y los cambios regulatorios, impulsan todavía más el continuo crecimiento del mercado de los servicios de ciberseguridad. Los factores principales para el gasto de ciberseguridad son los riesgos de ciberataques, las necesidades comerciales, los cambios en la industria y los resguardos de la privacidad de la información.

Las preocupaciones sobre la privacidad de la información impulsarán al menos un 10% de la demanda de servicios de ciberseguridad en los próximos años e impactarán en una variedad de segmentos. Todo lo anterior impulsará el gasto adicional de los servicios de ciberseguridad en más de un 40% hasta el 2020.

Adicional a lo anteior, el informe del Cibersecurity Trends estable que los principales obstáculos para la implementación de una estrategia de ciberseguridad corresponde a una alta demanda de profesionales calificados, limitaciones en la obtención de recursos, empleados y por ultimo falta de colaboración entre áreas en aspectos de seguridad (ver Figura 6).

Figura 6. Principales obstáculos: Personal Calificado, Recursos, Cambio Cultural



Fuente: 2017 Spotlight Report – Cybersecurity Trends

En conclusión, el mercado global de la ciberseguridad tiene alto potencial de crecimiento, según el informe de Gartner, “Magic Quadrant for Managed Security Services, Worldwide - 2018”, se espera que este mercado a nivel global siga creciendo a una tasa de compuesta anual (CAGR) del 11% hasta el 2021, y además existen limitaciones para su implementación asociadas principalmente a habilidades y los recursos: la falta de empleados calificados (45%), seguida de la falta de presupuesto (45%) y la falta de conciencia de seguridad entre los empleados (40%), que dificultan la implementación de estrategias de ciberseguridad para las organizaciones que demandan estos servicios.

El escenario mencionado en el párrafo anterior se presenta desfavorable para muchas empresas, pero en el caso de un proveedor de servicios de ciberseguridad, como es ENTEL S.A., esto representa una oportunidad de crecimiento en este mercado.

4.2 Mercado Latinoamérica y Chile

De acuerdo con un estudio realizado por International Data Corporation (IDC) el año 2017, el mercado mundial de la ciberseguridad mueve alrededor de USD 97 billones al año, y en Latinoamérica alrededor de 3 billones de dólares, con un crecimiento proyectado de 12% anual hasta el 2021.

Por otra parte, en el indice de Ciberseguridad Global publicado el año 2018 (ranking que desarrolla la Unión Internacional de Telecomunicaciones) Chile se ubica en el puesto 83 y a nivel latinoamericano se posiciona en el noveno lugar, detrás de países como México, Uruguay, Brasil, Cuba, Colombia y Panamá. En relación a la inversión en Ciberseguridad de las empresas, IDC indica que Chile está por debajo del promedio de Latinoamérica en este ítem. La clasificación anterior indica que nuestro país tiene grandes oportunidades de desarrollo en este ámbito. El apoyo del estado en este desafío, se manifestó en el lanzamiento de la Política Nacional de Ciberseguridad el año 2017; cuyo fin es garantizar que los Gobiernos (de cualquier tendencia política) construyan una estrategia que los proteja de ciberataques, que pueden poner en riesgo la estabilidad política y económica del país

Adicionalmente, Chile es el país de la región que cuenta con el mayor gasto TI per cápita, pero solo el 12% de las empresas invierte en ciberseguridad, muy por debajo de la media del 21% (ver Figura 7).

Figura 7. Ciberseguridad en Chile

Fuente: IDC Latin America Cybersecurity Report 2017

Las cifras de ciberdelitos registrados en la región Latinoamericana han experimentado un crecimiento muy significativo en los últimos años. Las principales amenazas son las de tipo malware, que representan el 37,6% de los incidentes registrados. En particular Chile es un país atractivo para los ciberdelicuentes debido a la alta tasa de penetración de Internet, además de contar con una economía estable.

Por todos estos motivos, la ciberseguridad es el sector con mayor proyección de crecimiento en las empresas chilenas, por encima incluso del sector TIC. Según estimaciones de The Boston Consulting Group (BCG), en Chile el sector de ciberseguridad es un mercado en crecimiento, Durante el año 2016 la inversión alcanzó los 187 millones de USD, cantidad que equivale al 0,07% del PIB, por debajo del promedio mundial que se sitúa en el 0,12% del PIB.

A nivel sectorial, la banca y los servicios financieros lideran la inversión en servicios de ciberseguridad, en un segundo grupo le siguen las empresas de retail y telecomunicaciones, en un tercer nivel se sitúan minería, y utilities (agua, gas y energía) que cada vez invierten más en sistemas de automatización. Y en último lugar, el sector salud que avanza a menor velocidad en estos cambios.

Además IDC informó que durante el 2018 en Chile se invirtió US$156 millones en soluciones de seguridad, y el 43% de las compañías considera a la Ciberseguridad como la principal prioridad de inversión en TI.

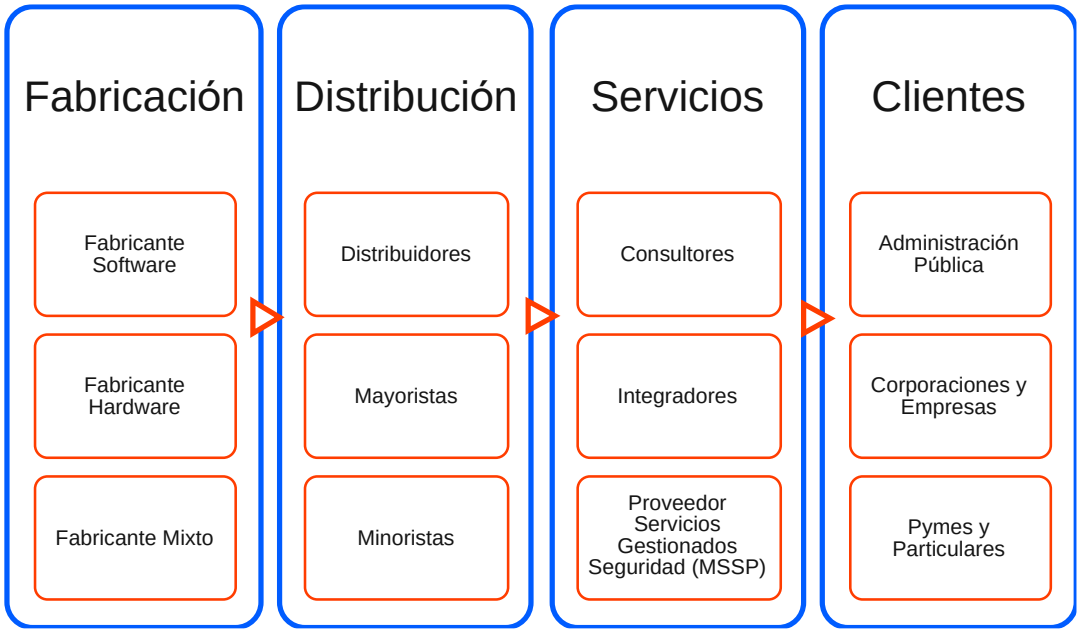
Por último, en relación con los aspectos organizacionales mencionados en el mercado global, la aparición del rol del responsable de ciberseguridad en algunas empresas chilenas constituye un aspecto positivo en la implementación de Estrategias de CiberSeguridad. Asimismo, la presencia del Director de Seguridad de la Información (CISO) en los organigramas de las empresas de Chile, será cada vez más frecuente y un apoyo relevante al CEO (Chief Executive Officer) en el establecimiento de estrategias de seguridad de las compañías.

4.3 Cadena de Valor Servicios Ciberseguridad

Para entender mejor el mercado, es necesario analizar las principales actores y actividades que forman parte de la cadena de valor para la creación de productos o comercialización de servicios de CiberSeguridad (ver Figura 8). Los servicios se dividen en tres grandes grupos:

- Fabricación de hardware y desarrollo de software
- Distribución de productos de ciberseguridad
- Prestación de servicios de ciberseguridad

Figura 8: Cadena de Valor Servicios Ciberseguridad



Fuente: INCIBE - Tendencias en el mercado de la Ciberseguridad

De acuerdo a la cadena de valor indicada anteriormente, se considerará a ENTEL S.A. como un Prestador de Servicios de Ciberseguridad que presta servicios de Consultoría, Integración (Venta e Implementación de Equipamiento) y de Proveedor Servicios Gestionados de Seguridad (MSSP).

La descripción y análisis de los servicios prestados por ENTEL S.A., serán parte del capítulo 7 del presente trabajo.

5 Clientes de ciberseguridad

5.1 Clasificación de Clientes

Anteriormente se dio a conocer toda la cadena de valor de los servicios de CiberSeguridad. Los primeros 3 elementos de la cadena se denominarán Proveedores y serán descritos en el capítulo 6 de este proyecto. A continuación, se detallará el elemento final de la cadena que se denomina Clientes.

La demanda de soluciones y servicios de ciberseguridad (Clientes) se puede clasificar en 3 grandes grupos: Administraciones Públicas, Corporaciones y Empresas, Pymes y Particulares.

Los servicios demandados por los clientes abarcan:

- **Servicios reactivos**, destinados a responder a un incidente y a minimizar su impacto.
- **Servicios proactivos,** dirigidos a reducir los riesgos de seguridad a través de la implementación de sistemas de protección y detección.
- **Servicios de gestión,** que tiene como finalidad brindar seguridad a los procesos operacionales.

5.1.1 Administraciones Públicas

Se clasificarán en el grupo de Clientes Administración Públicas a los distintos organismos gubernamentales del país. Entre sus principales amenazas que demandan servicios de ciberseguridad, se destacan:

- Ciberespionaje político: Ataques cibernéticos entre gobiernos, difusión de noticias falsas en redes sociales y medios de comunicación o hackeo de cuentas de correo electrónico.
- Robo y venta o publicación de información sensible
- Disrupción de sistemas

Dado lo anterior, las administraciones públicas demandan soluciones y servicios de ciberseguridad integrales, tanto de ciberinteligencia como de ciberdefensa, ofertados por consultoras, integradores y proveedores de servicios gestionados de seguridad (MSSP).

5.1.2 Corporaciones y Empresas

Se clasificarán en el grupo de Clientes Corporaciones y Empresas a las organizaciones privadas con o sin fines de lucro. La demanda de soluciones de ciberseguridad del sector privado varía en función del ámbito, exposiciones a normativas legales y de la criticidad de los servicios en el que opera la empresa.

Las amenazas que enfrentan están asociadas a ataques de Ciberespionaje industrial, de control e interrupción de sistemas y de sustracción y venta de información confidencial. Una de las mayores amenazas son los “insiders”, personas que han mantenido o mantienen alguna relación con la empresa y tienen o han tenido acceso a los sistemas e información sensible.

Estas empresas demandan todo tipo de soluciones y servicios, desde auditorías técnicas, gestión de incidentes, soluciones de seguridad integral hasta seguridad en la nube.

5.1.3 Pymes y Particulares

Se clasificarán en el grupo de Clientes Pymes y Particulares, a las pequeñas y medianas empresas y a las personas naturales.

Su principal amenaza está asociada a la venta de datos proporcionados a organizaciones públicas y privadas, así como a posibles ataques de ciberdelincuencia. Los productos demandados por este grupo son soluciones básicas.

5.2 Marco normativo en Chile

En el contexto Global de la CiberSeguridad, se menciona la importancia del establecimiento de políticas públicas que regulen los aspectos asociados a la ciberseguridad. En este sentido Chile, durante los últimos años, ha comprometido una estrategia regulatoria cuyo fin es garantizar que los Gobiernos (de cualquier tendencia política) establezcan iniciativas para protegerse de ciberataques, que pueden poner en riesgo la estabilidad política y económica del país.

Esta estrategia regulatoria establece un marco normativo que determina los lineamientos que deben cumplir las empresas y particulares en Chile.

A continuación, se detallarán las principales iniciativas que forman parte del marco normativo en Chile.

5.2.1 Agenda Digital 2020

Es una hoja de ruta formulada en el año 2015, con un conjunto de 63 medidas que establecen las líneas maestras para el desarrollo digital del país, de manera inclusiva y sostenible a través de las Tecnologías de la información y la Comunicación. Entre las

medidas incluidas en la Agenda se menciona la elaboración de una Estrategia de Ciberseguridad, que corresponde a la actual Política Nacional de Ciberseguridad. Además en otras, la elaboración de Ley de Proyección de Datos Personales, la mejora de la protección de los derechos de los consumidores en la red, el desarrollo de un Plan Nacional de Infraestructura de Telecomunicaciones o el perfeccionamiento de la normativa sobre firma electrónica entre otras medidas.

5.2.2 Política Nacional de Ciberseguridad (PNCS)

La Política Nacional de Ciberseguridad (PNCS) fue establecida en el año 2017 de acuerdo los objetivos definidos en la Agenda Digital 2020. El Comité Interministerial sobre Ciberseguridad, integrado por las Subsecretarias de Interior, Relaciones Exteriores, Defensa, Hacienda, Secretaria General de la Presidencia, Economía, Justicia, Telecomunicaciones y la Agencia Nacional de Inteligencia, fueron los organizamos responsables de su elaboración, para la cual se contó con la colaboración de representantes de entidades gremiales, de empresas, de organizaciones de la sociedad civil, académicos y expertos nacionales e internacionales en ciberseguridad.

La PNCD tiene dos competentes centrales: Una política de Estado, diseñada con objetivos orientados al año 2022, y una agenda de medidas específicas para cumplir sus objetivos. A través de este diseño se propone una visión general de hacia dónde debe dirigirse Chile en el mediano y largo plazo, a la vez que se proponen medidas que puedan ser implementadas en el futuro cercano.

5.2.3 Normas en materia de ciberseguridad

Los aspectos relacionados con la ciberseguridad en Chile están regulados por un conjunto de normas legales y reglamentarias, las cuales están en revisión y actualización conforme a la Política Nacional de Ciberseguridad (PNCS) y a los tratados internacionales a los que el país se ha adherido. Estas normas están presenten en la Constitución política de la república, Leyes y Decretos. Por ejemplo, la ley Nº 19.223 sobre delitos informáticos o la ley Nº 19.628 sobre protección de la vida privada, entre otras.

Además, a nivel sectorial existen guías y directrices dictadas por las Superintendencias, fundamentalmente la Superintendencia de Bancos e Instituciones Financieras (SBIF). Dicho organismo ha emitido directrices como el capítulo 20-7 sobre Externalización de Servicios, el capítulo 20-8 sobre Comunicación Inmediata de Incidentes Operacionales o el capítulo 20-9 sobre Gestión de Continuidad del Negocio. En diciembre del año 2017, modifico el capítulo 1-13 de la Recopilación Actualizada de Normas sobre la Administración del Riesgos Operacional, incorporando la exigencia a los bancos de implementar una adecuada gestión de la infraestructura critica a efectos de Ciberseguridad.

Estas directrices son de cumplimiento obligado en caso de investigación penal. Por otra parte, el sector privado no informa de violaciones sufridas por posibles efectos negativos sobre su reputación.

5.2.4 Tratado de Budapest

En el año 2017, Chile se adhirió al Convenio de Budapest, este convenio constituye el primer tratado internacional sobre delitos informáticos y delitos cometidos a través de Internet y de otras redes informáticas. Además, incluye una serie de competencias y procedimientos, como la búsqueda de las redes informáticas y la interceptación legal, con el fin de mejorar la investigación de este tipo de delitos.

La adhesión de este instrumento internacional permite a Chile formar parte de un sistema rápido y eficaz de cooperación internacional en tareas tales como: extradición de personas, asistencia mutua en investigación y persecución de ilícitos, así de formar parte de una red de colaboración que funciona 24/7.

5.2.5 Ley de Protección de Datos Personales

La Ley de Protección de Datos Personales aprobada en el año 2018, se enmarca en los esfuerzos que ha realizado Chile para lograr la adaptación de sus políticas públicas y legislación interna a las recomendaciones emitidas por la Organización para la Cooperación y el Desarrollo Económico (OCDE).

La ley tiene como objetivo general actualizar y modernizar el marco normativo e institucional con el propósito de establecer que el tratamiento de los datos personales de las personas naturales se realice con el consentimiento del titular o en los casos que autorice la ley, reforzando la idea de que los datos personales deben estar bajo el control de su titular, favoreciendo su protección frente a toda intromisión de terceros y estableciendo las condiciones regulatorias bajo las cuales los terceros pueden efectuar legítimamente el tratamiento de tales datos, asegurando estándares de calidad, información, transparencia y seguridad.

Las normativas mencionadas anteriormente han provocado que las empresas deban adaptar sus procesos y tecnologías acorde a los marcos regulatorios vigentes, y con ello a buscar un partner que los guie en los Procesos de Compliance. En consecuencia, la demanda de los servicios de CiberSeguridad se ha incrementado, lo que significa una oportunidad para los proveedores de estos servicios, como es ENTEL S.A.

6 Proveedores de ciberseguridad

6.1 Clasificación de Proveedores

Considerando las etapas de la cadena de valor en la que intervienen, los proveedores se clasifican en los siguientes grupos:

- Fabricación de hardware y desarrollo de software
- Distribución de productos de ciberseguridad
- Prestación de servicios de ciberseguridad

6.1.1 Fabricación de hardware y desarrollo de software

En este grupo de empresas se desarrollan soluciones y herramientas físicas de cifrado para garantizar la seguridad en la movilidad y en las redes corporativas. Y en el caso del desarrollo de software, se crean soluciones y aplicaciones (no físicas) para garantizar la seguridad en la red y contribuir a la gestión y control de acceso web e identidad de los usuarios.

6.1.2 Distribución de productos de ciberseguridad

Este grupo está compuesto por empresas que hacen de intermediarios entre las actividades de fabricación y prestación de servicios. En esta actividad operan Distribuidores, Mayoristas y Minoristas.

- Distribuidores: Venden directamente a empresas de ciberseguridad o a clientes finales los productos de ciberseguridad. Pueden comercializar sus productos a los prestadores de servicios.

- Mayoristas: Compran y venden productos de ciberseguridad a consultoras, a los integradores y a los proveedores de servicios gestionados de seguridad. Los mayoristas pueden estar especializados en seguridad TIC o bien, dedicarse a una actividad más genérica (informática, electrónica, etc.).

- Minoristas: Son puntos de venta constituidos por tiendas físicas de informática, retail e incluso pequeñas consultoras enfocadas a Pymes y particulares.

6.1.3 Prestación de servicios de ciberseguridad

Son parte de este grupo las empresas que comercializan sus bienes y servicios al cliente final, entre los que destacan la Administración Publica, Corporaciones y Empresas, y Pymes y los particulares.

- Consultoras: Prestan servicios especializados en ciberseguridad en torno a dos ámbitos: negocio y tecnología. Las consultoras de negocio se dedican a la consultoría y asesoría orientada a los asuntos legales y organizativos de la seguridad de la información. Sin embargo, las consultoras tecnológicas se encuentran especializadas en servicios de asesoramiento, respuesta y soporte relativos a las tecnologías de seguridad.

- Integradores: Crean soluciones complejas de seguridad TIC, adaptándose a las necesidades de los usuarios. Utilizan, con frecuencia, productos de diversos fabricantes y los complementan con soluciones propias.

- Proveedores de servicios gestionados de seguridad (MSSP, Managed Security Service Providers). Proporcionan servicios externalizados de seguridad al cliente con un enfoque integral y multidisciplinario de la seguridad, incluyendo servicios de consultoría, servicios de desarrollo o de integración.

Es importante señalar que algunas empresas pueden pertenecer a varios grupos de proveedores y no seguir necesariamente la secuencia de la cadena de valor. Por ejemplo, los de fabricantes de software que venden a minoristas, o directamente a clientes finales, y además ofrecen servicios de ciberseguridad. Otro ejemplo, es IBM, que está presente en las cinco actividades de comercialización. Del mismo modo, Telefónica y Entel, además de proveedores son también integradores, entregan servicios de consultoría y servicios gestionados de seguridad.

6.1.4 Proveedores de servicios gestionados de seguridad (MSSP)

En el contexto de este proyecto, la formulación de una estrategia competitiva asociada a los Servicios de CiberSeguridad se centrará en el análisis de los Proveedores de Servicios gestionados de seguridad (MSSP). De acuerdo con la anterior, Gartner, en su informe de “Magic Quadrant for Managed Security Services, Worldwide - 2018” establece que los MSSP se categorizan en tres grupos, pudiendo existir superposición entre estos grupos, pero estos tienden a caer en una de las categorías.

Player de Nicho: Generalmente son MSSP empresas que se centran por completo en los servicios de seguridad. La mayoría de estos MSSP tienden a servir a un mercado o región local, pero no a todas las regiones del mundo. Por lo general este tipo de proveedores son adquiridos o subcontratados por otras empresas de proveedoras de Servicios de TI o MSSP para incorporar conocimiento y experiencia que estas empresas no poseen.

Telcos: Son proveedores de conectividad y ancho de banda de red que administran y supervisan productos de seguridad de red. A menudo proporcionan monitoreo remoto, tecnologías locales y servicios basados en la nube a través de sus conexiones a Internet.

Los clientes que consumen servicios de telecomunicaciones administrados tienden a incluir MSS cuando están disponibles como firewalls y otras tecnologías de seguridad basadas en la red pueden ser un componente central de los acuerdos de outsourcing.

TI: Son proveedores de servicios de TI que generalmente administran dispositivos de seguridad como parte de grandes iniciativas de outsourcing o integración de sistemas, donde tiene sentido que los clientes consuman MSS como parte de acuerdos generales de administración y monitoreo de infraestructura.

Además de los grupos anteriores, los proveedores de Consultoría de seguridad y algunos fabricantes de tecnologías son participantes emergentes que ofrecen servicios de MSS. La consultoría de seguridad se ha dado cuenta de que los servicios de MSS y los contratos de operaciones de seguridad son una fuente de ingresos rentable, predecible y de crecimiento más rápido que los proyectos de consultoría por si solos. También vale la pena señalar que muchos subcontratistas de TI con empresas de consultoría de seguridad también se están volviendo más activos como MSSP, a través de adquisiciones o el desarrollo de capacidades de seguridad.

Considerando la categorización anterior, podemos identificar en el mercado chileno a los principales proveedores de MSSP y Consultoras (ver Figura 9). ENTEL S.A. lograr establecer una ventaja al estar presenten en el outsoucing de servicios TELCO, TI, Consultoría y MSSP, logrando incorporar la gestión de servicios de seguridad de punta a punta dentro de su portafolio de servicios.

Figura 9: Proveedores de Servicios gestionados de seguridad (MSSP) en Chile

Fuente: Elaboración Propia

6.2 Soluciones de CiberSeguridad

Los proveedores mencionados en este capítulo, cuentan con diversos tipos de soluciones que pueden ser adaptadas a las necesidades de cada cliente. De acuerdo con el informe elaborado por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI, 2015), Las soluciones de ciberseguridad se pueden clasificar en tres tipos Prevención, Control y Mitigación.

6.2.1 Soluciones de Prevención

Buscan evitar que se produzcan incidentes. Se incluyen las siguientes:

- **Anti-malware:** Anti-virus, Anti-adware, Anti-spyware, Gestión Unificada de Amenazas.

- **Anti-fraude:** Anti-phising, Anti-spam, Herramientas de filtrado de navegación, Gestión unificada de amenazas y plataformas de protección endpoint.

- **Soluciones de prevención de funda de información:** Control de contenidos confidenciales, Gestión del ciclo de vida de la información, Control de dispositivos externos de almacenamiento, Cifrado de discos duros y soportes de almacenamiento.

- **Protección de las comunicaciones:** Cortafuegos o firewall, Redes privadas virtuales (VPN), Routers seguros, Gestión unificada de Amenazas, Prevención y detección de intrusiones IPS IDS, Cifrado de las comunicaciones, Filtro de Contenidos, Herramientas de Control P2P, Gestión y Control de ancho de banda, Herramientas de monitorización y reporting, Seguridad en el correo, Seguridad Web.

- **Seguridad en dispositivos móviles:** Seguridad para dispositivos móviles, Seguridad redes inalámbricas, Seguridad para “trae tu propio dispositivo” o BYOD.

6.2.2 Soluciones de Control

Destinadas a la gestión y cumplimiento de normativas. Tales como:

- **Auditoría técnica:** Análisis de logs y puertos, Análisis de vulnerabilidades, Auditoria de contraseñas, Auditoria de sistemas y archivos, Auditoria de red, Herramientas de recuperación de datos, Herramientas de testeo de software y aplicaciones Web.

- **Soluciones de certificación normativa:** Sistemas de gestión de la seguridad de la información (SGSI), Análisis de riesgos, Planes y políticas de seguridad, Normativas de Seguridad, Borrado seguro y Destrucción documental.

- **Soluciones de control de acceso y autentificación.** Control de acceso de red (NAC) y a la web, Gestión de identidad y autenticación, Herramientas de autenticación o validación única, Certificados digitales, Firma electrónica, Tarjetas inteligentes y dispositivos biométricos, Brokers de acceso cloud.

6.2.3 Soluciones de Mitigación

Una vez ocurrido el incidente, este tipo de soluciones tratan de restaurar el funcionamiento normal de los sistemas y mitigar el daño. Se agrupan en las siguientes:

- **Soluciones de contingencia y continuidad:** Gestión de planes de contingencia y continuidad, Herramientas de recuperación de sistemas, Copias de seguridad, Infraestructuras de respaldo, Seguridad de virtualización, Herramientas de seguridad en la nube.

- **Soluciones de inteligencia de seguridad:** Gestión de eventos de seguridad (SIEM), Gestión de información de seguridad (SIM) y Gestión de información de eventos de seguridad (SIEM), Soluciones Big Data, Herramientas de monitorización y reporting.

Dado los antecedentes entregados anteriormente los principales componentes del portafolio de Servicios de CiberSeguridad de ENTEL S.A. deben considerar los siguientes:

- **Servicios Especializados en Ciberseguridad** con foco en Consultorías y Compliance, es lo que nos dará una diferenciación, y por los cuáles permitirá realizar una Preventa Consultiva y establecer con los clientes una hoja de ruta de Seguridad.

- **Gestión Estratégica de los Riesgos** como una Metodología aplicada en el Levantamiento de los proyectos como en la Operación para la protección de los Activos e Infraestructura Critica de los clientes.

- **Gobierno de la Seguridad**, permite generar asesoras para alinear los procesos, personas y tecnología en una estrategia de defensa común y orientada a los clientes.

- **Centro de Operaciones de Ciberseguridad (C-SOC)**, comienza a ser la base para el monitoreo proactivo, gestión de eventos, control de ataques y análisis de la seguridad en las empresas. Este puede estar entregado en un modelo interno, externo o híbrido, el modelo dependerá de las necesidades de los clientes

ENTEL S.A. como prestador de servicios de CiberSeguridad, pone a disposición de sus clientes todas las soluciones mencionadas anteriormente y pueden ser adaptadas a las distintas necesidades. En el capítulo siguiente se analizará en detalle el catalogó de soluciones ofrecidas por ENTEL S.A.

7 Servicios de Entel CyberSecure

En el capítulo anterior se analizó la industria de ciberseguridad, su cadena de valor y la clasificación de clientes, proveedores y servicios que son parte de este mercado. Como parte de este capítulo se analizará la propuesta de valor actual de ENTEL S.A en su servicio de CiberSeguridad.

Antes de detallar la propuesta de valor del servicio de CiberSeguridad de ENTEL S.A., es necesario revisar algunos elementos de contexto de la compañía en Chile y describir la estrategia corporativa actual. Posteriormente, se profundizará en las características del segmento Corporaciones, en donde está inserto el portafolio de servicios de CiberSeguridad.

7.1 Descripción de la Organización

Empresa Nacional de Telecomunicaciones (Entel S.A.) es un operador importante de telecomunicaciones en Chile desde el año 1964 y a partir del año 2013 cuenta con una creciente operación en Perú. En ambos países su foco es la experiencia de clientes, con énfasis en la innovación, operando sobre la base de una infraestructura de red y de servicios propia y de última generación.

En Chile ofrece servicios para los segmentos de clientes Personas, Empresas y Corporaciones, atiende desde necesidades cotidianas a procesos complejos, de negocios o instituciones a través de acompañamiento en transformación digital, contact center y outsourcing de servicios de tecnologías de la información y comunicaciones.

La propuesta de valor de ENTEL S.A. consiste en entregar experiencias de servicios simples y eficientes, a través de una infraestructura para comunicaciones móviles, fijas y tecnologías de la información digitales.

- Propósito: Acercar las infinitas posibilidades que da la tecnología y así transformar responsablemente la sociedad.

- Misión: Hacer que todos vivamos mejor conectados, contribuyendo responsablemente a transformar nuestra sociedad.

- Visión: Una empresa de servicio de clase mundial, que entrega una experiencia distintiva a sus clientes. Un lugar donde su gente se realiza. Una empresa que se reinventa permanentemente para profundizar su rol de liderazgo.

7.1.1 Estrategia Corporativa

El modelo de negocios de ENTEL S.A ha transitado desde los servicios de voz a los datos, con una oferta que evoluciona constantemente según las necesidades del mercado. La estrategia corporativa se establece sobre la base de cuatro pilares esenciales:

1. Innovación y Adaptación:
   La innovación es un fundamento estratégico para ENTEL S.A, que le permite construir ventajas competitivas y facilita la adaptación permanente ante el escenario cambiante. Por ello, la innovación está integrada en sus pilares culturales y es responsabilidad de todos sus colaboradores.

2. Organización y cultura agiles:
   Durante los últimos tres años, ENTEL S.A ha adaptado su organización, con el objetivo de alinearla a la estrategia de negocios y las necesidades del mercado. Ha definido la estructura organizacional bajo un esquema tradicional y otro ágil, cuenta con estrategias de gestión de personas diferenciadas según sus características y necesidades (Gestión, Proyectos, Expertos), que permiten un desarrollo profesional más eficiente.

3. Experiencia Distintiva:
   ENTEL S.A ofrece a sus clientes una experiencia distintiva basada en soluciones estándar y particulares a cada cliente, de acuerdo con un modelo de trabajo en equipo transversal y con un alto grado de innovación. Buscado aumentar el valor de sus negocios.

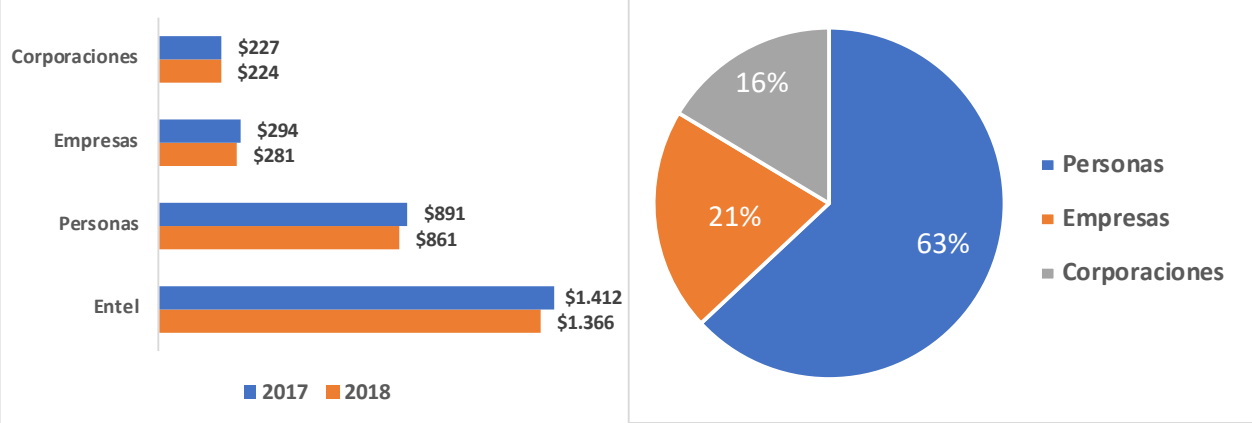
4. Infraestructura moderna y robusta:
   En un escenario altamente competitivo y que evoluciona constantemente, Entel invierte en forma continua en redes, plataformas y data center. En este contexto, durante el año 2017 la compañía destinó en total de US$ 521 millones a infraestructura.

La estrategia corporativa de ENTEL S.A, considera distintas líneas de acción para los principales segmentos de mercado que la compañía ha definido: Personas, Empresas, y Corporaciones. Por su especificidad, cada uno de estos segmentos, organizacionalmente estructurados como Vicepresidencias, cuenta con equipos propios para las funciones de innovación y desarrollo de productos, precios, marketing, ventas y servicio al cliente, alineados a lo establecido en los pilares estratégicos de la compañía.

7.1.2 Participación de Mercado en Chile

La industria de telecomunicaciones en Chile, incluyendo servicios a Personas, Empresas y Corporaciones, durante el año 2018 alcanzó los $5.934 miles de millones en ingresos brutos, según estimaciones de la compañía en base a información publicada por los participantes de la industria. La participación de mercado de ENTEL S.A. ese mismo año fue de un 24,1%. La distribución de los ingresos de Entel S.A. del año 2018, por tipo de mercado, se detalla en la tabla siguiente:

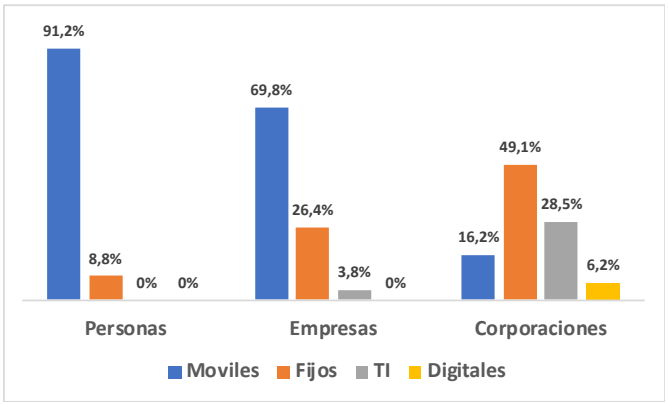
Tabla 1: Distribución de ingresos Mercados de ENTEL S.A.



Fuente: Memoria Corporativa 2018 ENTEL S.A.

La oferta de los principales servicios de la compañía para cada mercado, se indica en la siguiente tabla:

Tabla 2: Participación de Servicios por Mercados de ENTEL S.A.



Fuente: Memoria Corporativa 2018 ENTEL S.A.

El desarrollo de este trabajo se enfocará en el segmento Corporaciones, que en el año 2018 generó ingresos por 224 miles de millones, equivalentes a un 16% de los ingresos totales.

En particular se abordará la oferta de Servicios de Ciberseguridad, que es parte de la línea de negocios Digitales, que corresponde a un 6,2% de los ingresos de Corporaciones. En los párrafos siguientes, se entrega el análisis detallado de este mercado.

7.1.3 Mercado Corporaciones

Comprende a cerca de 586 conglomerados (2.360 Rut's) con operaciones en Chile que requieren soluciones específicas, así como a servicios públicos del Estado. Para dar respuesta a los procesos estratégicos de las operaciones de estos clientes, ENTEL S.A. provee soluciones particulares, especializadas y convergentes de servicios Móviles, Fijos, TI y Digitales.

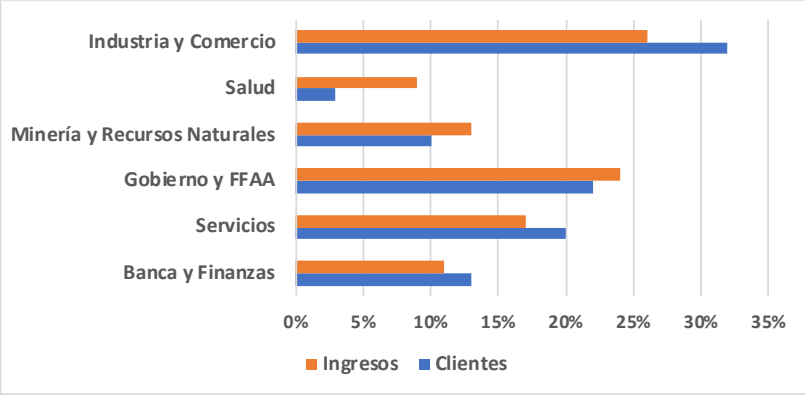
La estrategia de negocio de ENTEL S.A. para este mercado, pone foco en lo siguiente:

- Incrementar ingresos a través de nuevos servicios digitales.
- Defender y evolucionar negocio tradicional.
- Incrementar rentabilidad, eficiencia y control de inversiones.

La estrategia por formular en este trabajo, para el Servicio de Ciberseguridad, se enmarca en los focos indicados en el párrafo anterior, y tiene por objetivo incrementar los ingresos y su participación de mercado en Chile.

La segmentación de clientes en el Mercado Corporaciones se compone de 6 grupos, agrupados de acuerdo a las características propias de sus industrias y operaciones: Banca y Finanzas, Servicios, Gobierno, Minería y Recursos Naturales, Salud, Industria y Comercio. El porcentaje de clientes y la participación de ingresos por cada segmento, se detalle en la siguiente tabla.

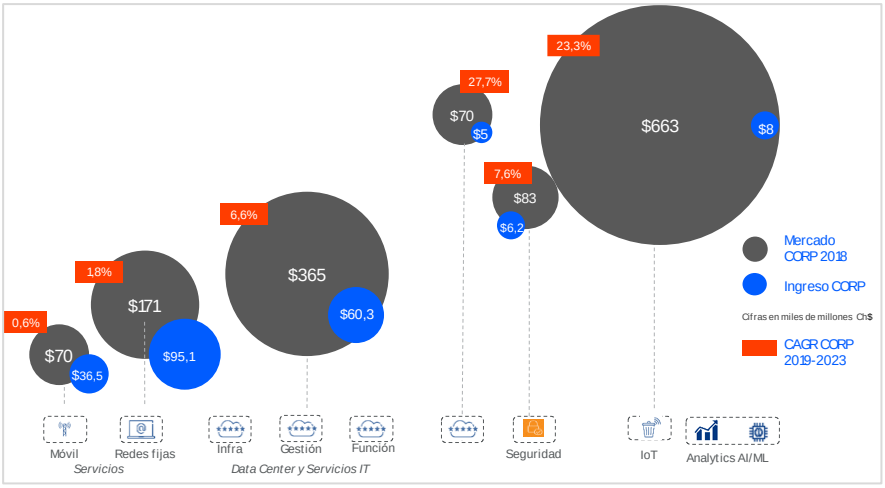
Tabla 3 – Clientes y porcentaje de Ingresos Mercado Corporaciones



Fuente: Estimación Interna VP Corporaciones ENTEL S.A. 2018

Según información IDC Chile, el tamaño del mercado Corporaciones (ver Figura 10) en nuestro país, durante el año 2018 alcanzó un total de 1.422 miles de millones de pesos; de los cuales 83 miles de millones de pesos corresponden a los servicios de CiberSeguridad. Para ENTEL S.A. los ingresos de este servicio alcanzaron 6,2 miles de millones de pesos y se espera una tasa de crecimiento anual (CAGR) de un 7,6% al 2023 según el informe de Cybersecurity: IDC, 2019.

Figura 10: Tamaño Mercado Corporaciones 2018



Fuente: IDC Chile + Estimación interna VP Corporaciones ENTEL S.A. 2018

Actualmente la participación de mercado de ENTEL S.A para los servicios de CiberSeguridad es de un 7,5%, esta cifra puede ser considerada baja, pero representa una oportunidad con alto potencial de crecimiento.

Los principales factores que explican el potencial de crecimiento de los servicios de Ciberseguridad, se detallan a continuación:

- En los capítulos 4 y 6 se describe la cadena de valor de los Servicios de Ciberseguridad. Entel S.A participa en la cadena de valor en la distribución, integración y gestión de servicios, lo que representa una ventaja en las oportunidades de venta de servicios
- Los servicios de Ciberseguridad pueden ser incorporados como complemento a las otras líneas de negocios del mercado Corporaciones (Servicios móviles y fijos, TI y negocios digitales), entregando una oferta de seguridad de punta a punta dentro de su portafolio de servicios.
- El punto anterior también representa una ventaja de crecimiento en el mercado Empresas de Entel S.A.
- Estos factores tienen efectos positivos para satisfacer y retener a los actuales clientes de Entel S.A., como en la atracción de potenciales nuevos clientes.

7.1.4 Entel CyberSecure

Entel ofrece “Entel CyberSecure” desde 2017, un portafolio de soluciones y servicios de ciberseguridad para la protección, defensa, gestión de riesgos y cumplimiento normativo de los sistemas TIC para las empresas, corporaciones y gobierno.

En el análisis del mercado, en particular, en la descripción de sus servicios, se mencionaron los componentes clave de un portafolio de Servicios de CiberSeguridad: Servicios Especializados en Ciberseguridad, Gestión Estratégica de los Riesgos, Gobierno de la Seguridad y Centro de Ciber Inteligencia (CCI). El alcance del portafolio Entel CyberSecure considera todos estos elementos.

7.1.4.1 Servicios

El portafolio de Ciberseguridad cubre una amplia gama de servicios, que se adapta a las necesidades de los clientes, se detallan en la figura 11:

Figura 11: Portafolio Entel CyberSecure

Consultorías		Soluciones	Servicios	
Consultorías Estratégicas	Business Continuity	Soluciones Ciberseguridad	Seguridad en la Nube	Suite CCI
• Governance & Risk (GRC, Risk Assessment) • Security Testing (Vulnerability Scanning, Ethical Hacking) • Análisis Avanzados (Análisis Forense, Análisis de Código) • Plan & Design	• DRP (Disaster Recovery Plan) • BCP (Business Continuity Plan)	• Protección WEB (WAF/Anti DDoS on premise) • Balanceo y Optimización • Comunicaciones Seguras (SDN WAN/CPE Seguro) • Correo Seguro • Anti APT/Sandboxing • Endpoint Protection • Control de Acceso y PAM	• CASB (Cloud Access Security Broker) • Escudo de Protección en la Nube • Secaas (Security as a Services)	• Servicios Detección (Gestión Vulnerabilidades, Gestión de Amenazas) • Servicios de Prevención (Hardening, Gestión de Eventos de Seguridad) • Servicios de Respuesta (Gestión Incidentes Seguridad, Threat Hunting, Forense)

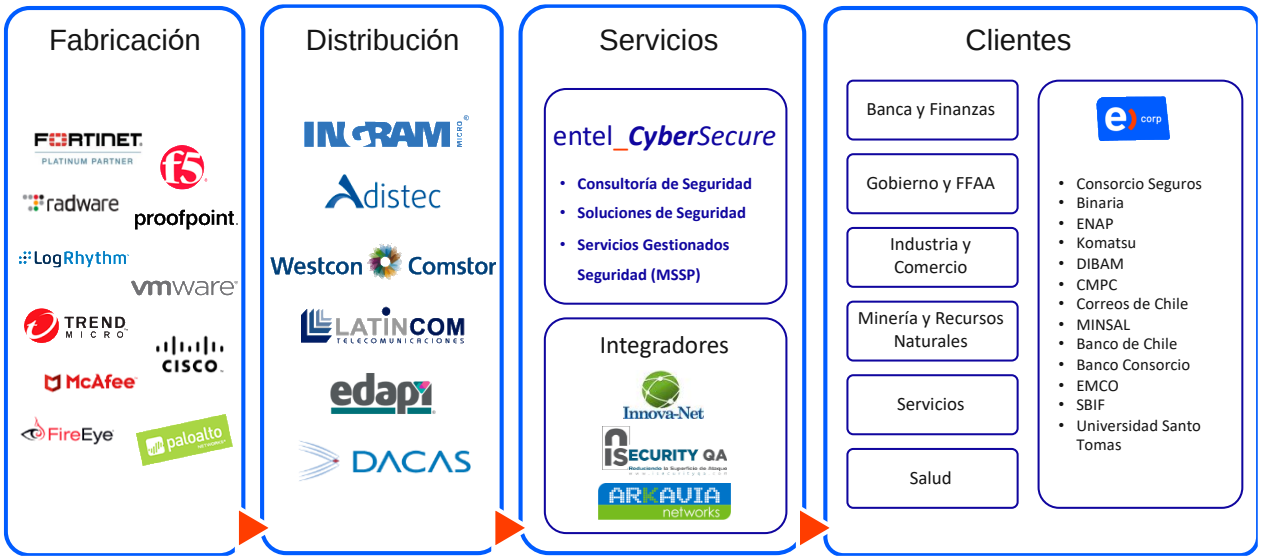
Fuente: VP Corporaciones ENTEL S.A. 2018

La descripción de estos servicios se encuentra disponible en el sitio de web de ENTEL S.A. en la siguiente dirección: https://www.entel.cl/corporaciones/ciberseguridad/.

7.1.4.2 Cadena de Valor

Tomando como base los conceptos de la cadena de valor de Ciberseguridad, mencionados en el capítulo 4 de este trabajo; en la figura 12 se describe la cadena de valor de ENTEL S.A en los servicios de Ciberseguridad.

Figura 12: Cadena de valor Servicio Ciberseguridad ENTEL S.A.



Fuente: Elaboración propia

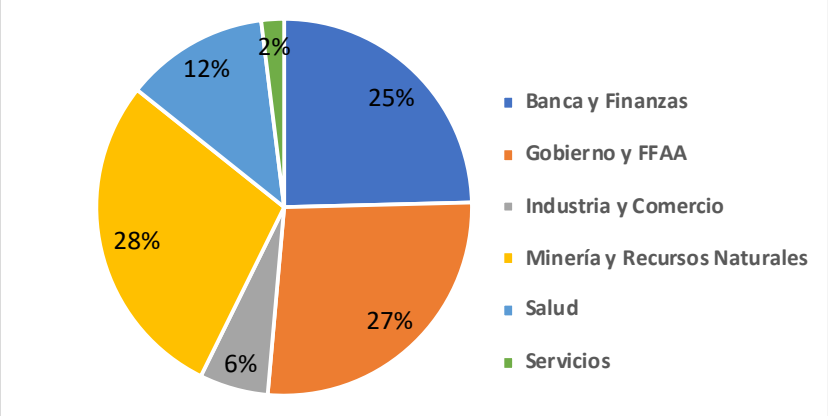
Fabricación: En esta etapa se seleccionan las tecnologías (productos) que forman parte del portafolio de Servicios. Estas tecnologías son creadas por un grupo de empresas que desarrollan y ponen a disposición del mercado soluciones de seguridad. La selección se realiza considerando las tendencias mundiales y las demandas particulares de los clientes. ENTEL S.A. cuenta con alianzas estratégicas y acuerdos con partners de seguridad a nivel mundial, con fines comerciales y certificaciones de calidad del servicio.

Distribución: Posteriormente, se gestionan las empresas que hacen de intermediarios entre las actividades de fabricación y prestación de servicios. Este rol es relevante en términos comerciales, en caso de que el fabricante no tenga representación de sus productos en Chile. Además, en términos logísticos, permite la rápida disponibilidad de productos sin generar costos adicionales de stock o traslado.

Servicios: La comercialización de los servicios al cliente final, por parte de ENTEL S.A., puede desarrollarse a través de consultorías, integración de soluciones, o la externalización de la operación de las soluciones de seguridad (MSSP). La entrega de estos servicios es realizada con capacidades internas de la compañía o mediante la alianza con otras empresas integradoras.

Clientes: Existen 13 Clientes que cuentan con servicios de CiberSeguridad. La composición de la cartera de clientes de acuerdo a la participación de ingresos por cada segmento se detalla en la siguiente tabla.

Tabla 4 – Distribución de ingresos Clientes Ciberseguridad Mercado Corporaciones

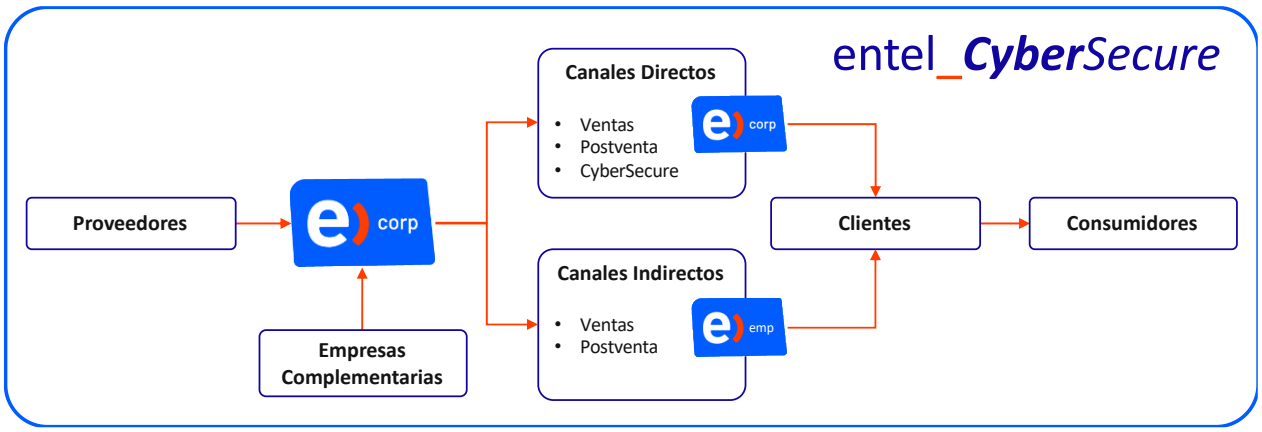


Fuente: Estimación Interna VP Corporaciones ENTEL S.A. 2018

7.1.4.3 Empresa Extendida

Al inicio de este trabajo, se menciona el concepto de Empresa Extendida, que de acuerdo al modelo Delta, corresponde a un sistema que se basa en la colaboración con clientes y proveedores, e integrar en la estrategia de negocio todos los elementos que forman parte de la cadena de valor. En la figura 13, se utiliza el concepto de empresa extendida para describir el sistema en que se entra inserto Entel S.A.

Figura 13 – Empresa Extendida, Servicios de Ciberseguridad ENTEL S.A.

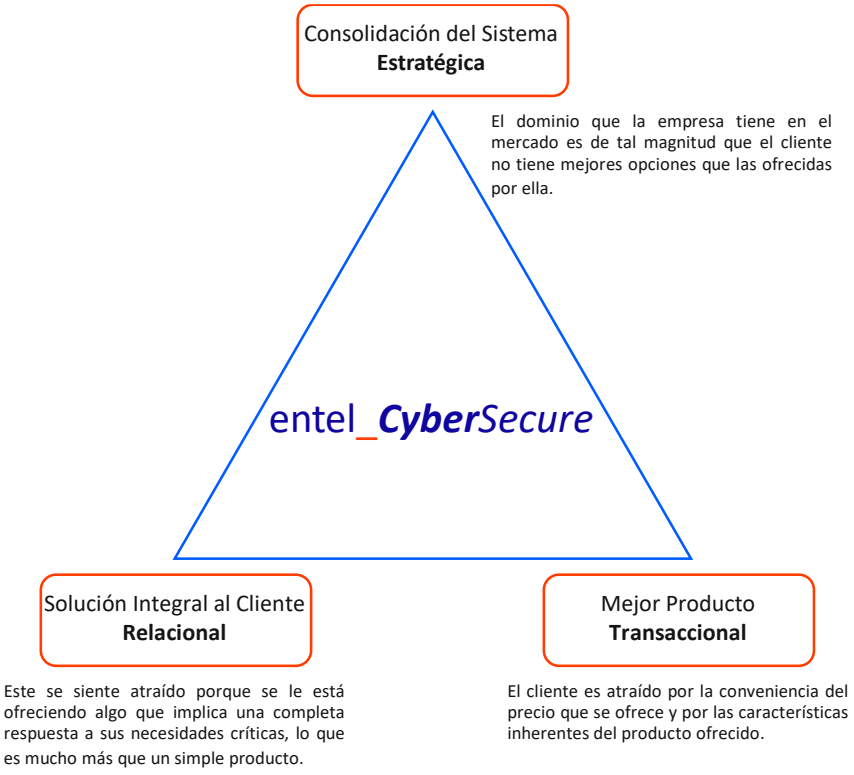


Fuente: Elaboración propia

El libro “Lecciones en Estrategia, hacia una gestión de excelencia”, menciona que es relevante identificar a todos los participantes en la empresa extendida y sus vínculos con la compañía. De acuerdo al Modelo Delta, estos vínculos pueden ser puramente “Transaccionales” en el vértice del Mejor Producto, “Relacionales” en el de la Solución Integral al Cliente o “Estratégicas” en el de Consolidación del Sistema.

En los párrafos siguientes se describirá la relación de ENTEL S.A. con los integrantes de la cadena de valor para los servicios de CiberSeguridad (ver Figura 14):

Figura 14 – Asociación entre la naturaleza de la relación y la posición estratégica.



Fuente: Hax, Arnoldo. Lecciones en estrategia

Relación con Proveedores:

Es un aspecto fundamental de la empresa extendida. Cuando existe confianza y comprensión mutua, un proveedor se transforma en un socio estratégico, capaz de generar “soluciones a la medida”. ENTEL S.A. mantiene en condición de socio estratégico a proveedores, mencionados en la cadena de valor como Fabricantes (Partnership de Seguridad Internacional), con los cuales existen alianzas y acuerdos. Las tecnologías que estos proveedores ofrecen al mercado, también pueden ser adquiridas por empresas competidoras; por lo tanto, la diferenciación en el portafolio de servicios se logra a través de las competencias y capacidades propias de la compañía.

Relación con empresas complementarias:

ENTEL S.A. se apoya con empresas complementarias para la entrega de los Servicios de Ciberseguridad, mencionadas en la cadena de valor como Integradores. El rol que cumplen estas empresas es aportar con conocimientos y experiencia en tecnologías específicas, lo que le permite ampliar su oferta de integración de servicios. La relación que ENTEL S.A. mantiene con estas empresas integradoras es transaccional; no se comparte mayor información respecto de necesidades del cliente y otros servicios que posean con la compañía.

Relación con los canales de distribución:

Corresponde a quien tiene el acercamiento final hacia el cliente por consiguiente, posee la mayor información y la más íntima relación con él. Por tanto, es una componente central de la estrategia hacer una adecuada definición y desarrollo. Para el caso de ENTEL S.A, se denominará canales directos a aquellas unidades que pertenecen al mercado Corporaciones: Ventas, post venta, especializados principalmente en los Servicios móviles, fijos y TI, y un área comercial especialista Cybersecure a cargo de los Servicios de Ciberseguridad. Los canales indirectos corresponden a las unidades comerciales venta y post venta del mercado Empresas.

Relación con clientes y consumidores:

Son el centro de la estrategia. La esencia de la estrategia radica no solo en lograr una ventaja competitiva permanente, sino en lograr establecer lazos irrompibles, un conocimiento profundo y una vinculación afectiva con el cliente. Desde esta perspectiva el cliente es un elemento relevante de competitividad. El mercado Corporaciones de ENTEL S.A. declara dentro de su estrategia, lograr una relación basada en la generación de valor. Este concepto guía al mercado corporaciones a ser los mejores en la industria, mediante el apoyo a los clientes para transformar y aumentar el valor de sus negocios; y con ello, multiplicar el crecimiento y el valor del negocio de Corporaciones. Actualmente este compromiso de relación con los clientes tiene dos áreas con oportunidades de mejora: Existen mecanismos de medición de calidad, a través de encuestas de satisfacción para los servicios móviles, fijos y TI, pero no para los servicios de Ciberseguridad. Además, el portafolio de servicios actual es transversal a todos los

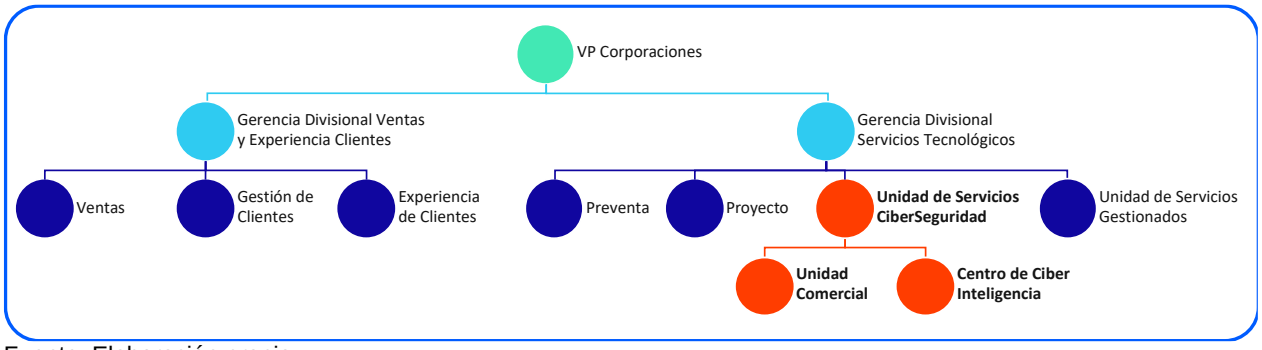
segmentos de clientes y no especializado de acuerdo a las características de la industria y operación de los clientes.

7.1.4.4 Estructura Organizacional

La Vicepresidencia de Corporaciones, cuenta con una estructura organizacional, con competencias y capacidades que le permiten desarrollar las distintas etapas de la cadena de valor. Esta estructura en su mayoría es compartida con los servicios móviles, fijos y TI; y en el caso de los de los Servicios de Ciberseguridad, existen unidades especializadas y dedicadas a apoyo comercial y la operación de las soluciones.

En la figura 15, se presenta la estructura organizacional que interviene en los servicios de Ciberseguridad, corresponde a una parte (no la totalidad) de la vicepresidencia de corporaciones de ENTEL S.A. En los párrafos posteriores, se describen cada una de las unidades relacionadas.

Figura 15 – Estructura Organizacional Mercado Corporaciones



Fuente: Elaboración propia

Gerencia Divisional Ventas y Experiencia Clientes:

Tiene la responsabilidad de la comercialización de los servicios móviles, fijos, TI y Ciberseguridad. Está conformada por tres unidades:

- **Ventas**: Gestión de la cartera de clientes, según la segmentación presentada anteriormente. Se especializan en los servicios móviles, fijos, y TI. No cuentan con las capacidades suficientes para la comercialización de los servicios de ciberseguridad, por lo anterior, se complementan con las capacidades de la unidad comercial especializada, de la Gerencia Divisional de Servicios Tecnológicos. La Vicepresidencia no cuenta con

incentivos comerciales adecuados, que propicien el desarrollo de capacidades en los equipos comerciales. Además, no se pone a disposición de los equipos, información propia del mercado de Ciberseguridad, que les permita ofrecer este portafolio a su cartera de clientes actual o atraer nuevos clientes.

- **Gestión de clientes**: A cargo de la post venta y administración de contratos de servicios móviles, fijos, y TI; organizados con la misma segmentación de clientes anterior. Para los servicios de Ciberseguridad, esta gestión está a cargo de la unidad comercial especializada, de la Gerencia Divisional de Servicios Tecnológicos. Al existir una gestión de post venta enfocada sólo en los servicios móviles, fijos, y TI, disminuye la oportunidad de capturar nuevos negocios con la cartera de clientes actual. Para los clientes que cuentan con Ciberseguridad y además alguno de los otros servicios anteriores, existirán dos canales de gestión; lo que no contribuye a generar oportunidades de integración a través de los distintos portafolios de servicios.

- **Experiencia de clientes:** Responsable de los estudios de satisfacción, sólo para los servicios móviles, fijos, y TI. Actualmente el portafolio de servicios de Ciberseguridad no posee estudios de satisfacción. Lo anterior no permite conocer si se resuelven las necesidades de los clientes, reforzar aspectos positivos del servicio, además de mejorar los aspectos negativos.

Gerencia Divisional Servicios Tecnológicos:

El alcance de sus responsabilidades se inicia con el apoyo a las unidades comerciales en la evaluación y diseño de las propuestas, hasta la implementación y operación de los proyectos adjudicados. Todo eso en el marco de los servicios móviles, fijos, TI y Ciberseguridad. Está conformada por cuatro unidades:

- **Preventa:** Unidades técnicas con distintas especialidades, cuya función es realizar la evaluación económica, técnica y diseño de las propuestas, para todos los servicios del mercado Corporaciones con excepción de los servicios de Ciberseguridad. Los especialistas de preventa trabajan en forma coordinada para la integración de estas soluciones. Los aspectos fundamentales para el desarrollo de su labor son los siguientes: **el conocimiento y la experiencia en las tecnologías**, implica una estrecha relación con los fabricantes e integradores. **La relación con el cliente,** permite capturar los requerimientos para la propuesta de diseño del servicio; actualmente en ambos aspectos, existe un vínculo transaccional, sólo enfocado en el mejor producto.

- **Proyecto:** Equipo a cargo de la implementación de los servicios móviles, fijos, TI y Ciberseguridad, de acuerdo a los alcances, costos y plazos definidos en la preventa. Se dividen en Jefes de proyecto (a cargo de liderar y coordinar la implementación con el cliente) y especialistas técnicos (que

ejecutan el diseño del proyecto). Los especialistas técnicos buscarán el apoyo de Integradores en los casos que requieran complementar conocimientos y experiencia en tecnologías específicas que estén fuera de alcance. Esta unidad mantiene una **relación directa con los clientes** finales, durante la implementación hasta la puesta en marcha de los servicios; con el objetivo de asegurar que la implementación cumpla con las expectativas de los clientes, existiendo un vínculo relacional entre ambos.

- **Unidad de Servicios Gestionados:** Equipo especialista multidisciplinario responsable de la continuidad operacional de los servicios implementados, resguardando el cumplimiento de los indicadores de continuidad establecidos en los contratos con los clientes. El alcance de sus responsabilidades es sólo para el portafolio móvil, fijo, TI (se excluyen servicios de Ciberseguridad). Realizan tareas de mantención preventiva, resolución de incidentes y ejecución de trabajos programados a solicitud de clientes. Esta unidad tiene un rol relevante en la satisfacción y retención de clientes, por tanto en los niveles de ingreso del mercado corporaciones. La relación de esta unidad con los clientes es transaccional. Por otra parte, los aspectos asociados a la administración del contrato, están a cargo de la unidad Gestión de Clientes. Actualmente existen indicadores de desempeño operacional de los servicios y estudios de satisfacción de los clientes.

  Para los clientes que cuentan con alguno de los otros servicios anteriores y Ciberseguridad, se mencionó anteriormente que existen dos unidades responsables de la continuidad de los servicios; lo que dificulta oportunidades de integración de los distintos portafolios de servicios, y como resultado no se concreta la posibilidad de captura de nuevos ingresos. El vínculo entre ambas unidades es transaccional, sólo para asegurar la continuidad de los servicios.

- **Unidad de Servicios de Ciberseguridad:** Está compuesta por dos áreas: comercial y operacional (Centro de Ciber inteligencia).

  - **Área Comercial:** Se enfoca en la comercialización del portafolio, la evaluación económica/técnica y el diseño de las propuestas (preventa). Además se encargan de la administración de los contratos de los servicios (gestión de clientes). Cuentan con las capacidades técnicas adecuadas para vender estos servicios. Actúan como el canal principal de venta y dada su especialización, como complemento para los otros canales del mercado Corporaciones. Existe un vínculo relacional con los clientes, buscado establecer soluciones integrales de Ciberseguridad.

    Para el desarrollo de soluciones integradas, ambos equipos de preventa trabajan en forma coordinada. Al igual que en el equipo preventa Corporaciones, **el conocimiento y la experiencia en las tecnologías**, implica una estrecha relación con los fabricantes e integradores. **La**

relación con el cliente, permite capturar los requerimientos para la propuesta de diseño del servicio; actualmente en ambos aspectos, existe un vínculo relacional, lo que genera una menor distancia con el cliente.

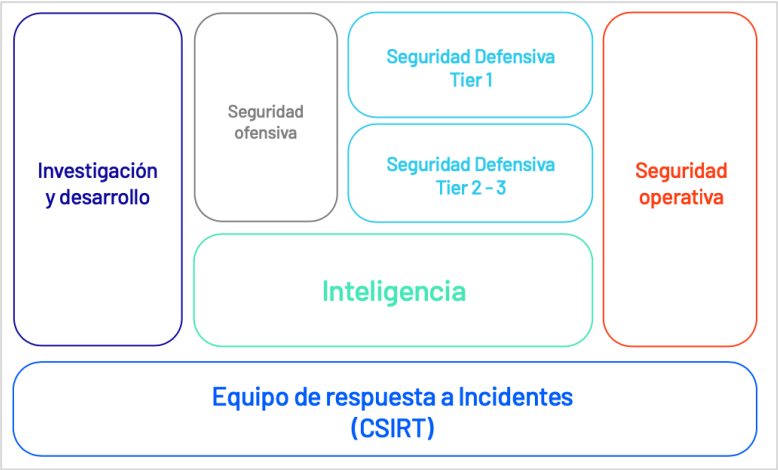
A pesar de que existe un vínculo relacional con el cliente, el portafolio de servicios de Ciberseguridad ofrece soluciones transversales a todos los segmentos, y no de acuerdo a las particularidades de cada industria.

La administración de contratos y la post venta, para clientes que tengan sólo Servicios Ciberseguridad, es de responsabilidad de esta unidad. En el caso de clientes que tengan más de un servicio, ambas funciones son realizadas por la unidad Gestión de Clientes de Corporaciones. Por esta razón, la oportunidad de capturar nuevos negocios en la cartera de clientes actual es menor.

- **Área Operacional - Centro de Ciber Inteligencia CCI:** Está compuesto por un equipo especialista y certificado en múltiples tecnologías de seguridad, a cargo de la protección, defensa y Ciber Inteligencia de las plataformas e infraestructuras de los clientes.

  Las funciones del CCI, se mencionan en la figura 16. El detalle de estas se encuentra disponible en el sitio de web de ENTEL S.A. en la siguiente dirección: https://www.entel.cl/corporaciones/ciberseguridad/.

Figura 16 – Funciones Centro de Ciber inteligencia



Fuente: VP Corporaciones ENTEL S.A. 2018

El desarrollo de sus funciones se enmarca en el cumplimiento normativo ISO 27001, NIST y FIRST. La certificación en estas últimas dos normas, es un elemento diferenciador en la industria de la Ciberseguridad. En la

actualidad ENTEL S.A. no cuenta con estas certificaciones. Complementario a lo anterior, existen certificaciones individuales de tecnologías de seguridad tales como: Fortinet, Tenable, Palo Alto, Trend Micro, Checkpoint, Cisco, entre otras.

El portafolio de servicios se beneficia con los acuerdos de colaboración con los principales Laboratorios y Centros de Investigación Desarrollo, de Fabricantes y universidades. A la fecha, existen acuerdos de colaboración con La Universidad Federico Santa María, Universidad de Chile y Fortinet.

Esta unidad opera en una infraestructura muy bien ubicada, con altos estándares de Seguridad física, conectividad de datos, electricidad e infraestructura redundante.

Actualmente esta unidad se vincula con los clientes de manera relacional, lo que permite cubrir los principales controles críticos de la seguridad de las empresas. La medición de desempeño operacional de los servicios, es una práctica instaurada recientemente, lo mismo ocurre con los estudios de satisfacción de clientes.

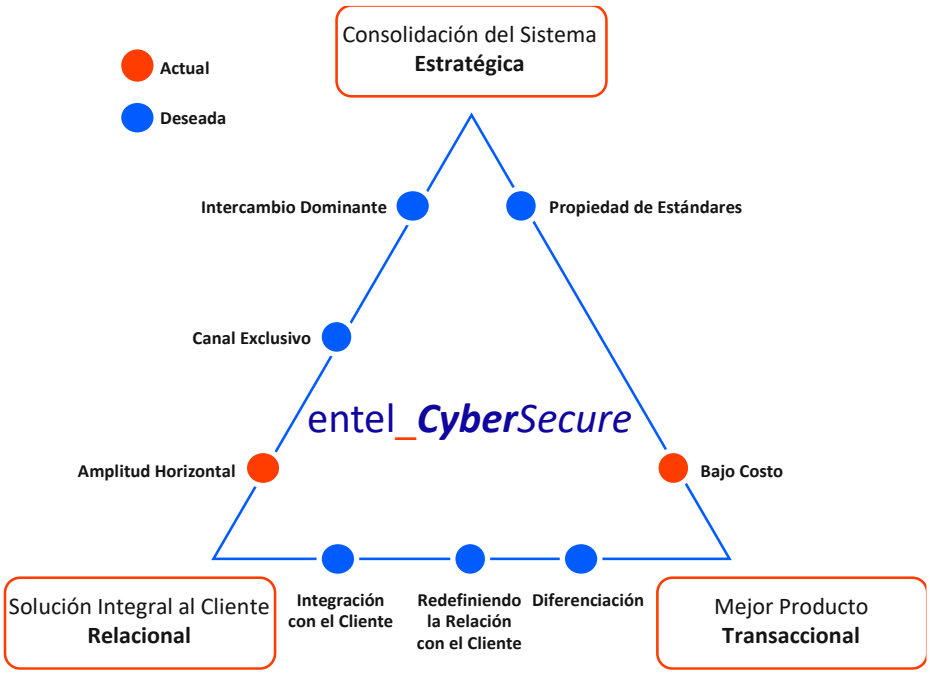
Como se mencionó anteriormente, existen dos unidades responsables de la continuidad de los servicios en el mercado Corporaciones, con un vínculo transaccional entre ellas; la integración de los distintos portafolios de servicios es compleja, y por tanto, la captura de nuevos ingresos es menor.

Al inicio de este capítulo, se indica que los servicios de Ciberseguridad representan una oportunidad con alto potencial de crecimiento para ENTEL S.A. Esta unidad juega un papel fundamental en que esto se concrete, atrayendo nuevos clientes a este y otros servicios, mejorando la satisfacción y retención de los actuales clientes del mercado Corporaciones.

7.1.4.5 Competencias Actuales y Deseadas

En este capítulo se describen las relaciones de vinculación entre los principales actores de la cadena de valor y la estructura organizacional que da soporte a estas relaciones. A partir de esta información, se detallarán las competencias actuales y deseadas del servicio de CiberSeguridad, que darán sustento a las líneas de acción propuestas en la estrategia. Estas competencias serán clasificadas según el Modelo Delta, en la figura 16.

Figura 16 – Competencias actuales y deseadas del Servicio de CiberSeguridad



Fuente: Elaboración Propia

Mejor Producto.

- **Bajo costo – Competencia actual**, el portafolio de servicios de Ciberseguridad ofrece una solución transversal a cualquier segmento. Aunque se trate de un servicio adaptable, no recoge por completo las particularidades del negocio de cada industria. Por otra parte, se dispone de una infraestructura eficiente y costos operacionales adecuados que permiten tener un margen operacional superior al de la compañía.

- **Diferenciación – Competencia deseada**. La amplia oferta de servicios del mercado corporaciones, proporciona al portafolio de Ciberseguridad la posibilidad de robustecer los servicios que esta ofrece. Este elemento diferenciador no es del todo suficiente para capturar mayor mercado. Debe

desarrollarse una solución verticalizada por industria, que en conjunto con lo anterior, aumente la disposición a pagar de los clientes.

Solución Integral al cliente.

- **Redefiniendo la relación con el cliente – Competencia Deseada.** El mercado Corporaciones declara en su estrategia, lograr una relación basada en la generación de valor con sus clientes. Este concepto está presente en los otros servicios, pero aún no está instaurado en los servicios de Ciberseguridad.

- **Integración con el cliente – Competencia Deseada.** La relación actual con los clientes del servicio de Ciberseguridad si bien es relacional, aun no logra transferir capacidades y conocimientos, que aporten valor al negocio de los clientes.

- **Amplitud horizontal – Competencia Actual.** ENTEL S.A ofrece un espectro completo de productos y servicios, brindado la posibilidad a sus clientes, de recurrir a un proveedor único para satisfacer sus necesidades. Esta amplia oferta, se complementa con los servicios de Ciberseguridad

Consolidación del Sistema.

- **Canal Exclusivo – Competencia Deseada**. Al inicio de este trabajo, se mencionó lo competitivo del mercado de Ciberseguidad en Chile. Además del acceso a la misma tecnología por parte de la competencia. Estos factores hacen muy difícil ser un canal exclusivo. Para lograr esta competencia, es necesario adquirir las competencias deseadas indicadas en el punto solución integral al cliente.

- **Intercambio dominante – Competencia Deseada.** El ecosistema en el que se sitúa ENTEL S.A. entrega condiciones favorables para que la compañía sea la principal interfaz entre partners e integradores. Esta condición le permitirá obtener una posición mayoritaria en el mercado de Ciberseguridad en Chile.

- **Propiedad de Estándares – Competencia Deseada.** Para alcanzar esta competencia, es necesario robustecer los acuerdos de colaboración con los principales Centros de Ciberinteligencia, Fabricantes y Universidades, con el objetivo de desarrollar competencias diferenciadoras y ampliar la oferta del portafolio de Ciberseguridad.

7.1.4.6 Resultados Financieros Actuales

El portafolio de Servicios Cybersecure, con la cadena de valor y la estructura organizacional mencionada en este capítulo, genera los siguientes resultados financieros:

Tabla 5 - Estado de resultados 2018, Servicios de Ciberseguridad

EERR 21018	MM$
Ingresos CiberSeguridad	$6.219
Costo Directos	39%
Costos Administración	9%
Costos Comerciales	15%
Costos Operacionales	4%
EBITDA	33%

Fuente: VP Corporaciones ENTEL S.A. 2018

Los ingresos del servicio de Ciberseguridad, en cifras del año 2018, representan el 0,32% de los ingresos totales de la compañía y el 2,8% de los ingresos del segmento Corporaciones. Estas cifras pueden considerarse bajas, por tratarse de un negocio emergente con alto potencial de crecimiento. Esta unidad de negocios genera un margen operacional superior al consolidado de la compañía (22,2% el año 2018).

Los resultados mencionados anteriormente, se utilizarán como base para las proyecciones de resultado de las líneas de acción, que son parte de la estrategia propuesta en este trabajo.

8 Estrategia de Negocio para el Servicio de Ciberseguridad

Con el análisis del mercado de Ciberseguridad y sus particularidades en Chile, además del diagnóstico de la propuesta de valor de este servicio en ENTEL S.A., se formulan las líneas de acción propuestas en la estrategia. La estrategia se enmarca en los focos estratégicos del mercado Corporaciones; tiene por objetivo incrementar los ingresos y su participación de mercado en Chile, y mejorar la rentabilidad del Servicio de Ciberseguridad.

8.1 Propuesta de Líneas de acción

De acuerdo a los objetivos de la estrategia, las líneas de acción se agruparán en dos ámbitos: Mejorar la productividad comercial y Transformación Operacional.

I. **Mejorar la productividad comercial**. Aprovechar las oportunidades que brinda el mercado en Chile, para incrementar la facturación, mediante la atracción de nuevos clientes y a través de clientes actuales del mercado Corporaciones y Empresas.

   a. **Mayor número de clientes:** Establecer incentivos comerciales, focalizados en ampliar el número de clientes del servicio Ciberseguridad, sobre la base de clientes actuales de los mercados Corporaciones y Empresas de ENTEL S.A.

   b. **Integrar oferta de Servicios:** Generar capacidades en todos los canales comerciales (Corporaciones y Empresas), que permitan incorporar el portafolio Ciberseguridad como complemento a las otras líneas de negocios (Servicios móviles y fijos, TI y negocios digitales).

   c. **Verticalizar oferta por Industria:** Desarrollar servicios de Ciberseguridad que se adapten a las particularidades de cada industria, priorizando los segmentos con mayor demanda (Gobierno, Industria y Comercio, Mercado Financiero).

   d. **Vinculación estrecha con el cliente:** Entrenamiento en modelo de relacionamiento y comercialización, basado en la vinculación estrecha con el cliente; con el objetivo de transformar y aumentar el valor de sus negocios.

   e. **Posicionamiento:** Desarrollar un plan de marketing (Entel Talks, Summit, publicaciones en la prensa, jornadas con gremios, entre otros), que permita posicionar a ENTEL S.A. como referente y experto en servicios avanzados y de asesorías de Ciberseguridad en Chile.

   f. **Experiencia de servicio distintiva:** Desarrollar estudios de satisfacción de clientes e implementar medidas que permitan mejorar la entrega de los servicios.

II. **Transformación Operacional.** Aprovechar los recursos, competencias y capacidades actuales, en conjunto con el desarrollo de capacidades deseadas, para mejorar la rentabilidad del Servicio de Ciberseguridad.

   a. **Sinergia Organizacional:** Integrar equipos comerciales y operacionales en torno a objetivos comunes, para aumentar las oportunidades de vinculación con el cliente y por tanto capturar nuevos negocios; además de fortalecer

la colaboración entre equipos, la transferencia de conocimientos y por último optimizar los costos actuales.

b. **Capital Humano:** Desarrollo de competencias y habilidades para todos los integrantes del servicio. Perfeccionar los mecanismos de medición de desempeño actuales. Implementar políticas para atraer, desarrollar y retener talentos.

c. **Procesos eficientes:** Redefinir procesos claves del servicio (en toda la cadena de valor) y sus indicadores de desempeño, maximizando la productividad y disminuyendo tiempos de reproceso, a través del uso de automatización para agilizar y simplificar a operación.

d. **Alianzas Estratégicas:** Ampliar y consolidar las alianzas estratégicas y acuerdos con partners de seguridad, con fines comerciales y certificaciones de calidad. Fortalecer la relación con distribuidores, para asegurar la disponibilidad de productos sin generar costos adicionales.

e. **Ecosistema:** Desarrollar una red de colaboración con Partners e Integradores, con el fin de compartir conocimientos y experiencia en tecnologías específicas, para ampliar la oferta de integración de servicios y responder con mayor agilidad a las necesidades de los clientes, además de lograr una posición mayoritaria en el mercado de Ciberseguridad.

f. **Calidad:** Certificar según normas ISO 27001, NIST y FIRST al Centro de Ciber Inteligencia (CCI), para garantizar las capacidades existentes. En complemento aumentar la cantidad de profesionales con certificaciones en tecnologías de seguridad. Ambas acciones permiten validar las competencias y habilidades que cuenta el CCI, siendo un diferenciador del servicio.

g. **Investigación y Desarrollo:** Aumentar la firma de acuerdos de colaboración con los principales Centros de Ciberinteligencia, Fabricantes y Universidades, para contar con competencias diferenciadoras.

h. **Infraestructura:** Ampliación de espacio y acondicionamiento de las instalaciones. Robustecer los estándares de Seguridad actuales.

8.2 Resultados esperados

El primer objetivo de la estrategia es incrementar los ingresos y su participación de mercado en Chile. El conjunto de líneas de acción asociadas a mejorar la productividad comercial y la transformación operacional, permitirán obtener los siguientes resultados:

Tabla 6 – Participación de mercado e Ingresos

	Año Base	Año 1	Año 2	Año 3	Año 4	Año 5	
Participación de Mercado	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**	**Tendencia**
Tamaño Mercado Ciber Chile Proyectado M$	**$ 83.000**	**$ 84.262**	**$ 85.524**	**$ 86.786**	**$ 88.048**	**$ 89.308**	
% Participación de Mercado Ciber Entel	7,49%	9,70%	12,56%	15,47%	18,60%	21,37%	
Ingresos Anuales Ciber Entel M$	**$ 6,219**	**$ 8,175**	**$ 10,738**	**$ 13,422**	**$ 16,375**	**$ 19,089**	
Variación Anual Ingresos Ciber Entel		31%	31%	25%	22%	17%	

Fuente: Elaboración propia

De acuerdo a las cifras de crecimiento de mercado Chileno (CAGR 7,6%), entregadas por IDC Chile, se estima que el tamaño de mercado al 2023 será de MM$ 89.308. Según las proyecciones de ingresos de la Vicepresidencia Corporaciones, que incluyen los criterios de crecimiento de mercado, se espera que la participación de mercado de los servicios de Ciberseguridad alcance un 21,37% al año 2023.

Como se indicó anteriormente, el año 2018 es la base para proyectar los costos operacionales. Las proyecciones de los años siguientes, recogen los resultados de las líneas de acción propuestas. El detalle de ingresos y costos proyectados al 2023, se muestra en tabla 7.

Tabla 7 – Costos operacionales y EBITDA

	Año Base	Año 1	Año 2	Año 3	Año 4	Año 5	
Estado de Resultado	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**	**Tendencia**
Ingresos M$	**$ 6.219**	**$ 8.175**	**$ 10.738**	**$ 13.422**	**$ 16.375**	**$ 19.089**	
Costo Directos	-39%	-35%	-35%	-33%	-31%	-30%	
Costos Fijos	-24%	-19%	-19%	-17%	-15%	-14%	
Costos Variables	-16%	-16%	-16%	-16%	-16%	-16%	
Costos Administración	-9%	-8%	-8%	-8%	-8%	-8%	
Costos Comerciales	-15%	-18%	-18%	-17%	-17%	-17%	
Costos Fijos	-4%	-4%	-4%	-3%	-3%	-3%	
Costos Variables	-10%	-14%	-14%	-14%	-14%	-14%	
Costos Indirectos	-4%	-4%	-3%	-3%	-3%	-2%	
Costos Operacionales M$	**67%**	**65%**	**64%**	**61%**	**58%**	**57%**	
EBITDA	**33%**	**35%**	**36%**	**39%**	**42%**	**43%**	

Fuente: Elaboración propia

A continuación, se detallan los principales impactos en costos de acuerdo a las líneas de acción formuladas en la estrategia:

Costos Directos:

Los costos directos presentarán disminuciones y aumentos, que en su conjunto generarán una disminución del 9% al año 2023, por efecto de las siguientes acciones:

a) Costos fijos: Disminución por la integración de los equipos operacionales, de acuerdo a la línea de acción **Sinergia organizacional**, este efecto es más visible el primer y quinto año. También aportará en esta disminución la línea de acción **Procesos Eficientes**, maximizando la productividad. Aumento por recursos destinados a la certificación de los procesos del Centro de Ciber Inteligencia (CCI) y de sus profesionales, en la línea de acción **Calidad**; este efecto es mayor los dos primeros años.

b) Costos variables, la estrategia no genera eficiencia en los costos variables, por lo cual la proporción se mantiene al 2023. El aumento en ingresos permite contar con mayores recursos que financien las siguientes iniciativas: 1. El ampliar y consolidar acuerdos con proveedores clave, asociado a la línea de acción **Alianzas Estratégicas**, permitirá disminuir o al menos mantener los costos actuales. 2. La línea de acción **Investigación y Desarrollo**, demandará recursos para cumplir sus objetivos. 3. **Ecosistema**, al igual que en el caso anterior, el desarrollo de una red de colaboración con empresas complementarias, inicialmente demanda mayores recursos que tendrán resultados positivos en los años futuros. 4. El desarrollo de soluciones particulares, según la línea de acción **Verticalizar oferta por industria**, tiene un costo importante los dos primeros años, pero va en directo beneficios de los ingresos.

Costos de Administración:

En esta categoría se incluye los recursos de la línea de acción **Capital Humano**, con el desarrollo de competencias y habilidades de los equipos, además de política para atraer, potenciar y retener talentos. Aunque la proporción de gastos disminuye un 1% el primer año, se mantiene fija hasta al 2023. El aumento sostenido en ingresos, permite año a año mayor cantidad de recursos disponibles para realizar las acciones propuestas.

Costos Comerciales:

Los costos comerciales presentarán disminuciones y aumentos, que en su conjunto generarán un alza del 3% los dos primeros años, se ajustarán en un 17% de los ingresos al 2023. Lo anterior, es efecto de las siguientes acciones:

a) Costos fijos: Disminución por la integración de los equipos comerciales, de acuerdo a la línea de acción **Sinergia organizacional**, este efecto es más visible el tercer año. Aumento por recursos destinados a la línea de acción **Integrar**

Oferta de servicios, para entrenamiento de equipos comerciales. Aumento por línea de acción **Experiencia de servicio distintiva,** para el desarrollo e implementación de estudios de satisfacción. Ambos efectos son más visibles los dos primeros años.

b) Costos variables, aumento por modificaciones en el plan de incentivos comerciales, propuesto en la línea de acción **Mayor número de clientes.** Aumento por recursos destinados al desarrollo del plan de marketing indicado en la línea de acción **Posicionamiento.** Aumento por recursos para entrenamiento en modelo de relacionamiento y comercialización, propuesto en la línea de acción **Vinculación estrecha con el cliente.** Estos tres efectos se evidencian a partir del primer año de implementación de la estrategia.

Costos Indirectos:

Este ítem será afectado por la Línea de acción de **Infraestructura**, asociada a la ampliación de espacios y acondicionamiento de las instalaciones. La proporción de gastos disminuye al 2023, sin embargo, el aumento en ingresos permite recursos disponibles para realizar las acciones propuestas. Por otra parte, la mayor cantidad de recursos de esta línea de acción, corresponde a activos de la compañía y son parte del plan de inversiones anual (Capex) y no de los costos operacionales (Estado de resultado).

Con todo lo expuesto anteriormente, el Ebitda del servicio de Ciberseguridad, aumenta en un 27,98 al 2023, alcanzando un 43% en este periodo.

9 Conclusiones y Recomendaciones

Los objetivos de la estrategia propuesta son incrementar los ingresos y participación de mercado en Chile, además de mejorar la rentabilidad del Servicio de Ciberseguridad. En el desarrollo de este trabajo, se logra concluir que estos objetivos son alcanzables.

En relación al incremento de ingresos, se evidencian elementos de contexto que sustentan un escenario favorable a la estrategia propuesta, estos elementos se traducen en la oportunidad de crecimiento del mercado global de la CiberSeguridad (cagr 11% al 2021) y el crecimiento proyectado de la industria de CiberSeguridad en Chile (cagr 7,6% al 2023). Dentro de este entorno positivo, la estrategia desarrolla capacidades y potencia las actuales, para atraer nuevos clientes a ENTEL S.A y aumentar la baja participación del servicio de ciberseguridad en el mercado Corporaciones (sólo 13 clientes de 586 conglomerados). Estos dos aspectos permiten concluir que el aumento en ingresos anuales del Servicio de Ciberseguridad es una posibilidad alcanzable, y por tanto, aumentar la participación de mercado en Chile, de un 7,5% a un 21,4% al 2023, es factible de conseguir.

El diagnóstico de la propuesta de valor actual del Servicio de Ciberseguridad, demostró que la mayoría de las capacidades existentes, se sitúan de acuerdo al modelo delta, en el lugar de posicionamiento estratégico de mejor producto, y dadas las características de este mercado (oferta transversal de tecnologías, alta rotación de talentos y bajas barreras de entrada), es necesario cambiar la posición estratégica hacia una solución integral al cliente y consolidación del sistema. Las líneas de acción propuestas en la estrategia, dan respuesta a esta necesidad. La estrategia pone foco en mejorar productividad comercial y transformar la operación actual. El conseguir la nueva posición estratégica permitirá obtener resultados favorables para ENTEL S.A., disminución de los costos operacionales del servicio, de un 67% a un 57% en 5 años y el aumento del Ebitda 33% al 43% en este mismo periodo.

La mayor parte de las líneas de acción se centran en cambios en la cultura de la organización, instaurando una nueva forma de operar y de relacionarse con los clientes. Estos cambios se generan de forma progresiva y requieren permear en toda la organización, para lo cual es necesario poner foco en el apoyo de los líderes y proveer herramientas de gestión del cambio.

Los resultados de ENTEL S.A en Chile han disminuido en los últimos dos años, la compañía se ve enfrentada al desafío de mejorar sus márgenes operacionales, disminuir el nivel de endeudamiento y rentabilizar sus inversiones. La estrategia propuesta en este trabajo apoya la mejora en los márgenes operacionales, y por tanto, aporta valor a los accionistas de la compañía.

10 Bibliografía

(1) ENTEL S.A. Corporaciones https://www.entel.cl/corporaciones/ciberseguridad/
(2) Memoria Corporativa Entel 2018
(3) Lecciones en Estrategia, Hacia una gestión de excelencia - Profesor: Arnoldo Hax, Ph.D. - Profesor: Nicolás Majluf, Ph.D.
(4) Administración estratégica, Competitividad y globalización. Conceptos y casos 7a. edición Michael A. Hitt, R. Duane Ireland, Robert E. Hoskisson
(5) Gartner - Magic Quadrant for Managed Security Services, Worldwide 2018
(6) Cybersecurity Trends 2017 Spotlight Report
(7) Ciberseguridad Avances y Nuevos Retos Diario Financiero Chile – 2018
(8) El mercado de la Ciberseguridad en Chile - Diciembre 2017 - Estudio de Mercado España Exportaciones e Inversiones
(9) Capitulo 4, Amenazas y desafíos para la seguridad nacional - Estrategia de Seguridad Nacional 2017 España
(10) Tendencias en Ciberseguridad: DDos en Latinoamérica (LATAM) - IDC InfoBrief 2017
(11) Política Nacional de Ciberseguridad - Gobierno de Chile 2017
(12) Ciberseguridad en Chile: Mirada Público-Privada - Ministerio del Interior y Seguridad Pública 2018
(13) Tendencias en el mercado de la Ciberseguridad, Instituto Nacional de Ciberseguridad España 2016
(14) McAfee Labs Threats Reports 2015
(15) Informe de riesgos mundiales 2019 14.ª edición