



**PLAN DE EMPRESA PARA BEEF UP TECH: SOLUCIONES PARA EL
SECTOR DE LA CIBERSEGURIDAD**

JONATHAN ANDRÉS GUERRERO ROSERO

**UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ D.C
2023**

**PLAN DE EMPRESA PARA BEEF UP TECH: SOLUCIONES PARA EL
SECTOR DE LA CIBERSEGURIDAD**

Presentado por:

JONATHAN ANDRÉS GUERRERO ROSERO

CÓDIGO: 2249693

**TESIS PARA OBTENER EL TÍTULO DE INGENIERO DE
TELECOMUNICACIONES**

Dirigido por:

ING. FERNANDO PRIETO BUSTAMANTE

**UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ D.C**

2023

PAGINÁ DE ACEPTACIÓN

NOTA DE ACEPTACIÓN

INGENIERO FERNANDO PRIETO BUSTAMANTE
Tutor Trabajo de Grado

Jurado Interno

Jurado Externo

Bogotá D.C. 01 de noviembre del 2023

A mis queridos padres, Jose Guerrero y Alba Rosero y mi Tía Inés Guerrero. Su apoyo incondicional ha sido la fuerza que me impulsó en cada paso de este camino académico. Cada sacrificio que han hecho y cada aliento que me han brindado han sido pilares fundamentales en la construcción de este logro.

Resumen

El propósito principal de este plan empresarial es abordar los desafíos presentes en el sector de la ciberseguridad, ya que este ha experimentado una serie de impactos negativos. A medida que se exploran los distintos capítulos, se destaca la importancia de establecer la protección en entornos digitales. Más aún, se ha desarrollado una solución concreta que no solo es factible de implementar, sino que también muestra un significativo potencial de crecimiento a lo largo del tiempo.

Para la implementación de esta solución **se requiere un presupuesto de \$140,000,000 COP**. Este capital se destinará a cubrir los gastos del primer año, y posiblemente una porción del segundo año. Un aspecto significativo del estudio se centra en la realización de una encuesta a una muestra representativa de personas interesadas en el ámbito de la ingeniería de telecomunicaciones y carreras afines. Los resultados reflejan una reacción positiva por parte de los encuestados, estas respuestas fortalecen la viabilidad del plan empresarial, ya que las impresiones iniciales sugieren que existe un ambiente ideal para su implementación.

Palabras clave: Lean Startup, Ciberseguridad, Ransomware, Phishing, Plan Empresa.

Abstract

The main purpose of this business plan is to address the challenges present in the cybersecurity sector, as it has experienced a number of negative impacts. As the various chapters are explored, the importance of establishing protection in digital environments is highlighted. Moreover, a concrete solution has been developed that is not only feasible to implement, but also shows significant potential for growth over time.

A budget of \$140,000,000 COP is required for the implementation of this solution. This capital will be used to cover the first year's expenses, and possibly a portion of the second year. A significant aspect of the study focuses on conducting a survey of a representative sample of people interested in the field of telecommunications engineering and related careers. The results reflect a positive reaction from the respondents; these responses strengthen the viability of the business plan, as initial impressions suggest that an ideal environment exists for its implementation.

Keywords: Lean Startup, Cybersecurity, Ransomware, Phishing, Business Plan.

Contenido

	Pág.
Resumen	V
Lista de Ilustraciones	XII
Lista de Tablas	XIV
Capítulo 1 Introducción del Proyecto	15
1. Introducción	16
1.1 Problema.....	16
1.2 Justificación.....	17
1.3 Objetivos	18
1.3.1 Objetivo General	18
1.3.2 Objetivos Específicos	18
1.4 Diagnóstico del Sector	19
Capítulo 2 Estudio de Mercado	21
2. Estudio de Mercado	22
2.1 Descripción del Sector	22
2.2 Situación del Mercado.....	23
2.2.1 Situación a Nivel Mundial	23
2.2.2 Situación en Colombia.....	30
2.2.2.1 Situación en Instituciones de Gobierno	32
2.3 Tendencias del Sector.....	34
2.3.1 Ransomware y Phishing en Evolución.....	34
2.3.2 Zero Trust.....	35
2.3.3 Ciberseguridad Impulsada por IA y Machine Learning.....	36

2.3.4	Ciberseguridad en la Nube	37
2.3.5	Ciberseguridad en IoT	38
2.4	Demanda	39
2.5	Competencia	40
2.5.1	IPSEC	40
2.5.2	Gtd Colombia	41
2.5.3	B-Secure	42
2.5.4	360 Security Group.....	43
2.5.5	Siguard.....	44
2.6	Análisis de la competencia	45
2.7	Análisis DOFA.....	47
Capítulo 3 Identidad Empresarial		49
3.	Identidad Empresarial	50
3.1	Mi Pensamiento Emprendedor	50
3.2	Nombre de la Compañía	50
3.3	Eslogan de la Compañía	50
3.4	Imagen de la Compañía	51
3.5	Pensamiento Corporativo	51
3.5.1	Misión.....	51
3.5.2	Visión	52
3.5.3	Valores	52
3.5.4	Objetivos	52
Capítulo 4 Metodología Lean Startup.....		53
4.	Metodología Lean Startup	54
4.1	Etapas Lean Startup.....	54
4.1.1	Validación de la Idea	54
4.1.2	Creación de un MVP	55
4.1.3	Medir el Impacto de MVP	55
4.1.4	Genera un Aprendizaje.....	55
4.1.5	Perseverar.....	56
4.2	Casos de Éxito	56
4.2.1	Dropbox.....	56

4.2.2 Slack	57
4.2.3 Zappos	57
4.3 Encuesta Exploratoria	58
4.3.1 Evaluación Del Sector: Resultados.....	58
4.3.1.1 Víctimas de estafas en línea	58
4.3.1.2 Términos clave en ciberseguridad.....	60
4.3.1.3 Interés en la ciberseguridad	61
4.4 MVP-1: Certified Cybersecurity Training.....	63
4.4.1 Beef Up Tech Certified Offensive Security Wireless	63
4.4.2 Beef Up Tech Certified Linux for Security Practitioners	64
4.4.3 Beef Up Tech Certified Ethical Hacker Analyst	64
4.4.4 Authorized Training Partner Certiprof	65
Capítulo 5 Constituyendo Una Empresa: Marco Legal y Organizacional.....	67
5. Marco Legal y Organizacional	68
5.1 Constitución Legal de Beef Up Tech	68
5.1.1 ¿Persona Jurídica o Natural?	68
5.1.2 Tipo de Sociedad	68
5.1.3 Homonimia	69
5.1.4 Actividad Económica (CIIU).....	70
5.1.5 Consulta Uso de Suelo.....	71
5.1.6 Trámites Ante Cámara y Comercio.....	72
5.2 Obligaciones fiscales.....	73
5.2.1 Impuesto al Valor Agregado (IVA)	73
5.2.2 Impuesto Sobre la Renta	73
5.2.3 Impuesto de Industria y Comercio (ICA)	74
5.2.4 Facturación electrónica	74
5.2.5 Otras Obligaciones	74
5.3 Estructura Organizacional	75
5.3.1 Accionistas	75
5.3.2 Junta Directiva.....	76
5.3.3 Lideres de Equipo.....	76
5.3.4 Equipos de Trabajo	76

Capítulo 6 Modelo Lean Canvas	77
6. Modelo Lean Canvas	78
6.1 Problema	78
6.2 Solución	79
6.3 Propuesta de Valor	79
6.4 Ventaja Injusta	80
6.5 Clientes	81
6.6 Canales	81
6.7 Métricas	82
6.8 Costos	83
6.8.1 Dominio y Hosting	84
6.8.2 Tercerización	84
6.8.2.1 Contabilidad y Facturación Electrónica	84
6.8.2.2 Credenciales Digitales	85
6.8.3 Estrategia de Marketing	86
6.8.4 Pasarela de pagos	86
6.8.5 Programas de Partners	87
6.8.6 Nomina	87
6.8.7 Costos Variables	88
6.9 Ingresos	89
6.9.1 Certificaciones	89
6.9.2 Programas de Partners	90
6.10 Factor de innovación	91
Capítulo 7 Estrategias Financieras	92
7. Estrategias Financieras	93
7.1 Variables Macroeconómicas	93
7.2 Estimación de Costos Operativos	94
7.3 Estimación de Costo Variables	95
7.4 Precios de Venta	96
7.5 Proyección de Ventas	97
7.6 Proyección de ingresos	98
7.7 Margen de contribución	99

7.8	Punto de Equilibrio	100
7.9	Estado de resultados.....	101
7.10	Estrategia de Financiamiento	102
7.11	Amortización de Crédito	102
Capítulo Final Conclusiones y Referencias.....		104
Conclusiones.....		105
Referencias.....		106

Lista de Ilustraciones

	Pág.
Ilustración 1: Proyección del mercado de ciberseguridad, 2021-2030.	23
Ilustración 2: Top 5 Ransomware LATAM 2022.....	24
Ilustración 3: Tamaño del mercado mundial de la ciberseguridad, 2021	25
Ilustración 4: Ciberataques por tipo, 2021	27
Ilustración 5: Costo promedio de un ciberataque por industria, 2021-2022.....	28
Ilustración 6: Costo promedio de un ciberataque por nivel de seguridad, 2020-2022 ...	29
Ilustración 7: Denuncias cibercrimen en Colombia 2022	31
Ilustración 8: Entorno Zero Trust	35
Ilustración 9: Logo IPSEC.....	41
Ilustración 10: Logo Gtd Colombia.....	42
Ilustración 11: Logo B-Secure.....	43
Ilustración 12: Logo 360 Security Group.....	44
Ilustración 13: Servicios SIGUARD.....	44
Ilustración 14: Logo SIGUARD	45
Ilustración 15: Como hacer un DOFA.....	47
Ilustración 16: Logo Beef Up Tech.....	51
Ilustración 17: Ciclo Lean Startup	54
Ilustración 18: Fraudes en Línea: ¿Ha sido víctima?	59
Ilustración 19: Fraudes en línea: ¿Conoce víctimas?	59
Ilustración 20: Percepción del “Phishing”	60
Ilustración 21: Percepción del “Ransomware”	60
Ilustración 22: Interés en la ciberseguridad	61
Ilustración 23: Percepción de la importancia de la ciberseguridad.....	61
Ilustración 24: Interés en la ciberseguridad	62
Ilustración 25: Certificaciones de interés.....	62
Ilustración 26: Certificación BCOSW	63

Ilustración 27: Certificación BCLSP	64
Ilustración 28: Certificación BCEHA	65
Ilustración 29: ATP CertiProf	66
Ilustración 30: Consulta homonimia	69
Ilustración 31: Organigrama	75
Ilustración 32: Modelo Lean Canvas.....	78
Ilustración 33: Beef Up Tech Certified Authorized Partner	90
Ilustración 34: Punto de equilibrio mensual	100

Lista de Tablas

	Pág.
Tabla 1: Comparación seguridad de la información e informática y ciberseguridad	20
Tabla 2: Costo aproximado de un ciberataque por país o región, 2021-2022	26
Tabla 3: Dominios gubernamentales comprometidos	33
Tabla 4: Algunas de las compañías de ciberseguridad	45
Tabla 5: Matriz DOFA	48
Tabla 6: Empresas competidoras con actividad económica	70
Tabla 7: Costos de legalización primera vez 2023	72
Tabla 8: Costo de un colaborador con SMLV 2023	88
Tabla 9: Proyección de variables macroeconómicas	93
Tabla 10: Proyección de costos operativos	94
Tabla 11: Proyección de costos variables	95
Tabla 12: Precios de venta por año	96
Tabla 13: Proyección de ventas en unidades	97
Tabla 14: Proyección de ingresos	98
Tabla 15: Margen de contribución	99
Tabla 16: Punto de equilibrio anual	101
Tabla 17: Estado de resultado por año	101
Tabla 18: Simulación de crédito	102

Capítulo 1 | Introducción del Proyecto

1. Introducción

Se ha evidenciado el cambio acelerado que ha generado la tecnología en la sociedad actual e igualmente el efecto post pandemia, donde las estadísticas indican, más robo de información, uso de la tecnología de forma insegura para el teletrabajo, y demás datos que indican que existe una brecha en el sector. Con el propósito de apoyar a la industria, se busca definir un plan de empresa, que permita brindar servicios B2B¹ y B2C² de Ciberseguridad, donde las soluciones y productos estén basados en ingeniería. *(Es importante tener en cuenta que la información proporcionada durante toda la investigación se basa en datos recopilados durante el período de 2020 al 2021.)*

1.1 Problema

El Covid-19 ha sido un protagonista importante en lo que se refiere a ciberseguridad, ya que esto permitió encontrar muchas vulnerabilidades importantes. Para ser más exactos hubo un **crecimiento del 605% en ataques** durante la llegada del Covid-19 [1], McAfee la empresa de ciberseguridad registró **tasa de 9 amenazas por segundo, esto tan solo en primer semestre del 2020**, los sectores afectados van desde servicios financieros hacia sectores como el de la educación, servicios públicos y demás [1].

La información sensible tiene un gran valor para la ciberdelincuencia, sobre todo la información empresarial. **En la Dark Web, se venden con frecuencia datos sensibles** como nombres y números de tarjetas de crédito, los cuales son utilizados para el fraude o el robo de identidad. Por lo cual no es nada extraño que las brechas de seguridad implican importantes pérdidas económicas para las compañías [2]. Además, un estudio realizado por la universidad del Rosario indica que el **60% de las PYMES cierran** luego de sufrir un ciberataque importante [3].

En Colombia según un informe de Fortinet en el año 2021 se registraron **11.200 millones de intentos de ciberataques** y para América latina más de 285.000 millones de intentos, **un incremento del 600% respecto al 2020**. Donde una de las puertas de entrada

¹ Business to Business (B2B): Negocio entre empresas

² Business to Consumer (B2C): De empresas a consumidores

es el trabajo remoto que ha registrado un aumento en el uso de escaneos para identificar brechas de seguridad, y seleccionar objetivos con mayor precisión [4].

Las brechas de seguridad son tan grandes que existe una organización dedicada exclusivamente a la búsqueda y la lucha contra estas en el software. OWASP³ es una organización sin ánimo de lucro la cual apoya este trabajo. Actualmente cuentan con un documento denominado, OWASP² Top 10 en el que da una concientización básica para desarrolladores y seguridad de las aplicaciones web [5].

“La ciberdelincuencia es la mayor amenaza para todas las empresas del mundo”.
Ginni Rometty, CEO de IBM en 2015 [3].

1.2 Justificación

Para justificar desarrollo del emprendimiento se observará desde una perspectiva de tendencias, datos e informes, que indican la alta demanda y crecimiento del sector de la ciberseguridad, donde el mercado habla y da a entender que existen oportunidades de negocio, y en donde **se puede brindar un apoyo constante hacia la industria**; por lo tanto, **las compañías deben capacitarse e implementar soluciones** que permitan desde el lado de la ciberseguridad dar continuidad con sus negocios.

Uno de los grandes cambios que han sufrido las empresas cuando venden y ofrecen sus productos es la digitalización, el uso de comercio electrónico tuvo un gran auge, especialmente durante la contingencia del COVID 19, en donde las organizaciones se vieron con la obligación de ofrecer sus productos por medio de internet y así sobreponerse a la problemática de no poder vender en sus tiendas físicas.

Con la digitalización de las compañías uno de los grandes problemas o desafíos que debe enfrentar la industria TIC es la seguridad, por ejemplo, solo en Colombia se estima que aproximadamente el **12,52% de los teléfonos celulares cuentan con algún tipo de malware** [6]. La ciudad que reporta el mayor número de ciberataques es Bogotá la cual cuenta con más de 8.000 casos, luego le sigue Medellín con más de 1.600 y Cali con más

³ Open Web Application Security Project.

1.500 [7]. Los principales ataques se centran en el phishing por medio de mensajes de texto y E-mail, para la realización de estafas o robo de información [7].

Los ciberataques más comunes de los que son víctimas las empresas colombianas son, en un 80% por medio de correos fraudulentos, en un 60% por suplantación de identidad, y en un 37% por infección por Ransomware⁴ [8]. El phishing sigue siendo el método más usado para cometer delitos, y la principal motivación es la económica, siendo sus principales víctimas las Pymes e identidades financieras [8]. En Colombia estos ataques generan un promedio de **pérdidas de entre 300 a 5.000 millones de pesos** [8].

El uso de datos sensibles por medios digitales hace indispensable que estos medios sean cada vez más seguros y confiables, y aunque **ningún sistema es 100% seguro** se debe garantizar la mayor seguridad posible, dado que vulnerar los derechos de protección de datos, puede acarrear en **millonarias multas**. Un plan de empresa que ofrezca tanto soluciones como capacitaciones en ciberseguridad es una respuesta esencial para abordar estos desafíos. **Concientizar a los empleados con las habilidades necesarias** para identificar amenazas cibernéticas es un factor clave en este proceso.

1.3 Objetivos

1.3.1 Objetivo General

Establecer un plan de empresa para la creación de una compañía que ofrezca servicios y soluciones en el sector de la ciberseguridad.

1.3.2 Objetivos Específicos

- Realizar estudios de mercado y factibilidad para determinar la viabilidad del proyecto entendiendo el comportamiento del sector.
- Definir identidad empresarial, imagen corporativa e identificar los productos o servicios que prestara la compañía
- Realizar los estudios financieros con proyección de ingresos a 5 años para determinar la viabilidad a corto, mediano y largo plazo.

⁴ Ransomware: Código malicioso, Secuestrador de datos

1.4 Diagnóstico del Sector

Actualmente en el mercado, y según ACIS⁵ existen un aproximado de 165 compañías que se dedican al sector de la ciberseguridad [9], estas empresas no alcanzan a cubrir la demanda del sector de la tecnología, en Colombia solo en la industria del software existen aproximadamente 29.000 empresas [10], y según el diario de La República **se estima un incremento del 115% en el uso de software en las empresas** [11]. **Ninguna de estas empresas puede garantizar que sus productos sean 100% seguros.**

Uber es una de las empresas de transporte más grandes del mundo, y en 2016 sufre un grave incidente de seguridad donde se encontró una vulnerabilidad en sus sistemas. Los ciberdelincuentes obtuvieron acceso a información personal de 57 millones de usuarios de la plataforma, incluyendo direcciones de correo electrónico, sus nombres y números de telefónicos. Uber ocultó el incidente y pagó a los ciberdelincuentes 100.000 dólares para que borrarán la información y se mantuvieran en silencio [12].

Debido a este incidente, Uber ha implementado medidas adicionales para fortalecer la seguridad de sus sistemas y ha adoptado un enfoque más transparente en el manejo de incidentes de seguridad. Aun así, en septiembre del 2022 **un ciberdelincuente de 18 años, llevó a cabo un ataque**, donde logró acceder a los estados financieros e información de los usuarios de la compañía. El ataque, según informes fue producido por una campaña de Phishing hacia uno de los colaboradores de la compañía [13].

Twitch es una de las compañías de streaming más importantes la industria del contenido audiovisual, y en octubre del 2021 un ciberdelincuente logró acceder de manera no autorizada a la plataforma de transmisión en vivo Twitch y obtuvieron información valiosa, como el código fuente de la plataforma, contraseñas encriptadas de usuarios y empleados, información de pagos a streamers conocidos, información sobre proyectos futuros y acceso a herramientas anti-hackers [14].

Grandes compañías de cualquier sector han sufrido importantes brechas de seguridad en sus plataformas donde se permite reconocer la necesidad que existe de

⁵ Asociación Colombiana de Ingenieros de Sistemas

ofrecer servicios relacionados al sector de la ciberseguridad donde las empresas buscan cada vez más herramientas tecnológicas con el fin de dar soluciones a sus problemáticas, abarcar un mayor número de clientes, ofrecer mejores y nuevos servicios, en general, implementar la digitalización en sus procesos.

Tabla 1: Comparación seguridad de la información e informática y ciberseguridad

<i>Característica</i>	<i>Seguridad informática</i>	<i>Ciberseguridad</i>	<i>Seguridad de la información</i>
<i>Ámbito de protección</i>	Dispositivos internos, privacidad e integridad de los datos.	Protege sistemas y dispositivos conectados a Internet, con prácticas ofensivas.	Toda la información almacenada y transmitida, con medidas preventivas.
<i>Amenazas</i>	Virus, malware, ataques a nivel de red, ataques físicos (como el robo de hardware).	Ataques cibernéticos (phishing, Vishing, etc.), amenazas informáticas (virus, malware), ataques (DoS), ataques de fuerza bruta.	Ataques cibernéticos, pérdida de datos, divulgación no autorizada de información confidencial
<i>Objetivo de protección</i>	Sistemas informáticos y datos almacenados	Sistemas, redes, dispositivos conectados a Internet, privacidad en línea, información almacenada en la nube	Toda la información almacenada y transmitida, incluyendo datos personales, financieros y comerciales

Fuente: Creación propia con base en datos de [15]

En la **Tabla 1**, se evidencia las diferencias entre la seguridad de la información e informática y la ciberseguridad ya que estas trabajan juntas para proteger la información y los sistemas. Por ejemplo, en seguridad de la información se realizan medidas preventivas para todo lo almacenado, la seguridad informática se encarga de la privacidad e integridad de los datos y la ciberseguridad abarca los dos campos mencionados que con prácticas ofensivas contribuye a un mejor ecosistema digital.

La ciberseguridad es un campo en constante evolución, y por lo cual es importante estar al tanto de las últimas tendencias y desarrollos. Algunas de las tendencias actuales incluyen la ciberseguridad en la nube, la inteligencia artificial aplicada a la ciberseguridad y la ciberseguridad en Internet de las cosas (IoT), y sobre todo estar actualizado de nuevas vulnerabilidades que podrían atacar al sector de la tecnología.

Capítulo 2 | Estudio de Mercado

2. Estudio de Mercado

El estudio de mercado es vital para evaluar la viabilidad del emprendimiento. Este proceso permite identificar clientes potenciales obteniendo información detallada sobre la industria de la ciberseguridad en Colombia, como el tamaño del mercado, la competencia, consumidores y tendencias. Con estos datos, se pueden determinar los servicios y soluciones que se debería prestar en la compañía. Esto facilitará la toma de decisiones acertadas y permitirá tener una visión clara de cómo avanzar en la industria de la ciberseguridad.

2.1 Descripción del Sector

El sector de la ciberseguridad se encarga de proteger los sistemas informáticos, las redes de comunicaciones y los documentos de las compañías de posibles ataques cibernéticos. Esto incluye la protección de datos sensibles, la prevención de violaciones de la privacidad y la protección contra cualquier tipo de amenazas cibernéticas que pongan en riesgo una compañía. Los profesionales de la ciberseguridad trabajan en una variedad de entornos, desde empresas privadas y gubernamentales hasta instituciones educativas. Su objetivo es garantizar que los sistemas informáticos y las redes de comunicaciones sean seguros y se mantengan protegidos contra posibles ataques [16].

Los profesionales de la ciberseguridad pueden trabajar en diferentes áreas, como la protección de la red, la normatividad de la seguridad de la información, la criptografía y el área forense. También pueden trabajar en la implementación y mantenimiento de medidas de seguridad, como los sistemas de detección de intrusiones y firewalls, así como en la gestión de incidentes de seguridad cibernética y en la formulación de procedimientos y políticas de seguridad. El sector de la ciberseguridad es indispensable para proteger y asegurar la información de posibles ataques, garantizando que los sistemas informáticos funcionen de manera segura y eficiente [17].

Para garantizar la ciberseguridad, es necesario investigar las necesidades de protección y los dispositivos que se utilizan a diario, instalar software de ciberseguridad y mantener sistemas operativos y sistemas de seguridad actualizados. Una red privada virtual (VPN) bien protegida puede ser suficiente para muchas personas, pero para aquellos que tienen una gran cantidad de datos importantes en múltiples dispositivos, puede ser necesario un sistema de seguridad más elaborado [18].

El sector de la ciberseguridad es cada vez más importante debido al aumento del cibercrimen y la dependencia hacia las nuevas tecnologías de la información. Los ataques cibernéticos pueden tener consecuencias graves para personas y empresas, incluyendo pérdida de datos, interrupción de operaciones y daños a la reputación. Las compañías que brindan servicios de ciberseguridad ofrecen soluciones para proteger contra estas amenazas, como software de protección y servicios de asesoramiento, etc.

2.2 Situación del Mercado

2.2.1 Situación a Nivel Mundial

Según Next Move Strategy Consulting empresa de consultoría y análisis de datos informa que el mercado de la ciberseguridad está **valorado para el 2022 en 289.320 millones de dólares** y se estima que incrementa a una tasa anual compuesta del 12,8% entre 2022 y 2030, **hasta llegar los 657.020 millones de dólares** para el 2030, como se muestra en la **Ilustración 1** [19], [20]. El crecimiento del mercado lo favorece factores como la evolución de las amenazas a la seguridad y el aumento de los ciberataques.

El modelo de trabajo desde casa también ha contribuido al crecimiento del mercado, ya que ha aumentado la necesidad de soluciones de seguridad para el trabajo híbrido. La adopción de un modelo de seguridad de confianza cero (Zero-Trust Security) para prevenir las violaciones de datos también se ha vuelto más frecuente. Se espera que el mercado de ciberseguridad continúe creciendo debido al aumento del uso de servicios en la nube, la adopción de la transformación digital y el crecimiento del Internet de las cosas. [19].

Ilustración 1: Proyección del mercado de ciberseguridad, 2021-2030.

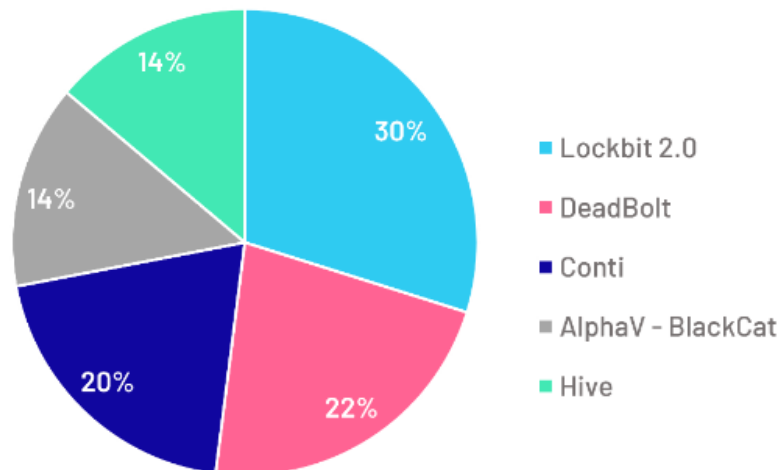


Fuente: Creación propia con base en datos de *Next Move Strategy Consulting* [19]

El cibercrimen está en crecimiento, y la industria de la seguridad cibernética está trabajando para proteger tanto a usuarios como a compañías. Según un informe de la Universidad de Maryland, **Estados Unidos sufre ataques cibernéticos cada 39 segundos** [21], además según Netdata Networks **cada día 30.000 sitios web son pirateados en el mundo** [22], y el **73% de las empresas han sufrido al menos un ciberataque** [23].

Uno de los malware⁶ más famosos es el Ransomware el cual cuenta con diferentes variantes como se observa en la **Ilustración 2**, y de acuerdo con Panda Security es el tercer método de ataque preferido [22]. Se ha vuelto tan famoso que los **ciberdelincuentes han creado un modelo de negocio denominado “Raas” Ransomware as a Service** [24], y donde algunas de las funciones ofrecidas por estos servicios incluyen la creación de malware y la posibilidad de unirse a un programa de afiliados para su distribución a cambio de un porcentaje de las ganancias [25].

Ilustración 2: Top 5 Ransomware LATAM 2022



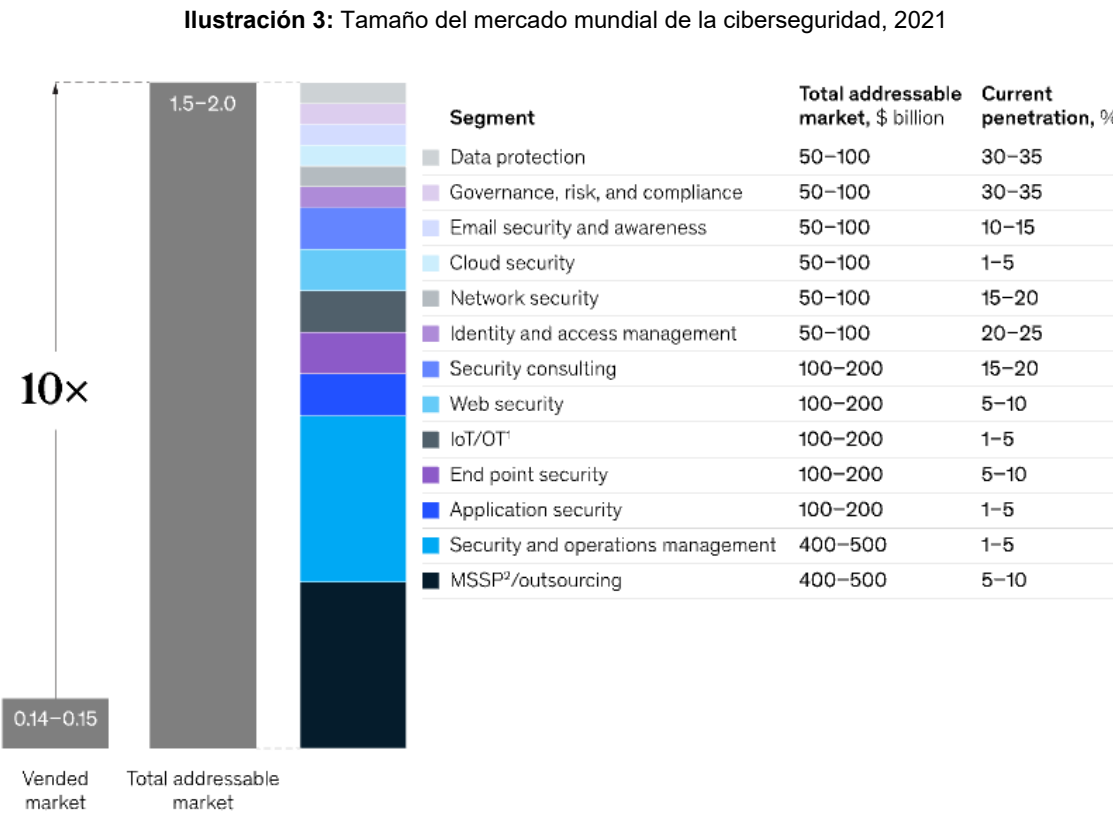
Fuente: CyberSecure [26]

Se espera que los **daños causados por estos tipos de ataques alcancen los 10.5 billones de dólares para el año 2025**, lo que se vería reflejado en un **aumento del 300%** en comparación con 2015. Para el 2021, las organizaciones **destinaron alrededor de 150**

⁶ Malware, Software malicioso.

mil millones de dólares para la ciberseguridad, lo refleja un crecimiento del 12,4% anual [27]. Actualmente, **las soluciones que brindan las empresas no satisfacen completamente las demandas del mercado** [27], los clientes buscan una amplia gama de servicios, como pruebas de intrusión, automatización, supervisión normativa, precios, servicios detección de amenazas entre otros [28].

Como se observa en la **Ilustración 3**, algunos de los segmentos de la ciberseguridad cuentan con menos del 5% en la penetración del mercado. **La industria ha ignorado sectores como el IoT**, lo que ha llevado a **un aumento del 123%** en los ataques hacia estos dispositivos en 2022 [29] y según McKinsey & Company, la brecha que existe actualmente en el mercado puede generar una **oportunidad de negocio que rondaría entre 1.5 a 2 billones de dólares** para los servicios de ciberseguridad [27], [28].



Fuente: *McKinsey & Company* [27]

Desde los inicios de Internet, la ciberseguridad ha sido un problema constante, donde los atacantes cada vez son más frecuentes y sofisticados. La pandemia conocida como COVID-19 ha agravado aún más esta tendencia, demostrando la capacidad de los

ciberdelincuentes para encontrar vulnerabilidades, como lo fue el **Zero Day Log4J**, que afectó a diversas compañías, como Microsoft, Google, Amazon e IBM, entre otras [30].

Según un estudio realizado por IBM a 550 compañías de 17 diferentes países e industrias, que se vieron afectas por algún tipo de ataque en el 2021, Estados Unidos por duodécimo año consecutivo sigue siendo el país con mayores costes promedio en un ciberataque, rondando la cifra de los 10 millones de dólares [31]. La región del medio Oriente sigue ocupando el segundo puesto con casi los 8 millones de dólares. Para la **Tabla 2** se observan los países y regiones que fueron analizados en el estudio.

Tabla 2: Costo aproximado de un ciberataque por país o región, 2021-2022

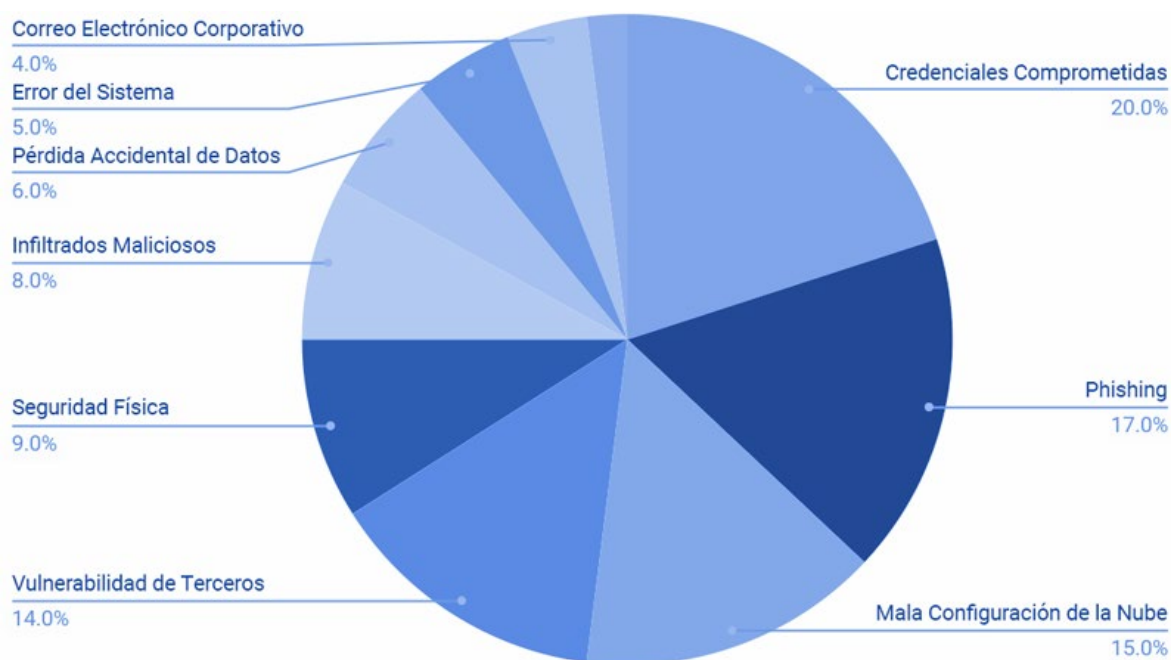
<i>N°</i>	<i>País</i>	<i>2021</i>	<i>2022</i>
1	USA	\$ 9.05	\$ 9.44
2	Medio Oriente	\$ 6.93	\$ 7.46
3	Canadá	\$ 5.40	\$ 5.64
4	Reino Unido	\$ 4.67	\$ 5.05
5	Alemania	\$ 4.89	\$ 4.85
6	Japón	\$ 4.69	\$ 4.57
7	Francia	\$ 4.57	\$ 4.34
8	Italia	\$ 3.61	\$ 3.74
9	Corea del Sur	\$ 3.68	\$ 3.57
10	Sudáfrica	\$ 3.21	\$ 3.36
11	Australia	\$ 2.82	\$ 2.92
12	Sudeste Asiático	\$ 2.71	\$ 2.87
13	Latinoamérica	\$ 2.56	\$ 2.80
14	India	\$ 2.21	\$ 2.32
15	Escandinavia	\$ 2.67	\$ 2.08
16	Brasil	\$ 1.08	\$ 1.38
17	Turquía	\$ 1.91	\$ 1.11

Fuente: Creación propia con base en datos de *IBM* [31]. Medido en millones de dólares

Para la **Ilustración 4**, según el informe de IBM el Phishing, las malas contraseñas y una mala configuración en la nube, son los vectores de ataque que más utilizan los Ciberdelincuentes como método de acceso, donde las credenciales comprometidas son el método más común para acceder a una red o sistema. Además, los ataques de phishing

son altamente efectivos debido a que los ciberdelincuentes utilizan tácticas de ingeniería social para atraer a los usuarios y conseguir que revele sus credenciales o realice acciones que les permitan acceder a sistemas o datos confidenciales [31].

Ilustración 4: Ciberataques por tipo, 2021



Fuente: IBM [31].

Una de las principales amenazas a nivel mundial es el Phishing⁷, ya está que sigue afectando a numerosa cantidad de usuarios en todo el mundo. Según un informe realizado por State of the Phish 2022, **el 80% de los ciberataques provenientes del Phishing⁶ terminan en éxito** [32], lo que demuestra la alta efectividad de los atacantes para aplicar técnicas de ingeniería social para atraer a los usuarios consiguiendo acceder a sus datos y sistemas.

Diferentes compañías trabajan para mitigar los ataques provenientes de la ingeniería social. Se estima **Google interviene en el 99,9% de los intentos de Phishing⁶ y boquea un promedio de 100 millones de correos** con algún tipo malware⁸ por día, todo con el fin de que estos no lleguen a los usuarios [33]. Es por esto por lo que es importante que

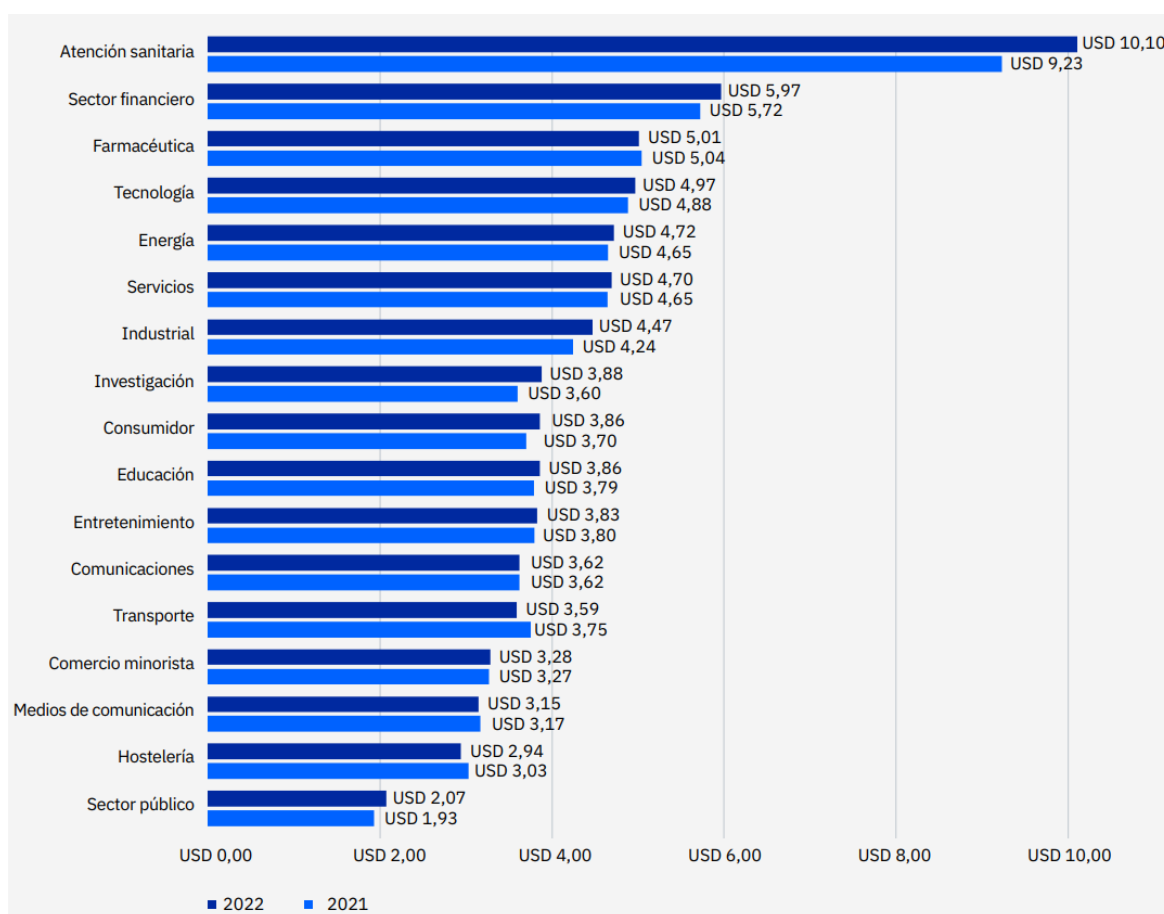
⁷ Phishing, ingeniería social aplicada para engañar a una persona, usualmente por E-mail.

⁸ Malware, Software malicioso.

los usuarios estén atentos y tomen medidas para protegerse contra estos ataques, como utilizar contraseñas seguras y estar alerta ante correos o mensajes sospechosos. Además se estima que el **97% de las personas el mundo no sabe identificar un ataque de Phishing** bien elaborado [34].

Para la **Ilustración 5** se observan las industrias más afectadas entre marzo de 2021 y marzo de 2022. En los informes de IBM, desde el año 2020, el sector de la atención sanitaria ha obtenido el primer lugar por doce años consecutivos en lo que se refiere a costos por filtración de datos, con un promedio de \$10,10 millones de dólares. **La salud es uno de los sectores más atractivos para los atacantes** junto con el sector financiero, que también sufre grandes pérdidas debido a la filtración de datos, con un costo promedio que ronda alrededor de los \$6 millones de dólares [31].

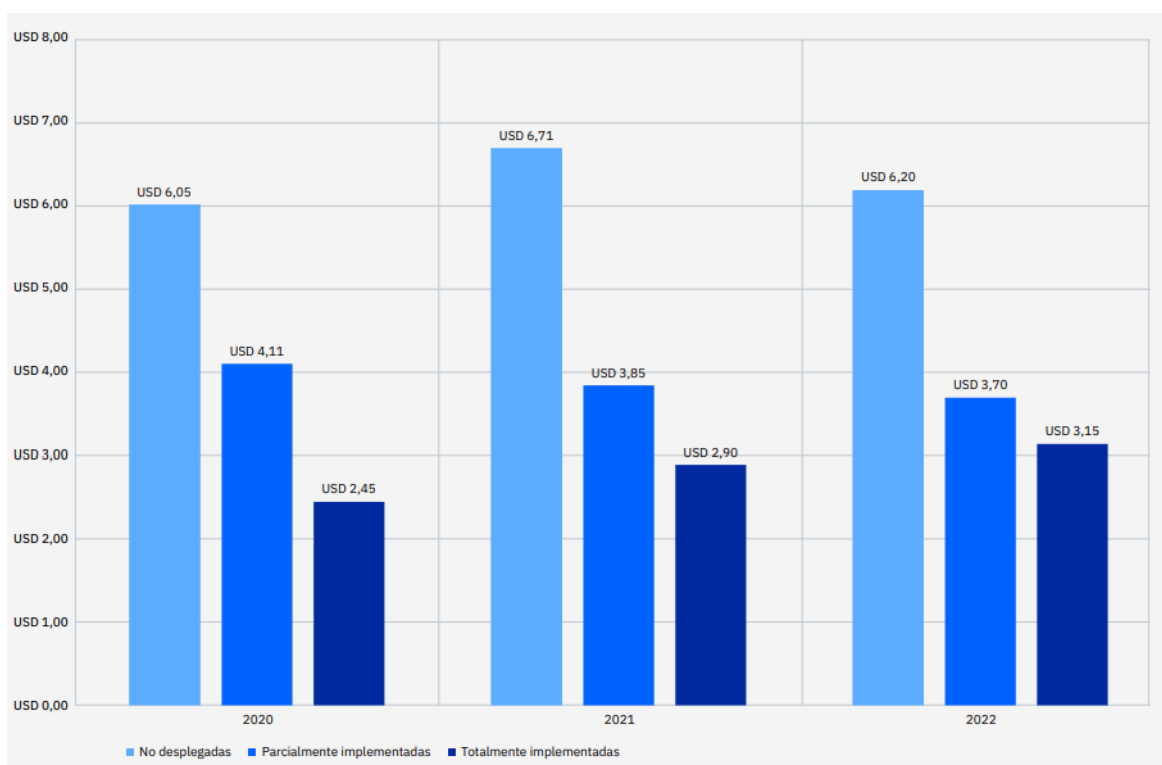
Ilustración 5: Costo promedio de un ciberataque por industria, 2021-2022



Fuente: IBM [31]. Medido en millones de dólares

En la **Ilustración 6** se observa como a medida que las empresas implementan técnicas de seguridad para mitigar los vectores de ataque, el costo disminuye frente a compañías que no realizan ningún tipo de acción frente a las amenazas cibernéticas. En promedio a las empresas que realizan algún tipo de técnica para reforzar su seguridad digital, les cuesta 3.05 millones de dólares menos contener una amenaza frente a una que no implementa ninguna acción, lo que indica un ahorro del 65,2% comparado con el costo más alto que es de 6,71 millones de dólares [31].

Ilustración 6: Costo promedio de un ciberataque por nivel de seguridad, 2020-2022



Fuente: IBM [31]. Medido en millones de dólares

En conclusión, es cada vez más importante que las compañías presten atención a la ciberseguridad debido al creciente número de ataques cibernéticos que se están produciendo. Estos ataques pueden tener consecuencias graves para las empresas, incluyendo la pérdida de datos confidenciales, la interrupción de servicios y la pérdida de los clientes. Según datos ya mencionados, se estima que el sector crezca significativamente en los siguientes años debido a la falta de soluciones y la constante evolución de las amenazas.

2.2.2 Situación en Colombia

Colombia es un país que ha experimentado crecimiento exponencial en la adopción de tecnologías digitales y el uso de Internet en los últimos años. En 2019, el 51,9% de los hogares en el país tenían acceso a Internet, y esa cifra aumentó a 56,5% en 2020 [35]. Como resultado, Según ICEX España, en América Latina uno de los países con la mayor tasa de adopción en el uso de Internet y transformación digital es Colombia. Sin embargo, a pesar de este progreso, **Colombia ocupa el segundo país en América Latina con un elevado número de incidentes de ciberseguridad**, reportando una cifra de **1,8 millones de ciberataques en el año 2021** [35].

Colombia ha obtenido una posición variable en diferentes rankings internacionales de ciberseguridad. Según el Global Cybersecurity Index 2020, Colombia ocupó el puesto 81º a nivel mundial y el 4º en América Latina, y según Comparitech el puesto 16º entre 75 países. Sin embargo, según el Cyber Threat Report 2021, **Colombia se encuentra entre los 10 países con mayores ataques por Ransomware⁸**, donde **ha crecido un 232%** desde 2019 hasta el 2022 y según McAfee es el cuarto país del mundo con mayores detecciones maliciosas [35] [36].

Para Colombia en el año 2021 entre enero y octubre se establecieron más de 42.000 denuncias y para el mismo periodo, pero en el año 2022 más 54.000 denuncias, lo cual indica un incremento del 20.5% respecto al año anterior además [36], según Fortinet Colombia registró **7 billones de intentos de ciberataques en el 2020** [37], y aunque las empresas se han esforzado por mejorar sus medidas de ciberseguridad, siguen produciéndose ataques como el robo de información y el secuestro de datos causados por Ransomware⁹ y ataques Zero Day [38].

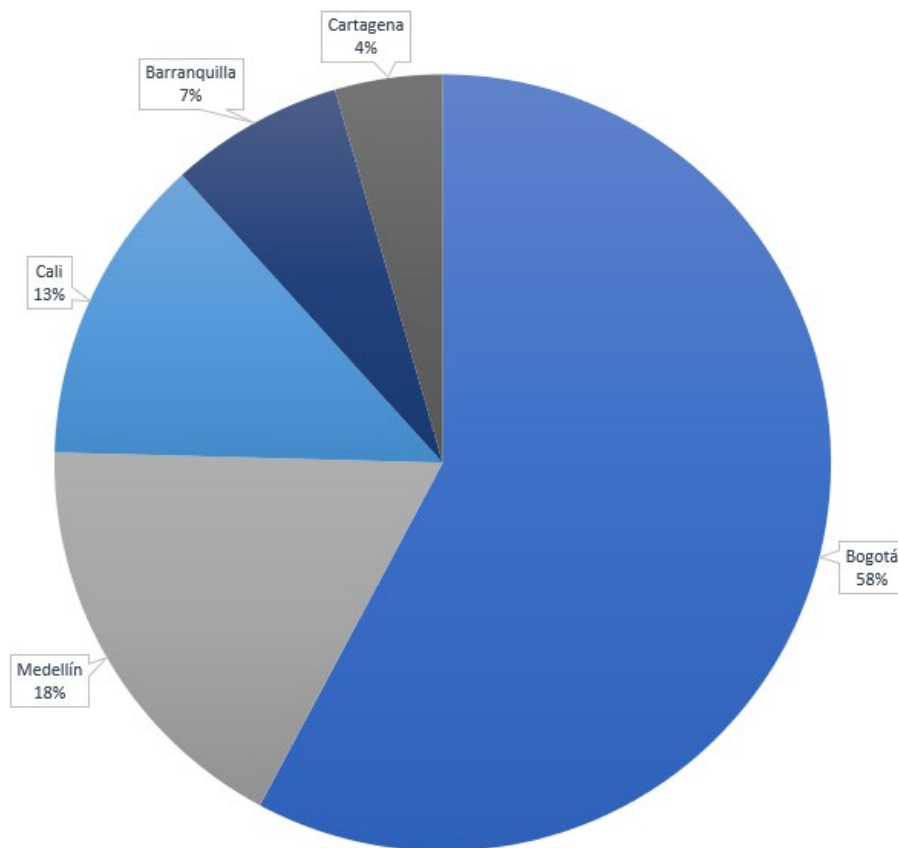
Además de las numerosas compañías de tecnología que sufren brechas de seguridad, en Colombia, para el mes de diciembre del 2022 se produjo un ataque cibernético a las empresas de salud Keralty, Sanitas y Colsanitas, que ha provocado largas filas y problemas en los procesos. Se estima que los **ciberdelincuentes poseen 700Gb de información**, y que esto habría sido un ataque de Ransomware⁸, es decir, un secuestro

⁹ Ransomware: Código malicioso, Secuestrador de datos.

de datos por parte de los atacantes, los cuales piden dinero a cambio de devolverla o no publicarla [39], [40].

Bogotá es una de las ciudades más grandes e importantes de Colombia, también una de las que más denuncias por cibercrimen presenta. Según el CCIT¹⁰ En el 2022 se realizaron **15.411 denuncias de cibercrimen en la ciudad**, lo que muestra la creciente preocupación por este tipo de delitos en la región. Medellín, otra de las grandes ciudades de Colombia, también tuvo un alto número de denuncias por cibercrimen, con 4.706 en el 2022. Cali, Barranquilla y Cartagena también experimentaron un alto número de denuncias, con 3.435, 1.933 y 1.197 denuncias, respectivamente [36]. El porcentaje de cibercrimen en dichas ciudades se puede observar en la **Ilustración 7**.

Ilustración 7: Denuncias cibercrimen en Colombia 2022



Fuente: Creación propia con base en datos del CCIT [36]

¹⁰ CCIT, Cámara Colombiana de Informática y Telecomunicaciones

En Colombia al igual que en el mundo, los sectores más perjudicados por el cibercrimen son el de gobierno, financiero, educación y salud, estos sectores se ven obligados a realizar inversiones en la seguridad digital, según un informe de Asobancaria el **presupuesto en el sector financiero creció más del 60 %** entre 2019 y 2020, una inversión de 70 millones de euros [35]. Además Datacrédito Experian, en 2021, reveló que **Colombia estuvo dentro del top 5 de cibercrimen y fraude**, donde las **perdidas superarán los 5.200 Millones de euros** [35].

El MinTIC¹¹ reporta que en comparación con años anteriores, la adopción del trabajo remoto se disparó cerca de 400% en el primer semestre de 2020. Lo que trajo como resultado que las empresas y las personas en Colombia están ahora más expuestas y susceptibles a los ciberataques. Según Global Data **el mercado de la ciberseguridad para Colombia se estableció en 3.200 millones de dólares en el 2021** [41], y según Mordor Intelligence espera que **en Colombia el mercado de la ciberseguridad crezca a un CAGR¹¹ del 9,54%** en el transcurso del periodo del 2022 al 2027 [42].

2.2.2.1 Situación en Instituciones de Gobierno

En Colombia, existen diversas iniciativas y organizaciones dedicadas a la ciberseguridad. Por ejemplo, una de las funciones del MinTIC¹² es promover la seguridad cibernética en el país y de coordinar la respuesta a los incidentes de seguridad cibernética [43]. Además, el Ministerio también cuenta con un equipo de respuesta ante emergencias informáticas CSIRT¹³, una unidad de seguridad cibernética que se encarga de proteger a las instituciones gubernamentales y a los ciudadanos de Colombia de los ataques cibernéticos [44].

El gobierno de Colombia en últimos años ha destinado una gran cantidad de recursos y esfuerzos a la protección de sus sistemas cibernéticos y a la prevención de ataques cibernéticos. Sin embargo, a pesar de estos esfuerzos, aún se han registrado compromisos en algunos de los dominios gubernamentales más importantes del país. En la **Tabla 3** se puede observar algunos de los dominios gubernamentales en Colombia que han sido

¹¹ CAGR, Tasa de crecimiento anual compuesto

¹² MinTIC, Ministerio de Tecnologías de la Información y las Comunicaciones

¹³ CSIRT, Computer Security Incident Response Team

comprometidos, entre los que se encuentran, Dirección de impuestos y Aduanas Nacionales (DIAN), el Instituto Colombiano para la Evaluación de la Educación (ICFES), el Servicio de Empleo, y Colpensiones, entre otros.

Tabla 3: Dominios gubernamentales comprometidos

Dominio	Credenciales Expuestas
muisca.dian.gov.co	3,318
simo.cnsc.gov.co	1,122
www2.icfesinteractivo.gov.co	933
personas.serviciodeempleo.gov.co	766
www.icetex.gov.co	555
evaluarparaavanzar311.icfes.gov.co	539
sede.colpensiones.gov.co	499
oficinavirtual.shd.gov.co	489
community.secop.gov.co	434
servidorpublico.sigep.gov.co	414
miseguridadsocial.gov.co	404
epagos.registraduria.gov.co	373
www.colpensiones.gov.co	359
jovenesenaccion.dps.gov.co	339
www.positivaenlinea.gov.co	307
web.sispro.gov.co	296
visibles.migracioncolombia.gov.co	273
www.fna.gov.co	265
snrbotondopago.gov.co	254
webazure.dian.gov.co	252
solicitudes.icetex.gov.co	213
www.medellin.gov.co	192
ecenso.dane.gov.co	182
www.funcionpublica.gov.co	176

Fuente: Creación propia con base en datos del CCIT [45]

No solamente dominios gubernamentales de Colombia fueron comprometidos, para febrero de 2022 se descubrió una **filtración de más de 12 millones de credenciales de usuario comprometidas de 49.880 sitios web gubernamentales de todo el mundo** [45]. Estos dominios han sufrido ataques cibernéticos o han sido expuestos a vulnerabilidades, lo que ha permitido a los atacantes cibernéticos obtener acceso a los sistemas y datos protegidos como las credenciales de los usuarios, esto significa que los inicios de sesión o contraseñas de acceso a estos dominios han sido revelados y pueden ser utilizados por los atacantes para acceder a los sistemas y datos.

2.3 Tendencias del Sector

El sector de la tecnología se encuentra en una evolución constante, lo que significa que los ciberdelincuentes aprovecharán las nuevas tecnologías que aún no cuentan con una protección adecuada. Esto hace que sea importante estar siempre atentos a las últimas tendencias del sector, por lo cual tanto empresas como usuarios deben tomar medidas para protegerse contra ataques cibernéticos, ya que estos ciberdelincuentes también se encuentran en constante búsqueda de vulnerabilidades.

2.3.1 Ransomware y Phishing en Evolución

El Ransomware y el Phishing ha dejado un rastro de daños multimillonarios a lo largo de del tiempo, puesto que los ciberdelincuentes se han beneficiado económicamente de estos ataques [46]. Sin embargo, el Ransomware y Phishing han evolucionado y sigue haciéndolo, según un informe del gobierno de Estados Unidos, **cada día se producen más de 4,000 ataques de Ransomware** [47]. Si bien es difícil determinar el costo total de estos ataques, se estima que los **daños totales por Ransomware superarían los 20,000 millones de dólares esto tan solo en 2021** [47].

Un factor que ha contribuido a la propagación del Ransomware es un servicio conocido como Raas "Ransomware as a Service" [48], el cual funciona como un modelo de negocio para el atacante, además de ser barato y fácil de obtener para cualquier ciberdelincuente. El Ransomware suele implementarse a través de campañas de Phishing, las cuales engañan a los usuarios para que descarguen el malware. También se han visto campañas de **Ransomware dirigido** [49], que atacan a empresas o usuarios específicos con el objetivo de beneficiarse económicamente [50].

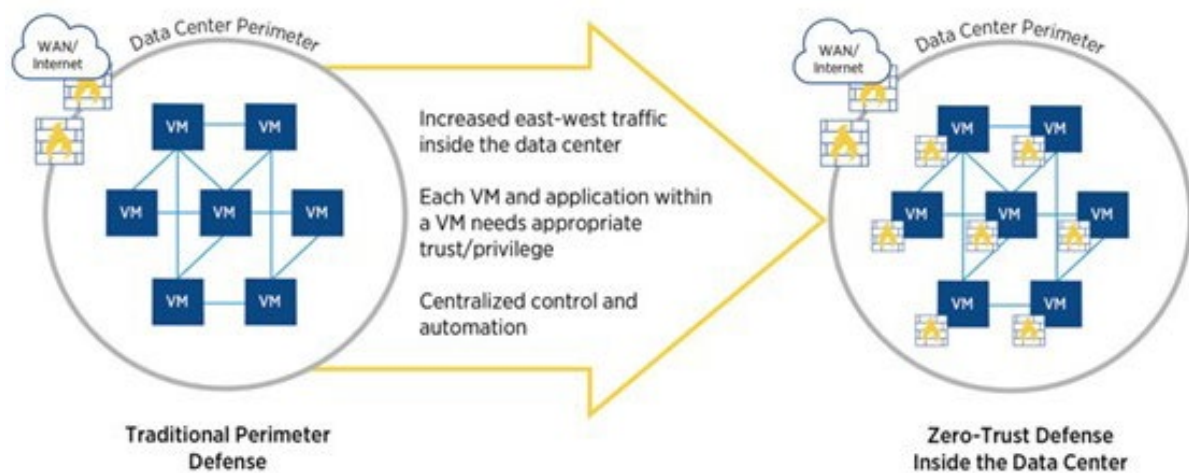
En 2022, el Ransomware fue la principal amenaza a la seguridad cibernética, y para el 2023 se espera que esta tendencia persista [51]. Las empresas seguirán luchando contra el Phishing y el Ransomware, pero es probable que veamos ataques de Ransomware y Phishing que evolucionen más allá de las capacidades de una empresa para protegerse. Por ejemplo, en Escocia, un ataque de **Ransomware comprometió más de 70,000 dispositivos médicos** [52], este dato es crítico e impórtate para que las empresas tomen medidas para protegerse y estén preparadas para hacer frente a esta amenaza en constante evolución [53].

2.3.2 Zero Trust

El modelo de seguridad Zero Trust es una estrategia que se está convirtiendo rápidamente en una norma en muchas organizaciones. Se basa en una estrategia en la cual no se puede confiar en nadie por defecto y que todas las solicitudes de acceso a la red deben ser verificadas y autorizadas antes de ser concedidas. Esto se aplica tanto a empleados como a dispositivos que se conectan a la red [48], [46].

En la **Ilustración 8** se puede observar dos entornos, donde la imagen izquierda hay una confianza generalizada en todos los equipos y usuarios donde se permiten todas las conexiones. Esto significa que, si un atacante consigue acceder a un recurso, puede tener acceso a todos los demás recursos de la organización. Por otro lado, en el entorno de la imagen derecha, hay una falta de confianza donde solo se permiten las conexiones necesarias. Esto significa que, si un atacante consigue acceder a un recurso, sería difícil acceder a los demás recursos, debido a las restricciones de acceso y comunicación [54].

Ilustración 8: Entorno Zero Trust



Fuente: Netronome [55]

Según Gartner, empresa consultora y de investigación tecnológica, **se espera que 6 de cada 10 empresas adopten la metodología Zero Trust para 2025** [56]. Esto se debe en parte al hecho de que la arquitectura de confianza cero está ganando importancia como medio para validar el acceso y mejorar la seguridad. Se espera que los equipos de seguridad aceleren sus planes de **adopción de Zero Trust en 2023** [53], aunque es probable que cometan algunos errores en el proceso.

El mercado de seguridad de confianza cero también está experimentando un crecimiento sostenido. Se espera que el modelo de seguridad **Zero Trust obtenga un CAGR¹⁴ del 18% durante el período del 2021 al 2026** [57]. Esto se debe en parte al hecho de **aproximadamente el 80% de las empresas optan implementar el modelo Zero Trust** como alternativa a las VPN¹⁵ [58], debido a sus beneficios en términos de seguridad y simplicidad de gestión.

En resumen, Zero Trust es una estrategia de seguridad que está ganando terreno rápidamente y que ofrece muchos beneficios a las empresas. Las organizaciones con un enfoque **Zero Trust implementado ahorraron casi \$1 millón de dólares en costos** en comparación con las organizaciones sin Zero Trust implementado [59]. Lumu Technologies estima la seguridad enfocada en **Zero Trust crezca cerca de los \$79 millones de dólares para el 2027** [60]. A medida que más organizaciones adopten esta tecnología, es más probable que se vuelva una tendencia en el mundo empresarial.

2.3.3 Ciberseguridad Impulsada por IA y Machine Learning

En la batalla contra la ciberdelincuencia, la inteligencia artificial (IA) tiene un gran potencial ya que a través del uso del Machine Learning (Aprendizaje Automático), **la IA puede analizar grandes cantidades de datos y detectar patrones de comportamiento sospechosos** que pueden resultar en actividad cibernética malintencionada. Esto puede ser especialmente útil para identificar ataques cibernéticos que podrían pasar desapercibidos para un ser humano [46] [56].

El uso de estas tecnologías para soluciones de ciberseguridad ha incrementado en los últimos años. Esta tecnología está ganando popularidad en la ciberseguridad alrededor del mundo debido a que estos sistemas utilizan algoritmos de aprendizaje automático para examinar de manera más efectiva datos que circulan en tiempo real a través de las redes de internet [49] [53].

Según IBM, **las empresas que utilizan IA y automatización para detectar comportamientos sospechosos ahorran un promedio de 3 millones de dólares en**

¹⁴ CAGR, Tasa de crecimiento anual compuesto

¹⁵ VPN, Virtual Private Network

comparación con aquellas que no lo hacen [61]. Se espera que para 2030, el mercado de **productos de ciberseguridad que implementen la Inteligencia Artificial (IA) valdrá cerca de \$139.000 millones de dólares**, esto significa un aumento de casi diez veces al valor del mercado en 2021 [61], esto muestra la importancia cada vez mayor de la IA en la ciberseguridad donde puede ser de gran ayuda para afrontar la transformación digital de manera segura y con garantías [62].

2.3.4 Ciberseguridad en la Nube

En la actualidad, las empresas le dan gran importancia a la seguridad en la nube, ya que cada vez es más frecuente el almacenamiento y procesamiento de datos importantes en servidores externos. **La adopción de la nube por parte de las organizaciones es cada vez mayor**, por lo cual es fundamental desarrollar soluciones de ciberseguridad adecuadas para proteger estos datos [56].

La pandemia conocida como COVID-19 ha cambiado significativamente la situación en que los seres humanos se comunican e interactúan, donde una de las consecuencias más notables ha sido el aumento del trabajo remoto, esta nueva forma de trabajo ha aumentado la necesidad de servicios e infraestructura basada en la nube, lo que significa un incremento en los riesgos para ciberseguridad. Sin embargo, muchos de los servicios en la nube no cuentan con medidas de seguridad suficientes, como encriptación y autenticación segura, lo que los hace vulnerables a los ataques [50].

Uno de los problemas más costosos en términos de ciberseguridad es la que se basa en la nube, por lo general esto ocurre por una **mala e incorrecta configuración de estos servicios**. Según un informe de CheckPoint, el 68% de las empresas considera que esta mala configuración es una de las principales causas. Además, se estima que el 20% de las violaciones de datos de las organizaciones son causadas por trabajadores remotos que utilizan plataformas basadas en la nube de la empresa [47].

Para proteger los datos y evitar brechas de seguridad, es crucial que las empresas apliquen medidas de seguridad adecuadas. Esto abarca la configuración adecuada de los servicios en la nube y la **formación en ciberseguridad a los empleados**. Aunque los servicios basados en la nube ofrecen muchas ventajas, es fundamental asegurarse de que se utilizan de manera segura para proteger los datos de la empresa.

2.3.5 Ciberseguridad en IoT

Internet of Things es una tecnología en rápido desarrollo la cual ofrece numerosas ventajas y comodidades, pero también crea nuevos riesgos de ciberseguridad. Según la empresa Gartner, estima que **un dispositivo IoT puede verse comprometido en tan solo 3 minutos por un ciberdelincuente**, pero pueden pasar hasta 6 meses hasta que se identifique el fallo de seguridad [48]. Esto plantea nuevos riesgos y obstáculos, que pueden ser especialmente problemáticos para las empresas que emplean IoT en sus operaciones diarias.

Se espera que para **2026 existan 64 mil millones de dispositivos IoT instalados alrededor del mundo** [50]. Con tantos dispositivos conectados, los problemas de seguridad podrían ser mucho más graves de lo que todo el mundo piensa. Desgraciadamente, no existe una norma general de seguridad del IoT, por lo que cada proveedor de dispositivos debe gestionar la seguridad de forma diferente. Según un artículo de **Kaspersky afirma que el 27% de los fabricantes IoT no tiene una política de seguridad** para los socios y proveedores que participan en este tipo de proyectos [63], como resultado, algunos dispositivos IoT podrían no ser tan seguros como deberían.

Para dar un ejemplo importancia de proteger los dispositivos IoT, en marzo de 2019, Medtronic una empresa de Estados Unidos la cual distribuye dispositivos médicos, saltó a los titulares al revelar **un fallo de seguridad en varios de sus dispositivos implantados en sus pacientes**. En particular, uno de sus dispositivos cardíacos recibió una evaluación de vulnerabilidad de 9,3/10 puntos, lo que los hace extremadamente vulnerables [64]. Según dos estudios de Network World, **solo el 7% de las empresas y fabricantes tienen un plan de IoT bien definido**, y más del 50% de las empresas están preocupadas por los riesgos de seguridad con sus propios dispositivos [47].

Los dispositivos IoT pueden ser utilizados por los ciberdelincuentes para crear una botnet. Esta red de dispositivos comprometidos es usualmente empleada para lanzar ataques conocidos como DDoS (denegación de servicio distribuido), donde uno de los malwares más reconocidos por la industria es **Mirai el cual se ha utilizado para capturar dispositivos IoT y llevar a cabo importantes ataques DDoS** [65]. La seguridad de la red puede verse comprometida por errores cometidos durante el despliegue de dispositivos IoT dentro de una red empresarial [66].

2.4 Demanda

La ciberseguridad es un campo en constante evolución, **en Colombia para el 2020 en particular se registró un aumento del 40%** en la demanda de servicios de ciberseguridad [67]. Se espera que persista esta tendencia en el futuro, y que la demanda de profesionales en ciberseguridad doble a la oferta. Además, **Microsoft estima que América Latina requerirá 10 millones de expertos en ciberseguridad para el 2024**, lo que indica que el mercado crece constantemente [68].

EALDE Business School estima que la industria de **la ciberseguridad es uno de los sectores que más contrata en la actualidad, marcando un 0% de desempleo desde 2011** y una tasa de contratación del 90% [68]. Una encuesta a algunas compañías reveló que el **55% de las empresas aumentarán sus inversiones en ciberseguridad en el futuro**, mientras que el 72% esperan reducir costes mediante el fortalecimiento de la ciberseguridad [69].

Encontrar profesionales con el perfil adecuado para el sector de la ciberseguridad puede ser un desafío, este campo sigue estando en constante crecimiento debido a que las empresas necesitan proteger los datos de sus usuarios contra posibles filtraciones. La mayoría de las empresas simplemente no pueden permitirse una filtración de datos, por lo que la ciberseguridad se ha vuelto fundamental para garantizar la seguridad de los sistemas y la confidencialidad de la información [70].

En Colombia existen alrededor de **165 compañías que se dedican al sector de la ciberseguridad** [9], tanto nacionales como internacionales, que ofrecen servicios de ciberseguridad para proteger a empresas y a los usuarios, sin embargo, estos servicios suelen estar dirigidos principalmente a grandes compañías, dejando a las **medianas y pequeñas empresas (Pymes) en una posición vulnerable** [71].

Las Pymes colombianas son fundamentales en la economía del país, ya que abarcan el 90% de las compañías y emplean a más del 65% de la población [72]. A pesar de su importancia, estas empresas por lo general no cuentan con los recursos y la capacidad necesaria para protegerse adecuadamente de los ciberataques [73]. Aunque existen empresas de ciberseguridad en el país, **no logran cubrir la demanda de las más de 5 millones de empresas existentes** [74].

Países como España son conscientes de esta problemática, y en el año 2021 abrió programa para emprendedores que quieran crear empresa en temas relacionados a la ciberseguridad, en el cual destinaron 191 millones de euros [75]. Para este año 2023, el Instituto Nacional de Ciberseguridad de España conocido como INCIBE¹⁶, está impulsando nuevamente este tipo de **emprendimientos de ciberseguridad con una inversión de 30 millones de euros** [76]. Estas iniciativas tienen como objetivo fomentar el desarrollo de nuevas empresas de ciberseguridad, satisfaciendo la creciente demanda del sector con el fin de proteger así a las Pymes y a otras empresas del país.

2.5 Competencia

El mercado de ciberseguridad es un sector en constante cambio y evolución. Para poder determinar el estado actual del mercado es importante y esencial analizar a algunos de los principales competidores del sector. Al hacerlo, podremos conocer los productos y servicios que ofrecen, sus propuestas de valor y su experiencia y tiempo en el mercado. Al tener una comprensión completa de estos factores, podremos tener una mejor visión de como esta industria está evolucionando y cómo se posicionan las empresas en el mismo.

2.5.1 IPSEC

Esta empresa, fundada en Colombia en 2005, cuenta con una gran trayectoria en el mercado de ciberseguridad, con más de 18 años de presencia en el sector. La empresa se enfoca en brindar servicios integrales de ciberseguridad y tecnología de la información para compañías de todos los sectores y tamaños. Ofrecen una amplia gama de servicios, desde consultorías de tecnología, implementación de soluciones de seguridad, administración y soporte [77]. Entre los servicios de ciberseguridad que ofrece la empresa se encuentran los siguientes:

- ❖ Análisis de Vulnerabilidad y Hacking Ético.
- ❖ Protección de aplicaciones Web & DDoS.
- ❖ Prevención Avanzada de Amenazas.
- ❖ Protección de Correo Electrónico.

¹⁶ INCIBE, Instituto Nacional de Ciberseguridad de España

- ❖ Seguridad como Servicio (SECaaS).
- ❖ Teletrabajo y acceso remoto seguro.
- ❖ Protección contra Phishing.

IPSEC cuenta también con servicios TI, pero para este caso solamente se tuvieron en cuenta los servicios que prestan en la parte de ciberseguridad, de los servicios mencionados en su sitio web no se realiza una descripción de lo que ofrecen por lo cual no queda muy claro que es lo que realizan en realidad.

Ilustración 9: Logo IPSEC



Fuente: IPSEC [77]

2.5.2 Gtd Colombia

Gtd Colombia es una empresa de servicios de telecomunicaciones, la cual cuenta más de 41 años en el mercado, con presencia en países como Perú, Chile, Ecuador y España, además realizan alianzas corporativas en las cuales incorporan empresas de distintos países los cuales cuentan con trayectoria, como lo fue Telefónica del Sur una empresa con 124 años de historia. Esta empresa puede ser un gran competidor en el mercado por su amplia trayectoria [78].

Al ser una empresa de servicios de telecomunicaciones cuenta con gran variedad de servicios y cobertura, entre los servicios que ofrecen se encuentran, servicios de transformación digital, continuidad del negocio, servicios TI, Blockchain, Big Data, IoT, inteligencia artificial, consultoría, servicios de data center y ciberseguridad [78]. Para los servicios de ciberseguridad cuenta con la siguiente oferta:

- ❖ **Protección EDR:** Este servicio lo describen como una inteligencia artificial que previene y mitiga amenazas avanzadas.
- ❖ **Co-Relación de eventos:** Este servicio lo describen como un análisis y correlación de logs.

- ❖ **Firewall como servicio:** Este servicio lo basan en monitoreo de la red, administración de seguridad y aplicación de políticas.
- ❖ **Centro de operaciones de seguridad (SOC):** Este servicio lo enfocan al monitoreo de los sistemas TI, especialmente para la detección, análisis y repuestas ante incidentes de ciber seguridad.

Ilustración 10: Logo Gtd Colombia



Fuente: *Gtd Colombia* [78]

2.5.3 B-Secure

Esta empresa se dedica únicamente a ofrecer servicios de ciberseguridad fue fundada en 1998, cuenta con más de 22 años de trayectoria en el sector y según su perfil en LinkedIn tiene más de 105 colaboradores lo que significa que ya está bien consolidada en el mercado, además de contratar colaboradores desde su página web, cuentan con certificaciones reconocidas por el sector como lo son CMMI-SVC nivel 3, ISO 9001 e ISO 27001 [79]. B-Secure al ser una empresa que se dedica únicamente a los servicios de ciberseguridad su oferta de servicios es amplia, en su página web se encuentran los siguientes servicios:

- ❖ Gestión de Vulnerabilidades
- ❖ Ethical Hacking (Pentest)
- ❖ Análisis de código y controles de seguridad
- ❖ Servicios de visibilidad
- ❖ Monitoreo de Ciberseguridad y Marca
- ❖ Amenazas Avanzadas
- ❖ Servicios de respuesta
- ❖ Gestión de Infraestructura de seguridad

- ❖ Optimización de controles de seguridad
- ❖ Ciberseguridad adaptativa
- ❖ Seguridad Cloud
- Gobierno, Riesgo y cumplimiento

Los servicios mencionados simplemente son los más representativos de su página web, acabe resaltar que cuenta con mucha más variedad de soluciones, productos y servicios, por la cual es un competidor bastante fuerte además de estar en el top 3 de Colombia Tech [80].

Ilustración 11: Logo B-Secure



Fuente: *B-Secure* [81]

2.5.4 360 Security Group

360 Security Group es otra de las empresas de Colombia que se dedican a brindar soluciones en ciberseguridad con más de 15 años en el sector, ofreciendo sus soluciones a sectores como el financiero, educativo, salud e incluso el sector industrial. Su página web no cuenta con mucha información sobre los servicios que prestan, cuentan con un modelo denominado CSIOC (Cybersecurity and Intelligence Operations Center) en el cual gestiona diferentes servicios, entre los que se pueden observar se listan los siguientes:

- ❖ Gestión SOC
- ❖ Monitoreo SOC
- ❖ Analítica SOC
- ❖ Inteligencia SOC
- ❖ Ethical Hacking
- ❖ Revisión de código
- ❖ Seguridad SDLC

Esta empresa no brinda mucha y según su trayectoria e información de la página web, su operación se basa en los servicios SOC, realizando, monitoreo, analítica, inteligencia, diagnóstico y demás [82].

Ilustración 12: Logo 360 Security Group



Fuente: 360 Security Group | LinkedIn [83]

2.5.5 Siguard

Según el perfil de LinkedIn la empresa fue fundada en 2018 lo cual indica que lleva un aproximado de 5 años en el sector, donde sus colaboradores están entre 11 a 50, es una PYME, ubicada en el sector de Bogotá en Colombia, de igual manera cuentan con una amplia gama de servicios en ciberseguridad como consultoría, respuesta a incidentes y demás servicios que se pueden observar en la **Ilustración 13**, apoya sectores como el sector de la salud, sector gobierno y sector financiero [84].

Ilustración 13: Servicios SIGUARD

 Prevención	 Seguridad Web	 Seguridad endpoint
• Ciberseguridad Colombia • Fugas de información • Ingeniería Social • Fortificación de Sistemas • Análisis de Vulnerabilidades • Hacking Ético • Pruebas Pentesting	• Prevencion de ataque DDOS • Seguridad en aplicaciones web • Seguridad en email • Administrador de accesos • Honeypots y Deception • Gestión de identidades • Seguridad en la nube	• Antimalware Avanzado • Seguridad Para Endpoints • DLP (Data loss prevention) • Segundo Factor de Autenticacion • Control de Amenazas • Mejora de productividad

Fuente: SIGUARD [84]

Esta empresa a pesar de llevar poco tiempo en el mercado ofrece diferentes soluciones de ciberseguridad entre las que destacan sus cursos formación en ciberseguridad los cuales cuentan con su propio certificado, entre los cursos que se observan en su página web destacan ISO 27001, ISO 22301, CISSP, CISM, CCNA, CISA, CEH, Security +, OSSTMM y PTES [84].

Ilustración 14: Logo SIGUARD



Fuente: *SIGUARD* [84]

2.6 Análisis de la competencia

En Colombia, el mercado de la ciberseguridad se ha tornado más competitivo en los últimos años debido a la mayor conciencia de las empresas sobre los peligros de la seguridad cibernética y la creciente necesidad de proteger sus sistemas y datos. Entre los competidores del mercado colombiano en ciberseguridad se encuentran diversas empresas, las cuales fueron analizadas y estudiadas, en la **Tabla 4** se observa un listado de algunas de las estas compañías, que para mi criterio ofrecen una amplia gama de servicios y pueden ser una gran competencia.

Tabla 4: Algunas de las compañías de ciberseguridad

N°	Empresa	Logo
1	DragonJAR [85]	
2	Appagate [86]	
3	Grupo Oruss [87]	
4	2Secure [88]	

5	Gamma Ingenieros [89]	 GAMMA INGENIEROS
6	SecPro [90]	 SecPro SECURITY PROFESSIONALS
7	a3Sec [91]	
8	Hack-Inn [92]	 Hack-Inn
9	iDentian [93]	 iDENTIAN ®
10	Internet Security Auditors [94]	 iSec auditors
11	J2K Security Group [95]	
12	NewNet [96]	 NewNet ® S.A.
13	Securesoft [97]	
14	Up Connection [98]	 Up Connection Ciberseguridad escalando la nube
15	IT Forensic Company [99]	 IT FORENSIC COMPANY
15	S2 Grupo [100]	 S2 GRUPO Anticipando un mundo ciberseguro

Fuente: Creación propia con base en datos de [85] - [100]

La mayoría de las empresas de ciberseguridad estudiadas ofrecen servicios SOC (Security Operations Center), los cuales se encargan de monitorear y controlar las redes de internet con el fin de hacerlas más seguras. Cabe destacar que, a diferencia de otras empresas, **Up Connection es la única que ofrece soluciones seguras para dispositivos IoT**. Es importante mencionar que **ninguna de las empresas estudiadas brinda un servicio de póliza de seguro contra un ciberataque**.

Al analizar las fortalezas y debilidades de estas empresas, se puede observar que una de las compañías más establecidas en el mercado colombiano es **B-Secure**, esta compañía cuenta con una gran variedad de servicios en ciberseguridad, ofrecen desde soluciones de seguridad para redes y sistemas, hasta servicios de cumplimiento normativo y consultoría. Esta compañía se ha destacado como una de las principales en el mercado, y es reconocida como una de las top 3 empresas de ciberseguridad en Colombia Tech [80], lo cual es una muestra de su experiencia y liderazgo en el sector.

2.7 Análisis DOFA

DOFA es un recurso estratégico para identificar fortalezas, debilidades, oportunidades y amenazas en un emprendimiento. El análisis DOFA no es un proceso estático, lo cual quiere decir que debe ser actualizado regularmente para adaptarse a las necesidades del ambiente empresarial, en la **Ilustración 15** se observan los factores a tener en cuenta para realizar este análisis [101].

Ilustración 15: Como hacer un DOFA



Fuente: Sistema TDC [102]

En conclusión, en análisis DOFA que se expone en la **Tabla 5** se puede observar que es un mercado con demasiada incertidumbre para realizar un emprendimiento, y para llegar al éxito se debe tener en cuenta cada una de estas fortalezas, debilidades, oportunidades y amenazas, las cuales permitan desarrollar un buen plan estratégico aprovechando esas fortalezas y oportunidades del sector, para así superar con éxito las debilidades y amenazas.

Tabla 5: Matriz DOFA

Fortalezas	Debilidades
• Estos servicios son necesarios en el mercado debido al aumento de la ciberdelincuencia en Colombia. • Existencia de empresas de ciberseguridad que no satisfacen la demanda. • Creación de nuevos empleos en áreas clave como la tecnología y la investigación.	• Poca experiencia en el sector, con un bajo reconocimiento de una nueva empresa en el sector. • No existe una estrategia clara para llegar al mercado. • Escasez de recursos para investigar y desarrollar nuevas tecnologías
Oportunidades	Amenazas
• Oportunidades para desarrollar programas educativos de capacitación, para ayudar al entendimiento y comprensión de las amenazas cibernéticas. • Creciente demanda en los sectores de ciberseguridad para IA, industria 4.0 e IoT. • Los ciberataques nunca podrán ser 100% evitables debido a los constantes avances tecnológicos	• Falta de profesionales altamente capacitados que requiere el sector. • Competencia cada vez más feroz de otras empresas de seguridad cibernética. • Falta de comprensión de las amenazas cibernéticas y de las medidas necesarias para protegerse.

Fuente: Creación propia

Capítulo 3 | Identidad Empresarial

3. Identidad Empresarial

En este capítulo, se busca establecer la identidad de la compañía, lo cual es fundamental para diferenciarse de los competidores y construir una reputación sólida en el mercado. La identidad empresarial es clave para establecer una relación de confianza con nuestros colaboradores y clientes y posicionarse en el mercado objetivo; en consecuencia, Jonathan Guerrero es el encargado de elaborar un plan estratégico para desarrollar y fortalecer la identidad de la compañía. Una vez establecida, es importante asegurar que todos los futuros colaboradores comprendan y respeten los elementos de la identidad empresarial, para poder mantenerla y protegerla a lo largo del tiempo.

3.1 Mi Pensamiento Emprendedor

El emprendimiento en Colombia puede presentar desafíos, pero no es imposible. A lo largo de los años, hemos visto a empresarios colombianos crear compañías exitosas, como Nu Bank, Addi, Littio, Frubana, Merqueo y Rappi, las cuales son una prueba de que con perseverancia y determinación se pueden superar los obstáculos, estas empresas me inspiran a elegir el camino del emprendimiento, que no solo se mide solo en ganancias, sino también en contribución, para ayudar a mejorar un país en desarrollo, con creación de empleos que generen impacto donde se fomenten la investigación e innovación, la educación y un hambre de constante superación.

3.2 Nombre de la Compañía

La elección del nombre de la compañía fue realizada de manera estratégica, con el objetivo de encontrar un nombre en inglés corto y fácil de pronunciar. Para lograrlo, se llevó a cabo una búsqueda de posibles opciones, analizando diferentes alternativas. Después de evaluar las diferentes opciones, se llegó a la conclusión de que el nombre adecuado para la empresa, y que además me resultaba agradable sería **Beef Up Tech**.

3.3 Eslogan de la Compañía

El eslogan de una empresa es una de las primeras cosas que los clientes ven y recuerdan de la marca; por lo tanto, es esencial que se elija cuidadosamente para transmitir de manera efectiva el mensaje y los valores de la marca. En el caso de Beef Up Tech, se buscó un eslogan que fuera creativo y estuviera relacionado con el nombre de la empresa.

Se trabajó en varias opciones, considerando diferentes aspectos como la claridad del mensaje y la originalidad. **"For Real Digital Protection"** es el eslogan más adecuado para Beef Up Tech. Este eslogan intenta transmitir la idea de que la empresa ofrece una protección real para entornos digitales, que es uno de los valores principales de la marca.

3.4 Imagen de la Compañía

Para el diseño de nuestro logotipo se utilizó un degradado lineal en colores morado violeta y azul. Para seleccionar el logotipo adecuado, se llevó a cabo un análisis de los diferentes tipos de logotipos, como los tipográficos, isotipos o pictogramas e imagotipos. Desde mi punto de vista, los más atractivos y efectivos son los imagotipos, ya que al combinar el nombre de la marca con una imagen o símbolo se crea una asociación visual que ayuda a los clientes a recordar la marca más fácilmente. Además, un buen imagotipo puede transmitir información sobre la marca, su personalidad y su propósito, todo en un solo diseño.

Ilustración 16: Logo Beef Up Tech



3.5 Pensamiento Corporativo

3.5.1 Misión

En Beef Up Tech queremos **llevar a otro nivel el talento de nuestros clientes y colaboradores, abordando los desafíos que surgen con la llegada de la cuarta revolución industrial**. Entendemos que la tecnología está cambiando constantemente y nuestro objetivo es mantenernos al frente para ofrecer soluciones adaptadas que puedan satisfacer las demandas de nuestros clientes y mejorar la eficacia de sus procesos organizativos, para esto contamos con un equipo altamente capacitado, comprometido y apasionado por su trabajo, lo que nos permite garantizar un excelente servicio.

3.5.2 Visión

Queremos ser referentes en el sector, donde nos esforzaremos para desarrollar una cultura de ciberseguridad en las empresas que mediante la constancia y el esfuerzo de todo nuestro equipo de profesionales puedan **hacer del mundo digital un espacio más seguro y confiable para todos**. Trabajaremos mano a mano con nuestros clientes y colaboradores, para alcanzar logros compartidos donde nuestro éxito, también sea el éxito de ellos.

3.5.3 Valores

- ✓ Nuestro activo más importante son nuestros clientes y colaboradores.
- ✓ Se ofrece lo que está al alcance de nuestros profesionales.
- ✓ Nuestros colaboradores tienen un compromiso con su desarrollo profesional y personal.

3.5.4 Objetivos

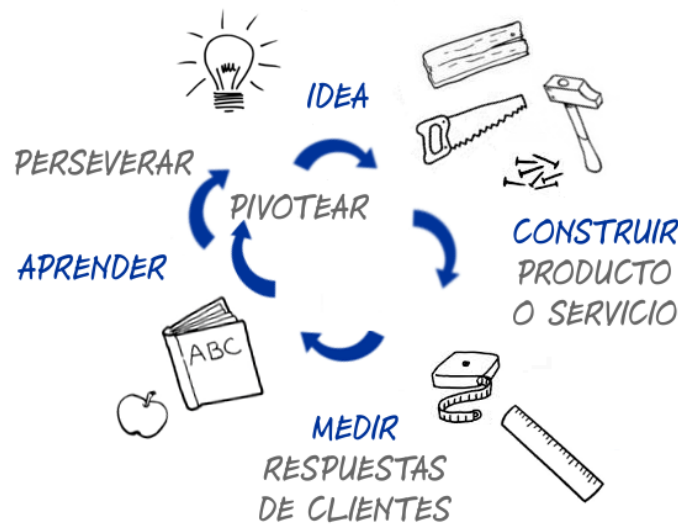
- ✓ Satisfacción de nuestros clientes.
- ✓ Mejoramiento progresivo de nuestros clientes.
- ✓ Dar a conocer y ayudar a que las empresas se apropien de las nuevas tecnologías.

Capítulo 4 | Metodología Lean Startup

4. Metodología Lean Startup

El método Lean Startup fue diseñado por Eric Ries en Silicon Valley y se ha convertido en una de las principales metodologías para lanzar un negocio exitoso, enfocándose en el menor riesgo posible. Como se observa en la **Ilustración 17** el proceso se divide en hipótesis y experimentos para descubrir si los modelos de negocios planteados son viables o no. A través de un proceso de aprendizaje validado, se pueden comprobar cuidadosamente hipótesis de un prototipo definido conocido como MVP. El objetivo principal de esta metodología es crear un modelo de negocio escalable utilizando la innovación continua para hacer los emprendimientos más ágiles [103].

Ilustración 17: Ciclo Lean Startup



Fuente: Designthinking [104]

4.1 Etapas Lean Startup

4.1.1 Validación de la Idea

Antes de dedicar tiempo y dinero a la creación de un buen producto o servicio, primero hay que validar la idea de negocio. Para asegurar el éxito del emprendimiento, es crucial confirmar que existe una verdadera demanda en el sector sobre el que se quiere influir. Esto se logra mediante un estudio detallado del sector, que permita analizar el potencial de la idea de empresa e identificar factores como la demanda, la rivalidad, los precios y los posibles clientes, entre otros [105].

En esta etapa, es importante realizar investigaciones para recolectar información valiosa y así tener una mejor comprensión del mercado y de los clientes, es recomendable analizar y comparar datos estadísticos con estudios previos que permitan ver otro ángulo del mercado y de la industria, el cual permite tomar decisiones informadas sobre el desarrollo del producto o servicio aumentando las posibilidades de éxito del emprendimiento [105].

4.1.2 Creación de un MVP

Una vez que se tiene una idea clara de lo que se quiere desarrollar, es importante crear un prototipo conocido como producto mínimo viable (MVP) el cual es una forma de validar la idea y ahorrar recursos al mismo tiempo donde solo se incluyen las funcionalidades esenciales del producto o servicio. La idea es empezar con un solo cliente y construir un MVP que incluya características que podrían impactar en el mercado, y como mínimo resolver el problema principal y demostrar el valor del producto. No hay una fórmula exacta para construir un MVP, lo importante es que ese producto o servicio mínimo sirva al emprendedor para conocer su viabilidad [106].

4.1.3 Medir el Impacto de MVP

Una vez que se ha construido el producto mínimo viable (MVP), es importante lanzarlo al mercado para recopilar feedback de los clientes, midiendo el interés y la demanda del mismo, lo cual permite conocer la reacción de los clientes y comprender cómo perciben el producto o servicio. Al recopilar y analizar estos datos de los clientes, se pueden ver las tendencias y hacer juicios sobre cómo mejorar los productos o servicios con el fin de realizar las modificaciones necesarias para satisfacer mejor la demanda sector y tener en cuenta las preferencias de los clientes [107].

4.1.4 Genera un Aprendizaje

Para esta fase independientemente si el MVP inicial fue un éxito o no, se debe mejorar el producto o servicio con el feedback que dieron los clientes. Esta etapa es donde se realizan los cambios necesarios con la retroalimentación recibida, la cual es información de datos valiosa y permite entender cómo se percibe el producto o servicio, qué cambios

son necesarios para mejorarlo y entender que la mejora continua es esencial para mantenerse competitivo en el mercado asegurando el éxito del negocio y adaptando el producto o servicio a las necesidades del cliente para que se pueda garantizar que se va entregar algo de calidad [107].

4.1.5 Perseverar

Perseverar es un factor determinante para triunfar en cualquier campo de nuestras vidas, especialmente cuando se trata de emprendimientos que aplica la metodología Lean Startup. Sin embargo, no siempre es fácil encontrar el éxito en el primer intento. Puede ser necesario pivotar, es decir, modificar el rumbo del desarrollo de un producto o servicio hasta encontrar el Product-Market-Fit. Pivotar no significa fracasar con tu idea, sino tomar la decisión de cambiar de rumbo antes de invertir demasiado tiempo y recursos en una solución que no funciona, dándose cuenta a tiempo de que ese producto o negocio no tiene futuro, ahorrándonos recursos y tiempo [108].

La metodología Lean Startup es un proceso iterativo, y pivotar es una parte importante de ese proceso. Es importante no aferrarse a una idea o solución que no funciona, sino estar dispuesto a cambiar de dirección para encontrar el éxito. La perseverancia y la capacidad de pivotar son las claves para alcanzar el éxito de la metodología Lean Startup [108].

4.2 Casos de Éxito

4.2.1 Dropbox

Dropbox es un servicio de transferencia de archivos sus fundadores antes de comenzar a desarrollar el producto querían validar si había interés en un servicio de sincronización de archivos, para ello crearon un video explicativo de 3 minutos que mostraba un producto funcionando, aunque en realidad no existía, la estrategia resultó ser un gran éxito, ya que más de 70.000 personas dejaron sus correos electrónicos para unirse a la lista de espera. La compañía aplicó el método de Lean Startup, creando un producto mínimo viable. Dropbox paso a ser tendencia de la noche a la mañana y sigue siendo una herramienta muy popular hoy en día [105] [109].

4.2.2 Slack

Slack, una plataforma de comunicación y colaboración en tiempo real para equipos, nació como una iniciativa interna de TinySpeck, una empresa de juegos. El modelo de ingresos inicial dependía de que la gente se suscribiera al juego Glitch, lanzado en 2011, que tuvo una vida útil limitada y terminó en 2012. A pesar del fracaso del juego, TinySpeck descubrió que aún disponía de un eficaz sistema de mensajería interna que había creado y utilizado durante el desarrollo del juego y que era de gran popularidad entre los miembros de la compañía [109].

Con el objetivo de recabar opiniones y conocer mejor la viabilidad de la aplicación, la empresa decidió pedir a usuarios externos que probaran y revisaran la herramienta. Esto fue bien recibido por sus usuarios y, finalmente, la empresa decidió concentrarse en Slack, lanzando su versión beta en agosto de 2013 y su versión oficial en febrero de 2014. Desde entonces, Slack ha escalado tanto que ha logrado convertirse en uno de los sistemas de comunicación y colaboración más utilizados a nivel global, llegando a ser muy popular entre empresas y equipos de trabajo. Slack salió a bolsa en 2019, con un valor de más de 10.000 millones de dólares [110].

4.2.3 Zappos

En 1999, Nick Swinmurn, fundador de Zappos, se encontraba indeciso sobre si lanzar su marca al mercado en línea. La pregunta que se hacía era si los clientes estaban realmente preparados para comprar zapatos a través de Internet. A pesar de que hoy en día las compras en línea son cada vez más comunes, en aquel entonces, el concepto aún era incierto. Sin embargo, en lugar de dejar pasar esta oportunidad, Swinmurn decidió probar su hipótesis a través del desarrollo de un producto mínimo viable [110].

Swinmurn comenzó tomando fotografías profesionales de algunas tiendas y publicarlas en un sitio web básico. Si recibía un pedido, se dirigía a la tienda física y compraba el calzado para enviarlo directamente al cliente. Este proceso se llevó a cabo durante un tiempo suficiente para comprobar que existía una demanda suficiente para que este negocio se convirtiera en algo rentable. Zappos se convirtió en una de las principales minoristas de calzado en línea, y su éxito demostró que los clientes estaban listos para comprar zapatos por Internet [110].

4.3 Encuesta Exploratoria

Al profundizar en el campo y observar los diferentes servicios que ofrecen las empresas del sector, llegué a la conclusión de que la opción más viable sería comenzar con certificaciones en ciberseguridad. Esta alternativa resulta menos costosa y más factible, por lo que decidí lanzar una encuesta para evaluar el interés y la demanda del mercado en ciberseguridad, así como recabar opiniones de los usuarios sobre este campo.

La encuesta se difundió a través de diversas plataformas como LinkedIn, Facebook y Discord, con el objetivo de obtener una amplia variedad de perspectivas. Las respuestas más relevantes se recopilaron principalmente de los miembros de la Universidad Santo Tomás de Colombia, de las facultades de Ingeniería de Telecomunicaciones e Ingeniería Electrónica.

4.3.1 Evaluación Del Sector: Resultados

Para garantizar la validez y la confiabilidad de los resultados del estudio, se pone a disposición el correo support@beefuptech.com, para que todos los participantes o lectores puedan validar los resultados de la encuesta. Esta medida se implementa con el fin de tener una oportunidad para verificar cualquier información relevante que pueda surgir de los resultados. En relación con la encuesta realizada, se recibieron un total de 87 respuestas, donde los participantes tienen una edad promedio de 21 años. Además, se observa que el 80,5% de los encuestados son estudiantes universitarios, mientras que el 19,5% restante se distribuye entre profesiones del sector TI.

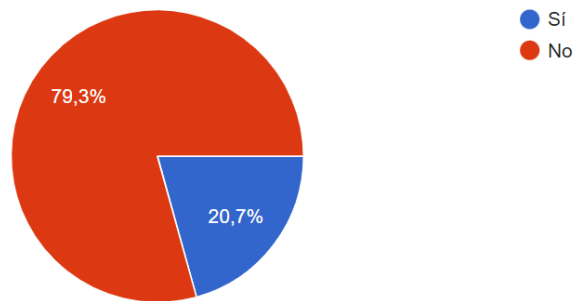
4.3.1.1 Víctimas de estafas en línea

En el estudio, se plantea una pregunta fundamental para determinar el número de personas que han sido víctimas de fraudes en línea. A los encuestados se les pregunta lo siguiente: "¿Ha sido víctima de algún tipo de estafa o fraude en línea, como suplantación de identidad o robo de información personal?" Como se observa en **Ilustración 18**, los resultados revelan que el 79,3% de los encuestados indicaron no haber sido víctimas de este tipo de fraudes en línea. Por otro lado, el 20,7% afirmó haber sido víctima de algún tipo de fraude en Internet, como suplantación de identidad o robo de información personal.

Ilustración 18: Fraudes en Línea: ¿Ha sido víctima?

¿Ha sido víctima de algún tipo de estafa o fraude en línea, como suplantación de identidad o robo de información personal?

87 respuestas



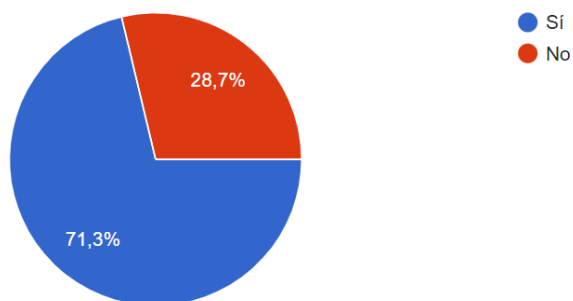
Fuente: Investigación propia

A pesar de los datos anteriores que indican que un porcentaje bajo de personas ha sido víctima de estafas en línea, es importante destacar tal y como se observa en la **Ilustración 19**, que el 71,3% de los encuestados afirman conocer por lo menos a una persona de su núcleo que si ha sido víctima de fraude en línea. Por otro lado, el 28,7% restante no conoce a nadie en su entorno que haya experimentado este tipo de situaciones. Estos resultados ponen en evidencia que, aunque algunos encuestados no han sido directamente afectados por fraudes en línea, existe una percepción de que estos incidentes ocurren a nivel cercano y afectan a personas conocidas.

Ilustración 19: Fraudes en línea: ¿Conoce víctimas?

¿Conoce a alguien que haya sido víctima de estafas en línea o que haya sufrido el robo de sus datos personales?

87 respuestas



Fuente: Investigación propia

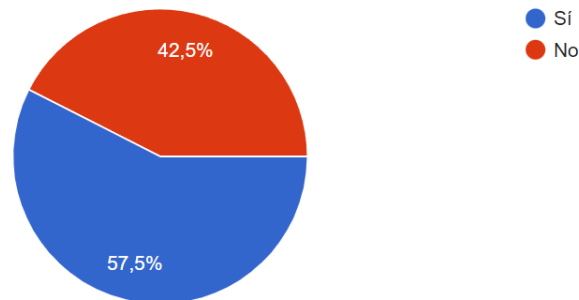
4.3.1.2 Términos clave en ciberseguridad

Con el objetivo de evaluar el nivel de conocimiento en el campo de la ciberseguridad, se planteó una pregunta para determinar si los participantes estaban familiarizados con el término "phishing". Los resultados muestran que el 42,5% de los encuestados afirmó no estar familiarizado con este término, mientras que el 57,5% indicó tener conocimiento sobre él. Estos resultados se pueden visualizar en la **Ilustración 20**.

Ilustración 20: Percepción del "Phishing"

¿Está familiarizado con el término "phishing" y su significado?

87 respuestas



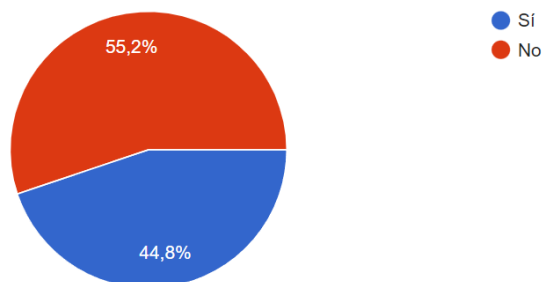
Fuente: Investigación propia

En el campo de la ciberseguridad, el término "ransomware" juega un papel crucial. El estudio realizado revela datos interesantes, donde el 55,2% de los encuestados admitió no tener conocimiento sobre el significado del ransomware. Por otro lado, el 44,8% de los encuestados afirmó estar familiarizado con este término. Estos resultados se pueden visualizar en la **Ilustración 21**.

Ilustración 21: Percepción del "Ransomware"

¿Está familiarizado con el término "ransomware" y su significado?

87 respuestas



Fuente: Investigación propia

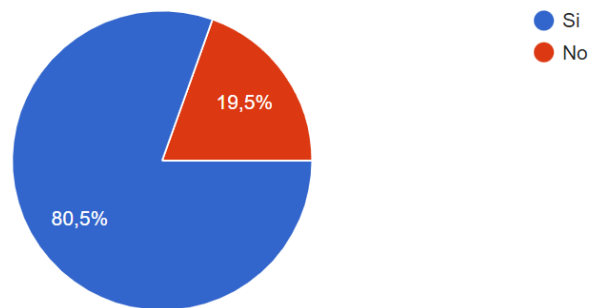
4.3.1.3 Interés en la ciberseguridad

Con el objetivo de indagar sobre el nivel de interés de los profesionales del área de TI en el campo de la ciberseguridad, se les formuló la siguiente pregunta: "¿Es la ciberseguridad un campo de su interés?". Como se observa en la **Ilustración 22**, los resultados obtenidos revelan que el 80,5% de los encuestados manifestaron un claro interés o atracción hacia dicho campo. Por otro lado, el 19,5% restante afirmó no sentir atracción por la ciberseguridad.

Ilustración 22: Interés en la ciberseguridad

¿Es la ciberseguridad un campo de su interés?

87 respuestas



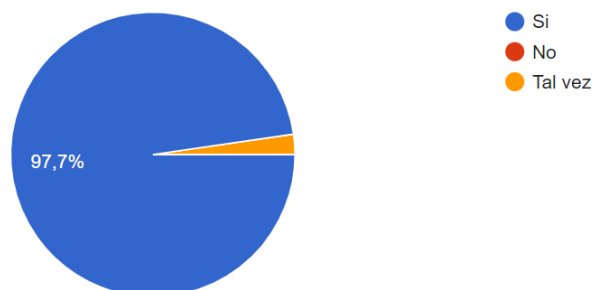
Fuente: Investigación propia

Por otro lado, los resultados de la encuesta revelan un dato significativo, y como se puede observar en la **Ilustración 23**, con un 97,7% de las personas encuestadas considera que el campo de la ciberseguridad es de gran importancia, por otro lado 2,3% de los participantes indicó que tal vez el campo de la ciberseguridad podría ser importante.

Ilustración 23: Percepción de la importancia de la ciberseguridad

¿Considera usted que la ciberseguridad es importante?

87 respuestas



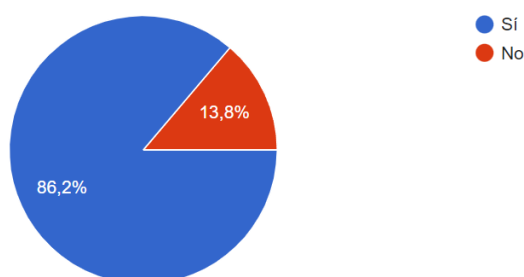
Fuente: Investigación propia

La **Ilustración 24** revela los resultados obtenidos al preguntar a los encuestados sobre su interés en el campo de la ciberseguridad y su disposición para ingresar al mercado laboral en dicho ámbito. Los datos demuestran que el 86,2% de los encuestados expresaron tener cierto interés en el campo y manifestaron su deseo de adquirir habilidades relacionadas con este ámbito en particular, por otro lado, un 13,8% de las personas encuestadas afirmaron no tener ningún tipo de interés.

Ilustración 24: Interés en la ciberseguridad

¿Está interesado en adquirir habilidades y conocimientos en un área (*Ciberseguridad*) de rápido crecimiento y alta demanda en el mercado laboral?

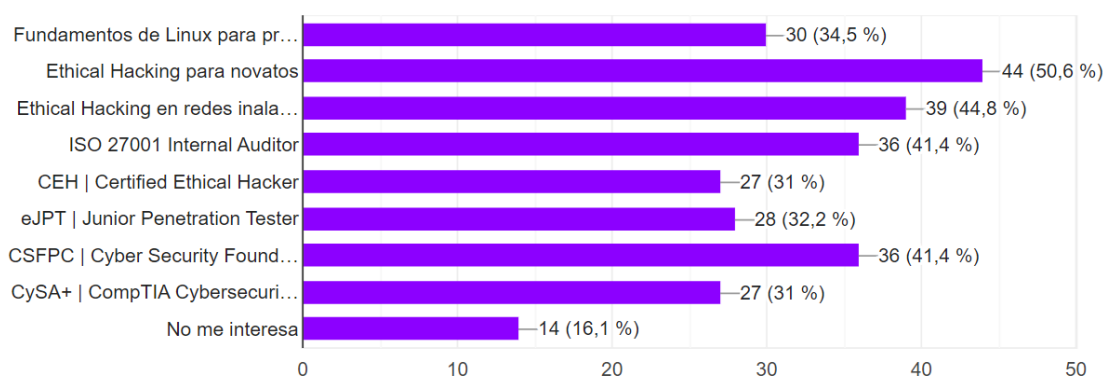
87 respuestas



Fuente: Investigación propia

En la ilustración 25, se evidencia el interés demostrado por los encuestados en aprender sobre temas de ciberseguridad y hacking. Los resultados revelan que los encuestados muestran un particular interés en adquirir bases sólidas y optar por cursos que les brinden los fundamentos necesarios para ingresar en este campo. Estos resultados confirman el claro interés que los encuestados tienen por la ciberseguridad.

Ilustración 25: Certificaciones de interés



Fuente: Investigación propia

4.4 MVP-1: Certified Cybersecurity Training

Al analizar los resultados de la encuesta, se observa un cierto interés por parte de los usuarios hacia el campo de la ciberseguridad. Teniendo en cuenta los resultados, se ha tomado la decisión de lanzar un par de certificaciones propias, específicamente diseñadas para abarcar los aspectos clave del campo. Además, con el objetivo de brindar una oferta más completa y diversificada, se establece una colaboración estratégica con Certiprof. A través de esta alianza, se impartirán las certificaciones que ellos ofrecen en el campo de la ciberseguridad, ampliando así el portafolio de formación y especialización para los interesados.

4.4.1 Beef Up Tech Certified Offensive Security Wireless

Los datos recopilados a través de la encuesta revelan un evidente interés por parte de los encuestados en el campo de la seguridad en redes inalámbricas. Tomando en cuenta esta demanda, hemos decidido desarrollar una certificación específica que permita a los interesados ampliar sus conocimientos sobre los diversos vectores de ataque presentes en el ámbito de las redes inalámbricas, el nombre de la certificación es Beef Up Tech Certified Offensive Security Wireless y su acrónimo BCOSW.

Ilustración 26: Certificación BCOSW



Fuente: Diseño propio

En la **Ilustración 26**, se observa la certificación digital que se otorgará a aquellos que logren completar satisfactoriamente todos los elementos evaluativos. Esta certificación representa un reconocimiento oficial y evidencia el dominio de los conocimientos y

habilidades necesarios en el campo de la seguridad en redes inalámbricas. Para obtener toda la información relacionada con la certificación, se podrá visitar el sitio web oficial en <https://beefuptech.com/>

4.4.2 Beef Up Tech Certified Linux for Security Practitioners

Esta certificación se desarrollará tomando en consideración la relevancia que tiene el sistema operativo Linux en el ámbito de la ciberseguridad. Linux desempeña un papel fundamental en numerosos campos, y la ciberseguridad no es una excepción. En la **Ilustración 27**, se observa la certificación digital que se otorgará a aquellos que logren completar satisfactoriamente todos los elementos evaluativos.

Ilustración 27: Certificación BCLSP



Fuente: Diseño propio

4.4.3 Beef Up Tech Certified Ethical Hacker Analyst

Esta opción de certificación estará diseñada para profesionales de nivel básico-intermedio que deberían contar con conocimientos básicos de Linux. Se recomienda a los aspirantes haber completado previamente la certificación "Beef Up Tech Certified Linux for Security Practitioners", ya que esta certificación requerirá un mayor compromiso y nivel de habilidades.

La certificación abordará temas avanzados en el campo de la ciberseguridad, centrándose en áreas como el reconocimiento y escaneo de sistemas, el uso de Docker para la creación de entornos seguros, así como el estudio detallado del OWASP TOP 10, que enumera las principales vulnerabilidades en aplicaciones web y servicios en línea. En

la **Ilustración 27**, se observa la certificación digital que se otorgará a aquellos que logren completar satisfactoriamente todos los elementos evaluativos.

Ilustración 28: Certificación BCEHA



Fuente: Diseño propio

4.4.4 Authorized Training Partner Certiprof

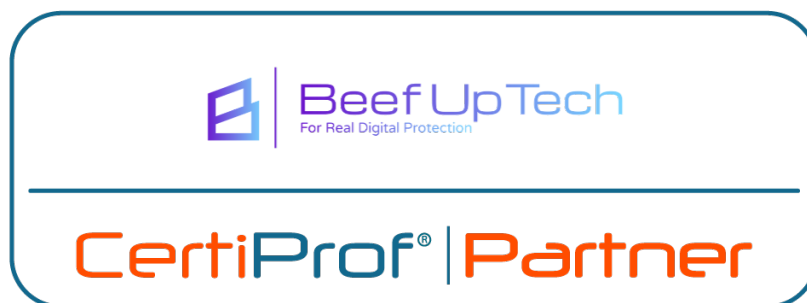
Con el objetivo de lograr un mayor reconocimiento en la industria y fortalecer el catálogo de certificaciones, se ha optado por tomar el programa de colaboración como Partner con CertiProf. Esta asociación estratégica permitirá ofrecer una amplia gama de certificaciones en ciberseguridad, reforzando así nuestro posicionamiento en este campo. Además, se aprovecharán las certificaciones de liderazgo ofrecidas por CertiProf, ya que creemos en la importancia de desarrollar habilidades de liderazgo en el sector de la ciberseguridad.

Como socios de CertiProf, tendremos acceso a una amplia gama de recursos, que incluyen material de estudio y simulacros de exámenes para todas sus certificaciones. Sin embargo, nuestro enfoque principal estará en las certificaciones de ciberseguridad que ellos ofrecen. Al apoyarnos de CertiProf lograremos tener certificaciones listas para salir al mercado, a diferencia de nuestras certificaciones internas, en donde sería necesario generar todo el material y los simulacros de exámenes, lo que requiere una inversión significativa de tiempo y esfuerzo.

Al contrario que con CertiProf, para nuestras propias certificaciones, no necesitaremos adquirir vouchers de certificación, lo que se traduce en un margen de

contribución más elevado. Además, aprovecharemos el reconocimiento de CertiProf como entidad certificadora para apoyarnos y emitir certificaciones respaldadas por el sello de CertiProf.

Ilustración 29: ATP CertiProf



Fuente: ATP Beef Up Tech [111]

Capítulo 5 | Constituyendo Una Empresa: Marco Legal y Organizacional

5. Marco Legal y Organizacional

El marco legal y organizacional es crucial para establecer y operar una empresa exitosa en cualquier país, y Colombia no es la excepción; por lo tanto, a la hora de crear una empresa en Colombia, es necesario considerar las leyes, regulaciones y políticas que se aplican al tipo de empresa que se quiere crear, así como a la industria en la que se va a operar. En este sentido, el capítulo que aborda estos temas puede resultar de gran ayuda para los empresarios que deseen establecerse en Colombia.

5.1 Constitución Legal de Beef Up Tech

5.1.1 ¿Persona Jurídica o Natural?

Para responder a la pregunta de si se debe constituir la empresa como persona jurídica o natural, es importante considerar el perfil de los potenciales clientes. Si los clientes son empresas legalmente constituidas a las cuales se les debe entregar facturas, lo más adecuado sería constituir la empresa como persona jurídica en lugar de persona natural, ya que esto permitiría cumplir con las obligaciones tributarias y fiscales requeridas para la emisión de facturas [112].

Es importante recordar que las personas naturales no están obligadas a emitir facturas, sino que pueden entregar cuentas de cobro. Por otro lado, una empresa constituida como persona jurídica tiene la capacidad legal para emitir facturas y cumplir con todas las obligaciones fiscales correspondientes; en consecuencia, al considerar el perfil de los potenciales clientes y las obligaciones fiscales y tributarias requeridas, resulta más adecuado constituir la empresa como **persona jurídica** en lugar de persona natural, ya que esto permitiría cumplir con los requisitos necesarios para la emisión de facturas y operar de manera legal y transparente en el mercado [112].

5.1.2 Tipo de Sociedad

En Colombia, existen diferentes tipos de sociedades que las personas jurídicas pueden establecer, tales como Sociedad Limitada, Sociedad Anónima, Sociedad en Comandita Simple, Sociedad en Comandita por Acciones, Sociedad por Acciones Simplificada y Empresa Unipersonal. Para Beef Up Tech, la opción más adecuada es

constituirse como **Sociedad por Acciones Simplificada (SAS)**, debido a que esta alternativa es la más flexible y se ajusta perfectamente a la actividad económica que se desea realizar [113].

La SAS permite una mayor libertad en la toma de decisiones, en la estructuración del capital y en la gestión de la empresa, lo cual se traduce en una mayor adaptabilidad y agilidad en la gestión de la empresa, especialmente para startups y empresas de tecnología. Además, la SAS no exige un capital mínimo para su constitución, lo que representa una ventaja para aquellas empresas que están iniciando su actividad económica y no disponen de una gran cantidad de recursos [113].

5.1.3 Homonimia

La Cámara de Comercio establece que, para registrar legalmente el nombre de una sociedad, este no debe ser idéntico al de otra empresa ya existente. A esto se le conoce como homonimia del nombre y se verifica a nivel nacional a través de la consulta en el Registro Único Empresarial (RUES) o a través de la Cámara de Comercio de Bogotá, estas consultas están disponibles desde sus páginas web [114].

En el caso específico de Beef Up Tech, como se observa en la **Ilustración 18** al realizar la consulta en el RUES se pudo comprobar que el nombre no se encuentra registrado, lo que significa que no existe otra empresa en Colombia con el mismo nombre y por lo tanto puede ser utilizado para establecer legalmente la empresa, al ser un nombre único y no tener homonimia con otras empresas [114].

Ilustración 30: Consulta homonimia

The image shows a web interface for a business or social consultation. At the top, the text 'Realice su consulta empresarial o social' is displayed. Below this is a search bar containing the text 'Beef Up Tech'. To the right of the search bar is a green checkmark icon and a red button with a white magnifying glass icon. A blue arrow points from the search bar area to a circular icon containing the number '1'. Below the search bar, there is a link that says 'Recomendaciones de uso'. At the bottom, a blue banner contains the text 'Info La consulta por Nombre no ha retornado resultados'. A blue arrow points from this banner to a circular icon containing the number '2'.

Fuente: Página RUES

5.1.4 Actividad Económica (CIIU)

Una vez decidido el tipo de sociedad a establecer, es importante identificar la actividad económica de la empresa mediante la Clasificación Internacional Industrial Uniforme (CIIU). Esta clasificación es un sistema utilizado a nivel mundial para clasificar las distintas actividades económicas. Para determinar la actividad económica de Beef Up Tech, se puede realizar una búsqueda de empresas similares que presten servicios idénticos o similares y, de esta manera, obtener los códigos de clasificación CIIU adecuados [114]. La **Tabla 6** muestra algunos de estos códigos para facilitar la identificación de la actividad económica de la empresa.

Tabla 6: Empresas competidoras con actividad económica

Empresa	Código CIIU	Actividad Económica (Descripción)
DRAGONJAR	6202	Actividades de consultoría informática y actividades de administración de instalaciones informáticas
	6201	Actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas)
	6209	Otras actividades de tecnologías de información y actividades de servicios informáticos
SECURESOFT	6201	Actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas)
	6202	Actividades de consultoría informática y actividades de administración de instalaciones informáticas
	6312	Portales web
	5820	Edición de programas de informática (software)
IT FORENSIC COMPANY	6209	Otras actividades de tecnologías de información y actividades de servicios informáticos
	6201	Actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas)
	6202	Actividades de consultoría informática y actividades de administración de instalaciones informáticas
SECPRO SAS	6202	Actividades de consultoría informática y actividades de administración de instalaciones informáticas
	6201	Actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas)
	8551	Formación para el trabajo
J2K SECURITY GROUP	6202	Actividades de consultoría informática y actividades de administración de instalaciones informáticas
	6209	Otras actividades de tecnologías de información y actividades de servicios informáticos

Fuente: Creación propia con base en datos del RUES y CCB

Una vez que se ha tomado la decisión sobre el tipo de sociedad que se va a establecer, resulta crucial determinar la actividad económica principal que va a desarrollar la empresa, ya que esto puede impactar el régimen tributario al que estará sujeta, así como las obligaciones fiscales y laborales. Es importante destacar que se puede seleccionar una actividad económica como mínimo y hasta un máximo de cuatro; en consecuencia, Beef Up Tech, se han identificado con los siguientes cuatro códigos CIIU que describen su actividad económica principal: 8559, 6202 y 6201.

- **CIIU 8559:** incluye las "Otras actividades de educación n.c.p¹⁷.", lo que sugiere que Beef Up Tech también puede ofrecer servicios de capacitación y formación en tecnología, ya sea para sus empleados o para clientes que buscan mejorar sus habilidades y conocimientos en este ámbito.
- **CIIU 6202:** se refiere a las "Actividades de consultoría informática y de gestión de instalaciones informáticas", lo que indica que Beef Up Tech también puede brindar servicios de asesoramiento y gestión de tecnologías de la información a sus clientes.
- **CIIU 6201:** Corresponde a la "Actividades de desarrollo de sistemas informáticos a medida", lo que sugiere que Beef Up Tech se dedica a la creación de soluciones tecnológicas personalizadas para sus clientes. Este tipo de actividad económica puede incluir el desarrollo de software, la integración de sistemas, la automatización de procesos y la consultoría tecnológica.

5.1.5 Consulta Uso de Suelo

La consulta de uso de suelos es obligatoria únicamente para los establecimientos de comercio que cuentan con un lugar físico, y es un trámite obligatorio que se debe realizar al crear una empresa en el país. Esta consulta se lleva a cabo con el objetivo de verificar si el lugar donde se pretende establecer el comercio cumple con los requisitos urbanísticos y ambientales exigidos por las normativas y leyes de Colombia. En el caso de Beef Up Tech, al ser una empresa que operará netamente digital, no es necesario realizar esta consulta ya que la empresa no tendrá una ubicación física [112].

¹⁷ N.C.P: No clasificadas en otra parte

5.1.6 Trámites Ante Cámara y Comercio

Para constituir legalmente Beef Up Tech, existen dos opciones disponibles, la primera es realizar el trámite de manera presencial ante la Cámara de Comercio de Bogotá (CCB), mientras que la segunda opción es realizar el trámite por medio de la página web de la entidad, en el apartado de VUE (Ventanilla Unica Empresarial), en ambos casos, se deben pagar los costos asociados [112].

La diferencia entre ambas opciones radica en el documento privado conocido como estatutos. Si se realiza el trámite de manera presencial, es posible definir con precisión la actividad económica a la que se dedicará la empresa. Por otro lado, si se realiza el trámite de manera virtual, los estatutos serán más genéricos, lo que significa que la empresa podrá dedicarse a cualquier cosa; ahora bien, para tener una mayor claridad en la actividad económica que realizará la empresa, este trámite se gestionará presencialmente ante la CCB, de esta forma se podrán definir los estatutos de manera precisa y adaptados a las necesidades específicas de la empresa [112].

Tabla 7: Costos de legalización primera vez 2023

Concepto	Valor
Derechos de inscripción	\$ 53,000
Situación de control ¹⁸	\$ 208,000
Formulario RUES ¹⁹	\$ 7,200
Impuesto de registro	0.6% * Capital suscrito ²⁰
Matricula mercantil	Ley 1780 de 2016

Fuente: Creación propia con base en datos de CCB

Es importante destacar que existe un beneficio al cual se puede aplicar a través del formulario del RUES conocido como “Ley 1780 de 2016”, donde indica que los emprendimientos de personas menores de 35 años pueden estar exentos del pago de la matrícula mercantil y su renovación durante el primer año [115]. Además, la Cámara de Comercio también se encarga de tramitar el RUT ante la DIAN, lo cual es un trámite

¹⁸ La manifestación de situación de control se solicita únicamente en los casos en que hay un único socio y este posee el 100% de las acciones.

¹⁹ RUES: Formulario de Registro Único Empresarial y Social

²⁰ El Capital suscrito es la cantidad de dinero que los accionistas han acordado aportar a la sociedad al momento de su constitución.

obligatorio para poder realizar actividades económicas en Colombia. En la **Tabla 7** se detallan los costos asociados con el proceso de legalización de una empresa ante la Cámara de Comercio de Bogotá. [112].

5.2 Obligaciones fiscales

Constituir una persona jurídica en Colombia implica asumir responsabilidades legales y fiscales ante el estado. Esto implica la presentación de una serie de impuestos que se calculan en función de las utilidades generadas por la empresa. Sin embargo, es importante tener en cuenta que no todos los impuestos aplican a todas las empresas, ya que algunos son específicos y solo se aplican a ciertos tipos de negocios, por esta razón, sería ideal contar con la ayuda de profesionales especializados que nos guíen en el cumplimiento de las responsabilidades legales y fiscales.

5.2.1 Impuesto al Valor Agregado (IVA)

El IVA es una obligación que debe cumplir toda empresa que realice actividades económicas sujetas a este impuesto. En el estatuto tributario 476 se establecen los lineamientos para determinar qué servicios están excluidos de cobrar el IVA, como por ejemplo los servicios médicos, de transporte público, ciertas construcciones, entre otros, donde cada caso en particular debe ser evaluado según corresponda.

Para este emprendimiento, es importante considerar el numeral 6 del artículo 476 del Estatuto Tributario y el artículo 2.2.16.3 del Decreto 1078 de 2015 para determinar qué servicios estarán sujetos al cobro del IVA 19%. En el caso de ampliar los servicios, cada situación debe ser evaluada de forma individual, además es importante mencionar que las personas naturales pueden estar exentas de cobrar el IVA hasta un límite de 3500 UVT (Unidades de Valor Tributario), que para el año 2023 se sitúa en \$42,412 pesos.

5.2.2 Impuesto Sobre la Renta

Este impuesto al que se hace referencia es la declaración de renta, un impuesto anual que grava las utilidades generadas por las empresas durante el período comprendido entre enero y diciembre. En el año 2023, este impuesto se establece en un 35% sobre las utilidades. Es importante destacar que existen fechas específicas para realizar el pago de

este impuesto para evitar posibles multas, tanto para personas naturales como para personas jurídicas, donde el solo hecho de no presentar la declaración ya genera una multa de \$424.000 pesos para el año 2023, la cual ira subiendo, dependiendo de cada situación en particular.

5.2.3 Impuesto de Industria y Comercio (ICA)

El impuesto de Industria y Comercio (ICA) establece que las personas naturales deben realizar la declaración correspondiente de acuerdo con los límites establecidos anualmente, para el caso de las empresas, es decir, las personas jurídicas, deben presentar la declaración si generan ingresos en su actividad comercial o de servicios. Este impuesto se aplica a cualquier actividad comercial o de servicios que se realice.

5.2.4 Facturación electrónica

Toda persona, tanto natural como jurídica, que genere ingresos superiores a 3500 UVT está obligada a emitir facturas electrónicas. La facturación electrónica tiene como propósito documentar todas las operaciones comerciales realizadas. El incumplimiento de esta obligación puede conllevar a multas o sanciones de acuerdo con lo establecido por los artículos 657 y 658 del Estatuto.

5.2.5 Otras Obligaciones

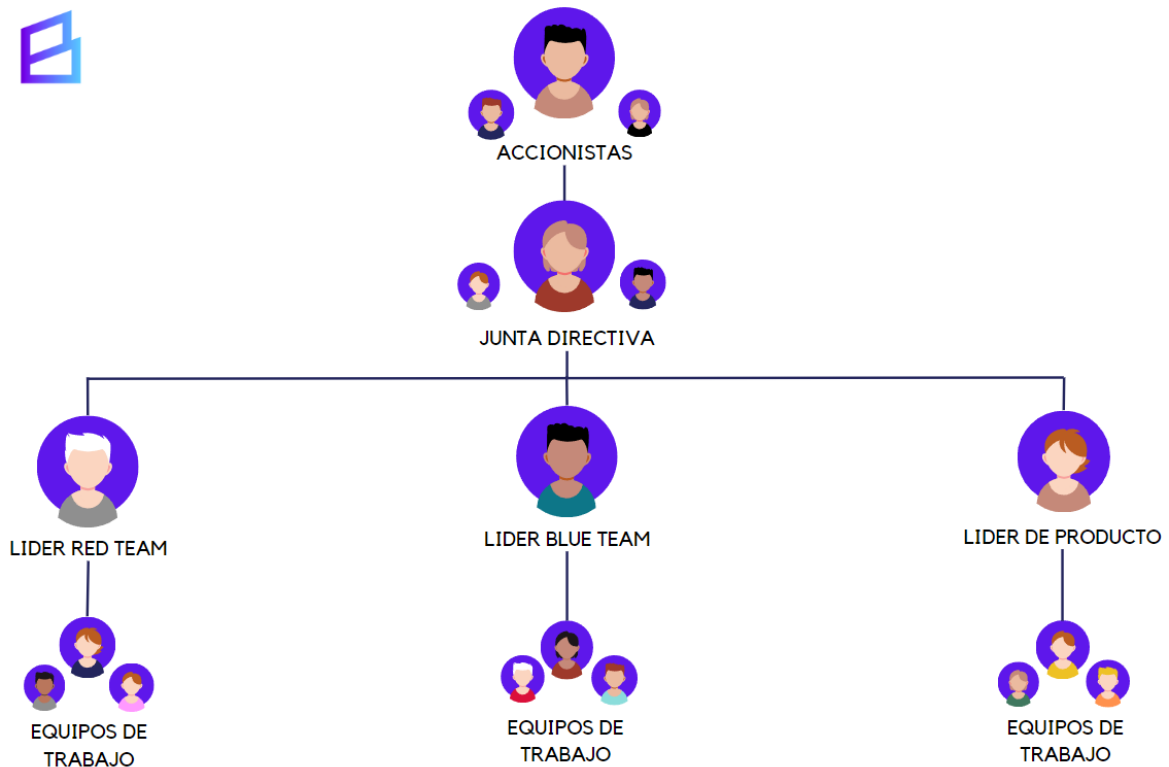
Cada empresa es única y presenta obligaciones fiscales particulares, por lo que contar con un experto en el campo es fundamental para manejar adecuadamente estas obligaciones. Además, aparte de los impuestos mencionados anteriormente, las empresas también tienen otras responsabilidades, como la presentación de Información Exógena, la entrega de Medios Magnéticos, el uso de la Nómina Electrónica, la obligación de llevar una contabilidad adecuada y, en algunos casos, contar con un Revisor Fiscal.

Por tanto, es importante tener en cuenta todas estas obligaciones y evitar incurrir en multas que podrían afectar las utilidades de la empresa. Contar con él profesional adecuado en temas fiscales puede ayudar una gestión óptima de todas las normativas legales. Esto no solo ayuda a evitar sanciones, sino que también contribuye a una administración financiera eficiente.

5.3 Estructura Organizacional

La **Ilustración 31** muestra el organigrama propuesto para Beef Up Tech, donde es importante establecer una estructura sólida que defina claramente cómo se organiza la empresa, a fin de determinar las actividades clave que cada equipo llevará a cabo para alcanzar los objetivos establecidos. El tener un organigrama bien definido, facilitará la asignación de responsabilidades y roles dentro de la organización.

Ilustración 31: Organigrama



Fuente: Diseño propio

5.3.1 Accionistas

En primer lugar, la empresa contará con un único accionista, quien asumirá la responsabilidad de proporcionar o conseguir el capital inicial para el emprendimiento y darle un rumbo, este será la persona que posea el 100% de las acciones y tenga autoridad sobre las decisiones de la empresa. Sin embargo, la empresa estará abierta a nuevas oportunidades para que otras personas interesadas puedan invertir y contribuir al crecimiento de Beef Up Tech. En este caso, se reserva el 100% de las acciones de la empresa para su fundador, Jonathan Andrés Guerrero.

5.3.2 Junta Directiva

La junta directiva estará conformada por el CEO, el CTO y otros líderes clave, quienes trabajarán en conjunto con el o los accionistas para tomar las mejores decisiones que impulsen el cumplimiento de los objetivos de la empresa, esta estructura asegurará que se mantenga el rumbo trazado. La participación de estos líderes en la junta directiva garantiza una amplia perspectiva y experiencia en la toma de decisiones estratégicas, lo que fortalecerá el éxito y el crecimiento de la empresa.

5.3.3 Líderes de Equipo

Dentro de los líderes de equipo o departamentos, encontraremos a personas encargadas de liderar áreas específicas en busca de alcanzar los objetivos de la empresa, tomando en consideración el valioso feedback de los clientes. Estos líderes trabajarán de manera colaborativa para satisfacer las necesidades del mercado y de los clientes, asegurando un enfoque integral y coordinado hacia el éxito de la empresa. En un inicio, se contará con tres líderes:

- El líder de equipo Red Team: Responsable de gestionar todo lo relacionado con la seguridad ofensiva.
- El líder de equipo Blue Team: Encargado de la seguridad defensiva.
- El líder de producto: Evaluará el desempeño de las campañas de marketing, y también tomará en cuenta todo el feedback recopilado por los clientes.

5.3.4 Equipos de Trabajo

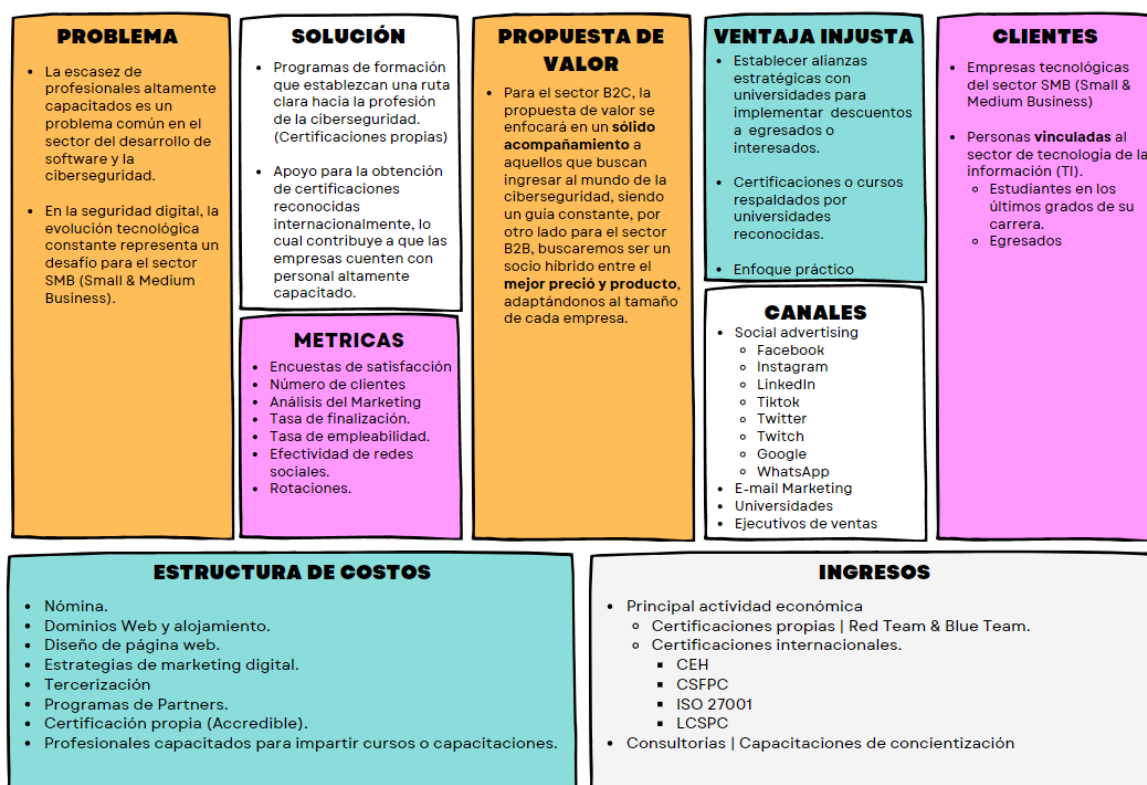
Dentro de los equipos de trabajo, se encontrarán las personas encargadas de brindar apoyo a los líderes de equipo, estos miembros contarán con habilidades específicas y serán responsables de determinar cuándo es necesario incorporar a otra persona al equipo. Sin embargo, cualquier decisión de este tipo deberá contar con la aprobación tanto de los líderes de equipo como de la junta directiva, esta medida asegurará que las adiciones al equipo sean estratégicas y estén alineadas con los objetivos de la empresa.

Capítulo 6 | Modelo Lean Canvas

6. Modelo Lean Canvas

Este capítulo abordará en detalle el enfoque del modelo Lean Canvas, el cual se centra en el ámbito del emprendimiento. Este modelo se caracteriza por su enfoque en la validación ágil de modelos de negocio, a diferencia del enfoque convencional del modelo Canvas que se orienta más hacia empresas consolidadas [116]. Para el caso específico de Beef Up Tech, como emprendimiento, utilizará el modelo Lean Canvas para agilizar y validar rápidamente la idea de negocio. Los resultados de este proceso podrán observarse en la **Ilustración 32**.

Ilustración 32: Modelo Lean Canvas



Fuente: Diseño propio

6.1 Problema

A lo largo del capítulo 2, en el cual se aborda todo el **Estudio de Mercado** relacionado con el campo de la ciberseguridad, se pudo identificar una problemática significativa. Esta problemática se manifiesta principalmente en el sector SMB (Small & Medium Business), donde la evolución tecnológica constante representa un desafío considerable para este tipo de empresas.

Inicialmente, se consideraron diferentes servicios para abordar esta problemática, como la prestación de servicios SOC (Security Operations Center) o pruebas de vulnerabilidades en aplicaciones, entre otros. Sin embargo, se descubrió que implementar estas soluciones requiere de un conocimiento técnico avanzado y de una inversión considerable, tanto en términos de recursos financieros como de expertos.

Profundizando en la problemática real, se llegó a la conclusión de que la raíz del problema se encuentra en **la escasez de profesionales altamente capacitados en el campo de la ciberseguridad**. Esta carencia de talento especializado es un factor crítico que dificulta la protección efectiva de las pequeñas y medianas empresas frente a las amenazas digitales.

6.2 Solución

Con base a la problemática identificada, se ha planteado una solución que se aborda en el capítulo 4 del informe. Específicamente, en la sección 4.4 donde se plantea **la implementación de programas de certificación** que establezcan una ruta clara hacia la profesión de la ciberseguridad y refuerce a los profesionales del sector. En esta idea no solo se ofrecerán certificaciones propias, sino que también **se brindara apoyo a las certificaciones existentes** en el mercado que cuenten ya con un reconocimiento.

El objetivo principal de estos programas de certificación es **proporcionar un apoyo a los profesionales interesados en ingresar al campo de la ciberseguridad**. A través de una estructura bien definida los participantes podrán adquirir los conocimientos y habilidades necesarias para desempeñarse eficientemente en el campo de la ciberseguridad. Esta idea representa una oportunidad significativa para impulsar el desarrollo del talento en el campo de la ciberseguridad.

6.3 Propuesta de Valor

Según una teoría del MIT (Massachusetts Institute of Technology), existen algunas propuestas de valor significativas. La primera opción radica en destacar como la mejor alternativa en términos de precio o producto, o incluso siendo un híbrido que equilibre ambas ventajas. Otra opción consiste en enfocarse en el cliente y brindar soluciones integrales, o bien, posicionarse como el integrador del ecosistema [117].

En el caso específico de Beef Up Tech, se ha decidido adoptar la propuesta de valor de ser el integrador del ecosistema, poniendo un fuerte énfasis en satisfacer las necesidades de nuestros clientes. Nuestra propuesta se basa en **brindar un acompañamiento activo** que permita diseñar y guiar un ecosistema confiable y seguro en los entornos digitales.

Para el sector B2C, la propuesta de valor se enfocará **en un sólido acompañamiento** a aquellos que buscan ingresar al mundo de la ciberseguridad, siendo un guía constante, por otro lado para el sector B2B, buscaremos ser un socio híbrido entre **el mejor precio y producto**, adaptándonos al tamaño de cada empresa, en ambos casos, buscamos ser un socio **confiable y comprometido en la protección y fortalecimiento de la seguridad digital** de nuestros clientes.

6.4 Ventaja Injusta

En el modelo Lean Canvas, la "ventaja injusta" se refiere a una ventaja competitiva que es muy difícil de copiar por los competidores. En el caso de Beef Up Tech, hemos identificado una lista de ventajas que consideramos pueden generar una ventaja competitiva y hacer que los clientes prefieran nuestros servicios. A continuación, se detallan estas ventajas:

- Establecer alianzas estratégicas con universidades: Implementar descuentos especiales para egresados o interesados en formación académica, brindando a nuestros clientes acceso privilegiado a programas de certificación en ciberseguridad.
- Certificaciones o cursos respaldados por universidades reconocidas: Ofrecer certificaciones y cursos en ciberseguridad respaldados por instituciones educativas de renombre, lo que brinda mayor validez y prestigio a las credenciales obtenidas por nuestros clientes.
- Enfoque práctico: Diseñar las certificaciones que se centren en la práctica constante. "Nuestro cerebro retiene el 10% de lo que lee, el 20% de lo que oye y el 90% de lo que experimenta". Por lo tanto, nos enfocamos en proporcionar a los interesados la oportunidad de practicar y experimentar activamente los conocimientos y habilidades de ciberseguridad.

6.5 Clientes

Nuestros servicios de certificación en ciberseguridad están dirigidos tanto a empresas de pequeño y mediano tamaño que desean fortalecer a sus colaboradores y medidas de seguridad digital, como a todas aquellas personas que deseen adentrarse en el campo de la ciberseguridad y no sepan por dónde empezar. Nuestros programas de certificación están diseñados para capacitar y actualizar las habilidades, sin importar su nivel de experiencia previa. A continuación, describimos los segmentos de clientes a los que nos dirigimos:

1. Empresas tecnológicas del sector SMB (Small & Medium Business): ofrecer programas de certificación específicos, y soluciones adaptadas a sus recursos y objetivos.
2. Personas vinculadas al sector de tecnología de la información (TI):
 - Estudiantes en los últimos grados de su carrera: Nos dirigimos a aquellos estudiantes que están finalizando sus estudios en carreras relacionadas con TI y desean complementar su formación académica con certificaciones en ciberseguridad para aumentar sus oportunidades laborales.
 - Egresados: Nuestros programas de certificación en ciberseguridad también están diseñados para egresados que deseen actualizar sus conocimientos y habilidades en el campo de la seguridad informática para avanzar en sus carreras profesionales.

6.6 Canales

Para los canales comunicación se usarán las redes sociales más populares como Facebook, Instagram, LinkedIn, TikTok, Twitter y Twitch, aprovechando su amplio alcance y capacidad para llegar a diferentes segmentos de público. Mediante contenido atractivo y estratégico, se creará una presencia sólida en estas redes, interactuando con los usuarios y promoviendo nuestras certificaciones en ciberseguridad. Además, se usará el e-mail marketing para mantener una relación cercana con los potenciales clientes, enviando información relevante y promociones exclusivas.

La página web será un elemento importante en la presencia digital de la empresa. En ella, se encontrará la información principal y relevante sobre todos los servicios de certificación en ciberseguridad, incluyendo detalles sobre las certificaciones que

ofrecemos, las características de nuestros planes, los diferentes medios de contacto y una sección de preguntas frecuentes.

Además de la página web, se creará un blog y un canal de YouTube que complementarán los canales de comunicación. El objetivo del blog será dar a conocer datos relevantes sobre los ciberdelitos, las consecuencias de los ciberataques, los ciberataques más comunes y cualquier otro tipo de información relacionada con la ciberseguridad esto con el fin de resaltar la importancia que tiene esta en las empresas actuales.

Para la estrategia de medios audiovisuales, se aprovechará plataformas clave como YouTube, TikTok y Twitch. Estos canales permitirán brindar información de interés sobre ciberseguridad y compartir datos relevantes con la audiencia. YouTube se convertirá en un canal principal, donde se compartirá contenido educativo, tutoriales y consejos relacionados con la ciberseguridad. Esta plataforma permitirá llegar a un amplio público y proporcionarles recursos visuales de calidad.

TikTok es una plataforma popular entre las generaciones más jóvenes, por lo cual se usará para transmitir mensajes cortos y atractivos sobre la importancia de la ciberseguridad. Para el caso de Twitch, se ha destacado como una de las mejores formas de interactuar con la comunidad en tiempo real, esta se implementará para organizar transmisiones en vivo y crear un ambiente cercano con la audiencia. Esto permitirá establecer una conexión más estrecha con la comunidad y generar mayor tracción hacia nuestras certificaciones.

Para ampliar nuestra visibilidad en el sector B2B y llegar a un público más amplio, implementaremos una estrategia adicional que involucra la incorporación de un ejecutivo de ventas, este ejecutivo desempeñará un papel clave en la promoción de nuestras certificaciones, en donde podría beneficiarse con una comisión del 3,49% sobre el margen de contribución. Para obtener esta comisión, es importante aclarar que las ventas logradas deben ser consignadas directamente en la cuenta de la empresa.

6.7 Métricas

Para las métricas, se reconocerá la importancia de contar con un sistema de medición adecuado que permita identificar qué aspectos están funcionando de manera

efectiva y tomar decisiones basadas en datos concretos. Para evaluar el desempeño y el impacto de nuestras certificaciones en ciberseguridad, se ha identificado una serie de métricas clave que proporcionarán una visión de nuestro progreso y permitirán realizar ajustes estratégicos cuando sea necesario.

- Encuestas de satisfacción: Se realizarán encuestas para recopilar la retroalimentación de nuestros clientes, evaluando su nivel de satisfacción con la certificación elegida. Esto permitirá identificar áreas de mejora y asegurarnos de brindar una experiencia de alta calidad.
- Número de clientes: Se Medirá el crecimiento y la evolución de nuestra base de clientes, monitoreando el aumento en el número de personas y empresas que optan por nuestras certificaciones en ciberseguridad. Esto nos ayudará a evaluar la aceptación y la demanda de nuestros servicios.
- Análisis del marketing: Se realizará un seguimiento detallado de nuestras estrategias de marketing para evaluar su efectividad. Esto incluirá el análisis de las campañas publicitarias, interacciones en redes sociales y tasas de conversión, lo que lo permitirá optimizar nuestras acciones de promoción.
- Tasa de empleabilidad: Se rastreará las personas que con nuestras certificaciones logren obtener empleo o mejorar sus oportunidades laborales en el campo de la ciberseguridad. Esto nos permitirá evaluar el impacto de nuestras certificaciones en la empleabilidad.
- Tasa de abandono: Se medirá la cantidad de participantes que abandonan las certificaciones antes de completarlas. Esto nos proporcionará información sobre posibles puntos débiles en nuestros programas y ayudará a realizar mejoras para aumentar la retención y finalización.
- Rotaciones: Mediremos la frecuencia con la que se adquiere una certificación para determinar cuándo volver a ofrecer cada una. Esto permitirá programar las ofertas de manera óptima y garantizar que nuestros estudiantes puedan acceder a los cursos en momentos relevantes para ellos.

6.8 Costos

Definir claramente los costos es esencial para la sostenibilidad de un emprendimiento, ya que permite tener una visión precisa de los gastos mensuales necesarios para mantener y hacer crecer el negocio. Identificar y analizar detalladamente

los costos operativos, de producción y administrativos ayuda a establecer prioridades, asignar recursos de manera eficiente y tomar decisiones informadas. Esta comprensión clara de los costos proporciona una base sólida para la planificación financiera y la toma de decisiones estratégicas.

6.8.1 Dominio y Hosting

En la búsqueda de una opción adecuada para el hosting y dominio de la página web, se considerando diferentes proveedores como Microsoft, AWS, GoDaddy, Hostinger, SiteGround y HostGator. Se analizaron criterios como el precio, la calidad y los servicios ofrecidos, donde después de evaluar cada opción, se decidió seleccionar Hostinger debido a su relación costo-beneficio, prestaciones y facilidad para lanzar rápidamente un Producto Mínimo Viable (MVP).

Se eligió el plan premium de Hostinger, **que tiene un costo mensual de 39.900 pesos y el dominio anual de 478.000 pesos**. Esta opción proporciona el dominio, el hosting y el correo corporativo necesarios para respaldar de manera efectiva nuestra presencia en línea, además se tienen todos los elementos esenciales para establecer y gestionar el sitio web de manera eficiente y profesional.

6.8.2 Tercerización

Para lograr una mayor eficiencia y enfoque en el core de nuestra actividad principal, resulta fundamental reconocer que habrá ocasiones en las que será beneficioso y estratégico tercerizar ciertas funciones o tareas. La tercerización puede proporcionar beneficios importantes, como la reducción de costos operativos, la flexibilidad para adaptarse a cambios en el mercado, y el acceso a tecnologías y conocimientos especializados.

6.8.2.1 Contabilidad y Facturación Electrónica

Para el manejo de la contabilidad y la facturación electrónica, se ha investigado diversas opciones de software que pueden brindar el acompañamiento necesario. **Entre las alternativas consideradas se encuentran Loggro+, Zen Smart, Siigo y Alegra.** Estos softwares contables ofrecen la funcionalidad de emitir facturas electrónicas y

también proporcionan la posibilidad de gestionar la nómina electrónica, un requisito obligatorio para las empresas en Colombia.

En cuanto a la elección del software contable, se dejará a disposición de la persona o empresa contratada en su momento. No obstante, se presentarán dos opciones: Siigo y Alegra. Ambas alternativas ofrecen funcionalidades adecuadas para el cumplimiento de las obligaciones fiscales, en donde se ha estimado un costo promedio **mensual para la suscripción de 80.000 pesos**, el cual podría variar en función del crecimiento del emprendimiento. Con estas opciones de software y con el asesoramiento adecuado, la empresa estará preparada para cumplir con las obligaciones fiscales, llevar una gestión contable eficiente y mantener el cumplimiento de la normativa legal vigente.

6.8.2.2 Credenciales Digitales

Al igual que grandes empresas como Microsoft, Google y Cisco, entre otras, Beef Up Tech otorgará certificaciones en colaboración con terceros, lo que permitirá un mayor crecimiento y credibilidad para aquellos interesados en obtener certificaciones relacionadas el sector de la ciberseguridad. En el mercado actual de credenciales digitales, existen dos plataformas líderes: Credly y su competidor Accredible.

Ambas son opciones válidas, pero presentan diferencias significativas. Credly es más reconocida, aunque establecer una alianza con ellos puede implicar ciertos requisitos que dificultan la entrada al mercado de forma sencilla. Por otro lado, Accredible es un poco más costosa, pero ofrece diversos beneficios, como la entrega no solo de insignias sino también de credenciales digitales, y su proceso de alianza es más accesible.

Debido a estas consideraciones, se ha decidido optar por **Accredible, cuyo plan más básico tiene un costo inicial de 960 dólares al año** el cual permite entregar 1000 credenciales. Sin embargo, a medida que la empresa experimente un crecimiento positivo, se podrán explorar opciones de planes más avanzados con Accredible, que incluyen beneficios como la integración con el dominio propio, múltiples integraciones, branding personalizado, entre otros.

6.8.3 Estrategia de Marketing

Para la estrategia de marketing de Beef Up Tech, se implementará una estrategia inicial basada en servicios gratuitos, aprovechando herramientas como HubSpot para probar diferentes funcionalidades y determinar la opción más adecuada. HubSpot ofrece un servicio de CRM gratuito que nos permitirá gestionar y organizar nuestras relaciones con los clientes de manera efectiva.

Además, se tendrá que crear contenido valioso para establecer una presencia sólida en las redes sociales y generar interés en nuestra audiencia objetivo. Este contenido será posteriormente promocionado a través de los anuncios en las mismas plataformas de redes sociales, aprovechando su capacidad de segmentación y alcance. Para esta estrategia se asignará un **presupuesto mensual de 2.000.000 pesos** para las campañas publicitarias en las redes sociales. Dicho presupuesto se utilizará para determinar y gestionar el gasto en cada plataforma, ya que cada una tiene precios específicos por campaña.

6.8.4 Pasarela de pagos

Es importante tener en cuenta que, al ser un emprendimiento completamente digital, las transacciones financieras se llevarán a cabo principalmente a través de canales digitales, como transferencias bancarias y pasarelas de pago. Sin embargo, en la actualidad, a las personas les gusta realizar pagos utilizando sus tarjetas de crédito o débito en sitios web. Por esta razón, es fundamental contar con una pasarela de pagos en nuestro sitio web que permita a los clientes pagar de manera segura y conveniente.

Para seleccionar la mejor opción, investigamos diferentes plataformas de pago, como Womppi de Bancolombia, PayU, Stripe, Adyen y Mercado Pago. Después de evaluar cada una de ellas y considerar sus tarifas, Stripe parecía ser la mejor opción. Sin embargo, dado que Stripe no opera en Colombia, optamos por la siguiente alternativa en la lista, que es PayU. Esta plataforma es fácil de integrar, tiene cobertura en toda Latinoamérica y su implementación es sencilla.

Inicialmente, se ha seleccionado el plan Starter para comenzar con la implementación de pagos a través de PayU. Este plan aplica **una comisión del 3,49% sobre el monto de cada transacción**, además de una **tarifa fija de 800 pesos**. Es

importante tener en cuenta que la comisión por venta en PayU estará directamente relacionada con el precio que se establezca para las certificaciones.

6.8.5 Programas de Partners

Como se mencionó en el capítulo 4, en la sección 4.4.4, se ha establecido una alianza estratégica con CertiProf para complementar las certificaciones en el campo de la ciberseguridad. Este programa de Partners implica un **costo de 200 USD** y tiene una duración de un año a partir de la fecha de compra. Al unirnos a CertiProf, accederemos a una serie de beneficios por ser Partners.

Entre los beneficios que otorga CertiProf se encuentran el acceso completo a todo el material disponible tanto para los aspirantes como para los profesores, lo que permitirá contar con recursos de alta calidad y actualizados para ofrecer una formación sólida y completa en ciberseguridad. Además, se ofrecen vouchers de examen con precios más económicos, lo que nos permitirá obtener un margen de ganancia en cada una de las certificaciones.

6.8.6 Nomina

Para garantizar el crecimiento del emprendimiento, es importante tener en cuenta los costos fijos, entre los cuales se encuentra la nómina destinada a apoyar el equipo de trabajo. Inicialmente, se establecerá la nómina en el Salario Mínimo Legal Vigente (SMLV). Sin embargo, es importante tener en cuenta que, aunque se pague el SMLV a un colaborador, al empleador le supone un costo adicional debido a conceptos como el auxilio de transporte, aportes parafiscales, seguridad social y prestaciones sociales. Estos factores implican un gasto mayor para el empleador, ya que cuanto mayor sea el salario devengado por el colaborador, más dinero costará tenerlo en la nómina de la empresa.

Inicialmente se seleccionarán cuatro colaboradores que acepten trabajar con el Salario Mínimo Legal Vigente (SMLV) más todos los beneficios establecidos por ley. Una de las principales ventajas será que el trabajo se realizará de forma totalmente remota, lo que evitará que los colaboradores tengan que desplazarse, ahorrándoles así mucho tiempo y costos de transporte. Es importante tener en cuenta este salario, ya que para

poder aplicar al fondo emprender, no es posible establecer una remuneración económica más alta. En la **Tabla 8** puede observar el costo de un trabajador para el empleador.

Tabla 8: Costo de un colaborador con SMLV 2023

Costo de un colaborador con salario mínimo 2023	
Salario mínimo	\$ 1.160.000
Auxilio de transporte	\$ 140.606
Total	\$ 1.300.606
Aportes parafiscales	
Sena (2 %)	\$ 23.200
ICBF (3 %)	\$ 34.800
Caja de compensación (4 %)	\$ 46.400
Total parafiscales	\$ 104.400
Seguridad social	
Salud (8,5 %)	\$ 98.600
Pensión (12 %)	\$ 139.200
ARL (0,522 %) Riesgo I	\$ 6.055
Total seguridad social	\$ 243.855
Prestaciones sociales	
Prima de servicios	\$ 108.384
Auxilio de cesantías	\$ 108.384
Intereses sobre cesantías	\$ 13.006
Vacaciones	\$ 48.372
Total prestaciones sociales	\$ 278.146
Costo total mensual	\$ 1.927.007

Fuente: Creación propia con base en datos de Actualícese [118]

6.8.7 Costos Variables

Además de los costos fijos, es importante tener en cuenta los costos variables, los cuales varían en función del volumen de ventas, esto significa que a medida que aumenten las ventas, los costos variables también se incrementarán. En el caso de Beef Up Tech, los costos variables estarán determinados por la cantidad de personas que adquieran una certificación, ya sea propia de la empresa o en colaboración con CertiProf.

Además, es importante tener en cuenta que los costos variables también estarán relacionados con el tipo de certificación que se elija y de la cantidad de estudiantes inscritos en cada una. Cuanto mayor sea el número de estudiantes, menor será el aporte individual que cada uno debe realizar para cubrir los costos. Por otro lado, si el número de estudiantes es menor, cada uno deberá hacer un aporte mayor, lo que podría implicar un aumento en el precio de la certificación. En el capítulo 7, se proporciona una descripción detallada de los costos variables asociados a cada una de las certificaciones que se ofrecerán inicialmente.

6.9 Ingresos

Los ingresos son fundamentales para garantizar la sostenibilidad y rentabilidad de la empresa, ya que representan el flujo de efectivo que ingresa gracias a todas las actividades económicas desarrolladas. Estos ingresos están disponibles antes de que se resten los gastos, por lo que es crucial contar con un buen margen de contribución en cada una de las certificaciones que se van a ofertar.

El margen de contribución es la diferencia entre los ingresos generados por una certificación y los costos variables asociados a ella. Es esencial que este margen sea suficiente para cubrir tanto los gastos fijos como los gastos variables, ya que esto garantizará que los ingresos generados sean capaces de respaldar y mantener todas nuestras operaciones. Además de garantizar la sostenibilidad financiera y rentabilidad de la empresa, los ingresos generados brindan la oportunidad de reinvertir en el crecimiento tanto de la empresa como de los colaboradores.

6.9.1 Certificaciones

La entrega de certificaciones será una de las principales fuentes de ingresos para el emprendimiento. Esto permitirá a los interesados obtener certificaciones en diversas áreas de la ciberseguridad, lo cual es una necesidad creciente en el mercado. Es importante destacar que este programa de certificaciones no solo estará disponible para el público en general (B2C), sino que también habrá oportunidades de colaboración con empresas interesadas en capacitar a sus propios empleados (B2B).

Establecer alianzas estratégicas con empresas será una estrategia clave para permitirles seleccionar las certificaciones más adecuadas para sus colaboradores. Esto

ofrece un beneficio mutuo, ya que las empresas podrán brindar formación especializada a sus equipos, fortaleciendo así sus capacidades en ciberseguridad y ayudando así a construir un ecosistema digital más seguro.

6.9.2 Programas de Partners

La creación de un programa de Partners será otra de las fuentes de ingresos para el emprendimiento, donde el programa estará dirigido a empresas y emprendedores que deseen contribuir a la creación de ecosistemas digitales más seguros, además de obtener nuestras certificaciones a un precio más económico. A través de esta iniciativa, se les ofrecerá la oportunidad de revender nuestras certificaciones, generando así una ganancia mutua.

Las membresías del programa de Partners podrán ser gestionadas de manera anual o mensual, brindando a los participantes acceso a todo el material de las certificaciones. Además, se les proporcionará un logo distintivo que los identificará como Partners de Beef Up Tech. Esto les permitirá destacar en el mercado y transmitir a sus clientes y colaboradores su compromiso con la ciberseguridad. En la **Ilustración 33** se muestra la insignia BCAP, la cual servirá como distintivo para identificar a todos los colaboradores que se convertirán en Partners de Beef Up Tech.

Ilustración 33: Beef Up Tech Certified Authorized Partner



Fuente: Diseño propio

6.10 Factor de innovación

Aunque el modelo Lean Canvas no aborda específicamente un factor de innovación, es importante tener en cuenta que toda empresa o emprendimiento debe buscar la innovación para mantener sus ventas y no quedarse rezagado frente a la competencia. A pesar de que inicialmente nos centraremos en impartir certificaciones relacionadas con la ciberseguridad, es importante tener una visión a largo plazo en la que podamos expandir nuestros servicios y ofrecer soluciones adicionales a las empresas.

Conforme se adquiera experiencia en el sector de la ciberseguridad, el objetivo será ampliar el catálogo de servicios más allá de las capacitaciones. Esto incluiría servicios como análisis de vulnerabilidades, consultorías, implementación de un SOC (Security Operation Center), análisis forense y otros servicios que ayuden a las empresas a llevar a cabo una gestión de ciberseguridad más efectiva y reducir el riesgo de ataques.

La innovación será fundamental en este proceso, ya que permitirá estar a la vanguardia de las últimas tendencias tecnológicas en ciberseguridad, brindando soluciones actualizadas y relevantes a las empresas. La idea será seguir investigando, desarrollando nuevas capacidades y buscando formas innovadoras de abordar los desafíos que tienen las empresas en la seguridad digital.

Capítulo 7 | Estrategias Financieras

7. Estrategias Financieras

En este capítulo, se abordará todo lo referente a la parte financiera, que constituye un elemento vital en cualquier emprendimiento. Se analizará lo que corresponde a la gestión del dinero y las estrategias para el manejo del capital, así como la búsqueda de la rentabilidad del negocio. Uno de los aspectos cruciales será la determinación del capital inicial, necesario para dar inicio al proyecto empresarial, donde se determinará cómo alcanzar el punto de equilibrio y lograr un crecimiento sostenible. Además de la elaboración de una proyección financiera a 5 años que permita evaluar la viabilidad del negocio a lo largo del tiempo.

7.1 Variables Macroeconómicas

Para llevar a cabo una proyección financiera precisa y cercana a la realidad, resulta importante considerar las variables macroeconómicas que influyen en el comportamiento del mercado. Entre estas variables cruciales, prestaremos especial atención al Índice de Precios al Consumidor (IPC), el Producto Interno Bruto (PIB), la Tasa Representativa del Mercado (TRM) y además de definir un crecimiento global en ventas moderado para poder realizar la estimación de cuanto se vendería por año. En la **Tabla 9**, presentaremos de manera conservadora estos datos más el crecimiento del salario mínimo proyectado para una evaluación completa.

Tabla 9: Proyección de variables macroeconómicas

Variables macroeconómicas	2023	2024	2025	2026	2027
<i>IPC</i>	8,70%	5,00%	3,80%	3,60%	3,80%
<i>PIB</i>	0,70%	1,60%	2,50%	2,80%	2,80%
<i>TRM</i>	\$ 4.758	\$ 4.611	\$ 4.708	\$ 4.708	\$ 4.708
<i>IVA</i>	19%	19%	19%	19%	19%
<i>CRECIMIENTO DE VENTAS GLOBAL</i>	0%	3%	4%	5%	6%
<i>SALARIO MÍNIMO</i>	\$ 1.160.000	\$1.240.000	\$1.287.120	\$1.333.456	\$1.384.128
<i>AUXILIO DE TRANSPORTE</i>	\$ 140.606	\$ 147.636	\$ 153.246	\$ 158.763	\$ 164.796

Fuente: Creación propia

7.2 Estimación de Costos Operativos

En este apartado de costos operativos, se detallarán los gastos mínimos necesarios para mantener en funcionamiento la operación del emprendimiento. En la **Tabla 10** se observará una proyección detallada de estos costos, lo cual permitirá una visión clara de los gastos estimados en el tiempo, desde el primer año hasta el año 5. Esta proyección nos ayudará a tener una claridad sobre los puntos clave mínimos para la operación, asegurando una planificación sólida a lo largo de los 5 años.

Tabla 10: Proyección de costos operativos

Costos fijos	Año 1	Año 2	Año 3	Año 4	Año 5
<i>Hosting</i>	\$ 478.800	\$ 520.456	\$ 540.233	\$ 559.681	\$ 580.949
<i>Dominio</i>	\$ 50.400	\$ 54.785	\$ 56.867	\$ 58.914	\$ 61.153
<i>Servicios públicos</i>	\$ 2.160.000	\$ 2.347.920	\$ 2.437.141	\$ 2.524.878	\$ 2.620.823
<i>Teams, Correo, SharePoint</i>	\$ 428.220	\$ 465.475	\$ 483.163	\$ 500.557	\$ 519.578
<i>Plataforma Marketing Digital</i>	\$ 720.000	\$ 782.640	\$ 812.380	\$ 841.626	\$ 873.608
<i>Plataforma de Contabilidad</i>	\$ 960.000	\$ 1.043.520	\$ 1.083.174	\$ 1.122.168	\$ 1.164.810
<i>Certificados Accredible²¹</i>	\$ 4.567.680	\$ 4.965.068	\$ 5.153.741	\$ 5.339.275	\$ 5.542.168
<i>ATP CertiProf²²</i>	\$ 951.600	\$ 1.034.389	\$ 1.073.696	\$ 1.112.349	\$ 1.154.618
<i>Inversión Marketing</i>	\$24.000.000	\$26.088.000	\$27.079.344	\$28.054.200	\$29.120.260
<i>Asesoramiento Contador</i>	\$9.600.000	\$10.435.200	\$10.831.738	\$11.221.680	\$11.648.104
<i>Nomina</i>	\$92.496.336	\$97.121.153	\$100.811.757	\$104.440.980	\$108.409.737
Total	\$136.413.036	\$144.858.606	\$150.363.233	\$155.776.309	\$161.695.809

Fuente: Creación propia

Es importante tener en cuenta que estos costos están asociados a los cuatro colaboradores proyectados para los próximos 5 años. Si el emprendimiento experimenta un crecimiento exponencial, será necesario ajustar la proyección y los valores correspondientes. Es fundamental señalar que estos costos son aproximados y se han

²¹ Software de credenciales digitales

²² Membresía CertiProf

planteado de manera conservadora, destinando los recursos necesarios para mantener el emprendimiento en funcionamiento de manera adecuada.

7.3 Estimación de Costo Variables

En la **Tabla 11**, se presenta la proyección estimada de los costos variables para cada uno de los productos que se ofrecerán inicialmente. Los costos variables se refieren a aquellos que dependen directamente del número de personas que adquieran la certificación, en estos gastos se incluirán el costo de los servicios profesionales que brindarán la capacitación y el costo del examen, en caso de ser con Certiprof. Es importante considerar que, para iniciar una certificación con acompañamiento, sería ideal tener al menos 15 personas interesadas, de lo contrario se buscarán alianzas estratégicas para garantizar la satisfacción del cliente.

Tabla 11: Proyección de costos variables

Productos o servicios	Año 1	Año 2	Año 3	Año 4	Año 5
<i>Professional ISO/IEC 27001:2022 Lead Auditor (I27001LA)</i>	\$323.562	\$351.712	\$369.297	\$383.331	\$397.131
<i>Professional Cyber Security Foundation - CSFPC™</i>	\$323.562	\$351.712	\$369.297	\$383.331	\$397.131
<i>Professional Scrum Master Professional Certificate - SMPC®</i>	\$323.562	\$351.712	\$369.297	\$383.331	\$397.131
<i>Professional Lead Cybersecurity - LCSPC™</i>	\$323.562	\$351.712	\$369.297	\$383.331	\$397.131
<i>BCOSW: Beef Up Tech Certified Offensive Security Wireless</i>	\$166.666	\$181.166	\$190.224	\$197.453	\$204.561
<i>BCLSP: Beef Up Tech Certified Linux for Security Practitioners</i>	\$166.666	\$181.166	\$190.224	\$197.453	\$204.561
<i>BCEHA: Beef Up Tech Certified Ethical Hacker Analyst</i>	\$233.333	\$253.633	\$266.315	\$276.435	\$286.386
<i>BCAP: Beef Up Tech Certified Authorized Partner</i>	\$ 50.000	\$ 54.350	\$57.068	\$59.236	\$61.369
<i>BCOSW: Partners</i>	\$50.000	\$54.350	\$57.068	\$59.236	\$61.369
<i>BCLSP: Partners</i>	\$50.000	\$54.350	\$57.068	\$59.236	\$61.369
<i>BCEHA: Partners</i>	\$50.000	\$54.350	\$57.068	\$59.236	\$61.369

Fuente: Creación propia

7.4 Precios de Venta

A lo largo de los años, tanto los costos operativos como los costos variables irán aumentando. Para mantener un equilibrio en la balanza y garantizar una utilidad constante por cada certificación, es necesario que los precios de venta también se incrementen. En la **Tabla 12**, se detalla cómo estos precios aumentarán gradualmente durante el período de cinco años. Esto permitirá mantener la rentabilidad del negocio y asegurar que los ingresos sigan siendo adecuados en relación con los gastos.

Tabla 12: Precios de venta por año

Productos o servicios	Año 1	Año 2	Año 3	Año 4	Año 5
<i>Professional ISO/IEC 27001:2022 Lead Auditor (I27001LA)</i>	\$924.533	\$1.004.968	\$1.055.216	\$1.095.314	\$1.134.746
<i>Professional Cyber Security Foundation - CSFPC™</i>	\$924.533	\$1.004.968	\$1.055.216	\$1.095.314	\$1.134.746
<i>Professional Scrum Master Professional Certificate - SMPC®</i>	\$924.533	\$1.004.968	\$1.055.216	\$1.095.314	\$1.134.746
<i>Professional Lead Cybersecurity - LCSPC™</i>	\$924.533	\$1.004.968	\$1.055.216	\$1.095.314	\$1.134.746
<i>BCOSW: Beef Up Tech Certified Offensive Security Wireless</i>	\$476.190	\$517.619	\$ 543.499	\$ 564.152	\$584.462
<i>BCLSP: Beef Up Tech Certified Linux for Security Practitioners</i>	\$ 666.667	\$ 724.667	\$760.900	\$ 789.815	\$818.248
<i>BCEHA: Beef Up Tech Certified Ethical Hacker Analyst</i>	\$ 1.166.667	\$1.268.167	\$1.331.575	\$1.382.175	\$1.431.934
<i>BCAP: Beef Up Tech Certified Authorized Partner</i>	\$625.000	\$679.375	\$713.344	\$740.451	\$767.107
<i>BCOSW: Partners</i>	\$ 156.920	\$ 170.572	\$ 179.101	\$ 185.906	\$ 192.599
<i>BCLSP: Partners</i>	\$ 196.150	\$ 213.215	\$ 223.876	\$ 232.383	\$ 240.749
<i>BCEHA: Partners</i>	\$ 235.380	\$ 255.858	\$ 268.651	\$ 278.860	\$ 288.899

Fuente: Creación propia

7.5 Proyección de Ventas

Se buscado realizar una proyección de ventas mediante una estimación prudente y conservadora para los próximos años. La **Tabla 13** muestra el número de ventas proyectadas para cada certificación a lo largo de cinco años, esta proyección está en unidades de ventas y con un **crecimiento escalonado del 3% al 6%**. Este enfoque gradual busca asegurar una planificación realista y fundamentada en el aumento progresivo de las ventas en el futuro, donde en el peor de los casos, se estarán abriendo dos certificaciones al año, por cada una de las que se ofertan. Se espera que el crecimiento sea mayor, pero se plantea un escenario bastante conservador.

Tabla 13: Proyección de ventas en unidades

Productos o servicios	Año 1	Año 2	Año 3	Año 4	Año 5
<i>Professional ISO/IEC 27001:2022 Lead Auditor (I27001LA)</i>	35	36	37	39	42
<i>Professional Cyber Security Foundation - CSFPC™</i>	37	38	40	42	44
<i>Professional Scrum Master Professional Certificate - SMPC®</i>	53	55	57	60	63
<i>Professional Lead Cybersecurity - LCSPC™</i>	31	32	33	35	37
<i>BCOSW: Beef Up Tech Certified Offensive Security Wireless</i>	28	29	30	31	33
<i>BCLSP: Beef Up Tech Certified Linux for Security Practitioners</i>	26	27	28	29	31
<i>BCEHA: Beef Up Tech Certified Ethical Hacker Analyst</i>	29	30	31	33	35
<i>BCAP: Beef Up Tech Certified Authorized Partner</i>	12	12	13	13	14
<i>BCOSW: Partners</i>	51	53	55	57	61
<i>BCLSP: Partners</i>	40	41	43	45	48
<i>BCEHA: Partners</i>	56	58	60	63	67
Total	398	410	426	448	475

Fuente: Creación propia

7.6 Proyección de ingresos

Una vez que hemos obtenido las proyecciones de ventas esperadas para cada año y cada certificación que ofreceremos, podemos calcular los ingresos proyectados. En la **Tabla 14**, se presenta de manera detallada esta proyección de ingresos esperados para cada uno de los años. Esta tabla nos brinda una visión completa de cómo se espera que los ingresos se desarrollen a lo largo del tiempo.

Tabla 14: Proyección de ingresos

Productos o servicios	Año 1	Año 2	Año 3	Año 4	Año 5
<i>Professional ISO/IEC 27001:2022 Lead Auditor (I27001LA)</i>	\$32.358.667	\$36.229.087	\$39.562.163	\$43.118.801	\$47.351.343
<i>Professional Cyber Security Foundation - CSFPC™</i>	\$34.207.733	\$38.299.320	\$41.822.858	\$45.582.733	\$50.057.134
<i>Professional Scrum Master Certificate - SMPC®</i>	\$49.000.267	\$54.861.189	\$59.908.418	\$65.294.185	\$71.703.462
<i>Professional Lead Cybersecurity - LCSPC™</i>	\$28.660.533	\$32.088.620	\$35.040.773	\$38.190.938	\$41.939.761
<i>Beef Up Tech Certified Offensive Security Wireless</i>	\$13.333.320	\$14.928.118	\$16.301.505	\$17.767.011	\$19.511.020
<i>Beef Up Tech Certified Linux for Security Practitioners</i>	\$17.333.342	\$19.406.583	\$21.191.989	\$23.097.148	\$25.364.365
<i>Beef Up Tech Certified Ethical Hacker Analyst</i>	\$33.833.343	\$37.880.149	\$41.365.123	\$45.083.847	\$49.509.278
<i>BCAP: Beef Up Tech Certified Authorized Partner</i>	\$7.500.000	\$8.397.075	\$9.169.606	\$ 9.993.953	\$10.974.960
<i>BCOSW: Partners</i>	\$8.002.920	\$8.960.149	\$9.784.483	\$10.664.108	\$11.710.897
<i>BCLSP: Partners</i>	\$7.846.000	\$8.784.460	\$9.592.630	\$10.455.008	\$11.481.271
<i>BCEHA: Partners</i>	\$13.181.280	14.757.893	\$16.115.619	\$17.564.413	\$19.288.536
Total	≈\$245,257M	≈\$274,592M	≈\$299,855M	≈\$326,812M	≈\$358,892M

Fuente: Creación propia

7.7 Margen de contribución

El margen de contribución representa la diferencia entre los ingresos por ventas y los costos variables asociados a la producción o prestación de servicios este margen de contribución será un factor importante para asegurar la sostenibilidad del emprendimiento, donde siempre se buscará que el margen sea igual o superior al 60%. Al mantener un margen de contribución del 60% o más, la empresa podrá cubrir los costos fijos, generar ganancias y estar preparada para enfrentar desafíos económicos o imprevistos. En la **Tabla 15**, se puede observar el margen de contribución para cada una de las certificaciones.

Tabla 15: Margen de contribución

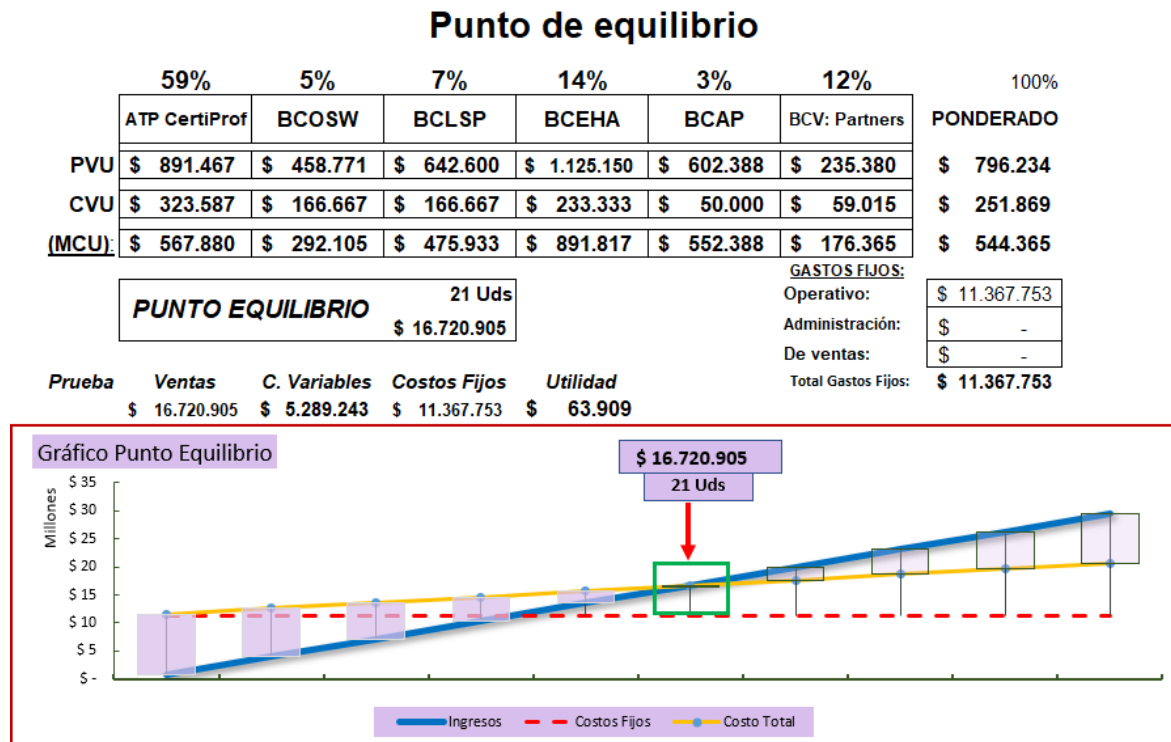
Productos o servicios	Precio de venta	Costo variable	Pasarela	M.C. \$	M.C. %
<i>Professional ISO/IEC 27001:2022 Lead Auditor (I27001LA)</i>	\$ 924.533	\$ 323.587	\$ 33.066	\$567.880	61,42%
<i>Professional Cyber Security Foundation - CSFPC™</i>	\$ 924.533	\$ 323.587	\$ 33.066	\$567.880	61,42%
<i>Professional Scrum Master Professional Certificate - SMPC®</i>	\$ 924.533	\$ 323.587	\$ 33.066	\$567.880	61,42%
<i>Professional Lead Cybersecurity - LCSPC™</i>	\$ 924.533	\$ 323.587	\$ 33.066	\$567.880	61,42%
<i>BCOSW: Beef Up Tech Certified Offensive Security Wireless</i>	\$ 476.190	\$ 166.666	\$ 17.419	\$292.105	61,34%
<i>BCLSP: Beef Up Tech Certified Linux for Security Practitioners</i>	\$ 666.667	\$ 166.666	\$ 24.067	\$475.934	71,39%
<i>BCEHA: Beef Up Tech Certified Ethical Hacker Analyst</i>	\$ 1.166.667	\$ 233.333	\$ 41.517	\$891.817	76,44%
<i>BCAP: Beef Up Tech Certified Authorized Partner</i>	\$ 625.000	\$ 50.000	\$ 22.613	\$552.388	88,38%
<i>BCOSW: Partners</i>	\$ 156.920	\$ 50.000	\$ 6.277	\$100.643	64,14%
<i>BCLSP: Partners</i>	\$ 196.150	\$ 50.000	\$ 7.646	\$138.504	70,61%
<i>BCEHA: Partners</i>	\$ 235.380	\$ 50.000	\$ 9.015	\$176.365	74,93%

Fuente: Creación propia

7.8 Punto de Equilibrio

Es importante considerar el punto de equilibrio al buscar obtener beneficios en un negocio., y para este caso no es la excepción, este punto se logra después de deducir los gastos operativos mensuales necesarios para el funcionamiento continuo del negocio. Una vez que este punto se supera, comienza a generarse rentabilidad. Para visualizar de manera más clara este concepto, la **Ilustración 34** representa el punto de equilibrio mensual recomendado.

Ilustración 34: Punto de equilibrio mensual



Fuente: Diseño propio

El cálculo del punto de equilibrio mensual se ha realizado mediante la asignación de porcentajes específicos que aporta cada certificación en el modelo de negocio. Dado que CertiProf inicialmente tiene un mayor reconocimiento en comparación con las certificaciones propias que serán impartidas, se le ha asignado el porcentaje más elevado en cuanto a la participación en las ventas del negocio. Este porcentaje se deriva de una evaluación de las ventas proyectadas, siendo las certificaciones de CertiProf las que representarán el 59% en dicha proyección y las certificaciones propias el 41%.

Asimismo, para alcanzar la rentabilidad a lo largo de los años, se presenta la **Tabla 16** que muestra el punto de equilibrio anual, evidenciando que en cada uno de los años las ventas proyectadas alcanzan a tocar el punto de equilibrio. Estos datos anuales proporcionan una visión más amplia de cómo el negocio debe mantenerse por encima del punto de equilibrio para lograr un rendimiento constante.

Tabla 16: Punto de equilibrio anual

Año	Ventas totales por año	Punto de equilibrio
<i>Año 1</i>	\$ 245.257.405	\$ 208.903.054
<i>Año 2</i>	\$ 274.592.643	\$ 221.641.576
<i>Año 3</i>	\$ 299.855.166	\$ 229.946.125
<i>Año 4</i>	\$ 326.812.146	\$ 237.108.467
<i>Año 5</i>	\$ 358.892.026	\$ 246.044.680

Fuente: Creación propia

7.9 Estado de resultados

La **Tabla 17** presenta la proyección de los resultados anuales, considerando el haber deducido los impuestos correspondientes. Aunque los beneficios anuales del negocio no alcancen los estándares típicos de una empresa tecnológica, es crucial recordar que esta simulación se desarrolla en un contexto altamente conservador.

Tabla 17: Estado de resultado por año

Concepto	Año 1	Año 2	Año 3	Año 4	Año 5
Ventas	\$ 245.257.405	\$ 274.592.643	\$ 299.855.166	\$ 326.812.146	\$ 358.892.026
Costos variables	\$ 74.196.141	\$ 83.070.741	\$ 90.713.250	\$ 98.868.371	\$ 108.573.290
Costos fijos de producción	\$ 43.916.700	\$ 47.737.453	\$ 49.551.476	\$ 51.335.329	\$ 53.286.072
Nómina de producción	\$ 92.519.674	\$ 97.145.657	\$ 100.837.192	\$ 104.467.331	\$ 108.437.090
Depreciación de producción	\$ 40.000	\$ 40.000	\$ 40.000	\$ 40.000	\$ 40.000
Utilidad bruta	\$ 34.584.890	\$ 46.598.792	\$ 58.713.248	\$ 72.101.115	\$ 88.555.575
Gastos de administración	\$ -	\$ -	\$ -	\$ -	\$ -
Nómina de administración	\$ -	\$ -	\$ -	\$ -	\$ -
Depreciación de administración	\$ 666.667	\$ 666.667	\$ 666.667	\$ 666.667	\$ 666.667
Gastos de ventas	\$ -	\$ -	\$ -	\$ -	\$ -
Nómina de ventas	\$ -	\$ -	\$ -	\$ -	\$ -
Comisión de ventas	\$ 8.559.483	\$ 9.583.283	\$ 10.464.945	\$ 11.405.744	\$ 12.525.332
Depreciación de ventas	\$ 1.000.000	\$ 1.000.000	\$ 1.000.000	\$ 1.000.000	\$ 1.000.000
Utilidad operacional	\$ 24.358.740	\$ 35.348.842	\$ 46.581.636	\$ 59.028.704	\$ 74.363.576
Gastos Financieros	\$ -	\$ -	\$ -	\$ -	\$ -
Utilidad antes de impuestos	\$ 24.358.740	\$ 35.348.842	\$ 46.581.636	\$ 59.028.704	\$ 74.363.576
Impuesto de Renta	\$ 8.525.559	\$ 12.372.095	\$ 16.303.573	\$ 20.660.046	\$ 26.027.252
Impuestos colchon	\$ 2.192.287	\$ 3.181.396	\$ 4.192.347	\$ 5.312.583	\$ 6.692.722
Utilidad neta	\$ 13.640.895	\$ 19.795.351	\$ 26.085.716	\$ 33.056.074	\$ 41.643.602

Fuente: Creación propia

7.10 Estrategia de Financiamiento

Uno de los puntos clave de cualquier emprendimiento es la obtención del capital necesario para operar durante los primeros meses o, en el mejor de los casos, durante el primer año, que suele ser el período más complicado. Para lograrlo, existen diversas estrategias, como invertir todos los ahorros en la idea, buscar financiamiento a través de inversionistas o bancos.

Luego de considerar varias opciones como, Apps.co, Innpulsa, Endeavor, entre otras, se ha tomado la decisión de elegir el Fondo Emprender como la primera alternativa, para financiar el emprendimiento. Este fondo ofrece recursos totalmente condonables a emprendedores que cumplan con el plan de empresa propuesto y alcancen los indicadores de ventas establecidos; en consecuencia, **el fondo Emprender se presenta como la mejor alternativa para obtener el capital necesario** y apoyar el crecimiento del emprendimiento.

7.11 Amortización de Crédito

Es importante destacar que este plan de negocio, no se considera viable la opción de adquirir un crédito para iniciar. En su lugar, se ha decidido por aplicar al financiamiento a través de Fondo Emprender, buscando obtener los recursos condonables. En **Tabla 18** se presenta una posible simulación de préstamo con la entidad Finaktiva. En este escenario, se contempla la posibilidad de solicitar un **préstamo de \$140.000.000** a 36 meses con una tasa efectiva anual del 19,56% y una tasa mensual del 1,5%. Este préstamo estaría destinado a mantener la operación durante el primer año. Es importante señalar que dado el caso, se deberá incorporar como parte de los gastos operativos mensuales.

Tabla 18: Simulación de crédito

Mes	Cuota	Interés	Capital	Saldo
0				\$ 140.000.000
1	\$ 5.061.227	\$ 2.099.820	\$ 2.961.407	\$ 137.038.593
2	\$ 5.061.227	\$ 2.055.403	\$ 3.005.824	\$ 134.032.769
3	\$ 5.061.227	\$ 2.010.319	\$ 3.050.908	\$ 130.981.861
4	\$ 5.061.227	\$ 1.964.560	\$ 3.096.668	\$ 127.885.193
5	\$ 5.061.227	\$ 1.918.113	\$ 3.143.114	\$ 124.742.080
6	\$ 5.061.227	\$ 1.870.971	\$ 3.190.256	\$ 121.551.824
7	\$ 5.061.227	\$ 1.823.121	\$ 3.238.106	\$ 118.313.718

8	\$	5.061.227	\$ 1.774.554	\$ 3.286.673	\$ 115.027.044
9	\$	5.061.227	\$ 1.725.258	\$ 3.335.969	\$ 111.691.075
10	\$	5.061.227	\$ 1.675.223	\$ 3.386.004	\$ 108.305.071
11	\$	5.061.227	\$ 1.624.437	\$ 3.436.790	\$ 104.868.280
12	\$	5.061.227	\$ 1.572.889	\$ 3.488.338	\$ 101.379.943
13	\$	5.061.227	\$ 1.520.569	\$ 3.540.658	\$ 97.839.285
14	\$	5.061.227	\$ 1.467.463	\$ 3.593.764	\$ 94.245.521
15	\$	5.061.227	\$ 1.413.562	\$ 3.647.665	\$ 90.597.856
16	\$	5.061.227	\$ 1.358.851	\$ 3.702.376	\$ 86.895.480
17	\$	5.061.227	\$ 1.303.320	\$ 3.757.907	\$ 83.137.573
18	\$	5.061.227	\$ 1.246.957	\$ 3.814.270	\$ 79.323.303
19	\$	5.061.227	\$ 1.189.748	\$ 3.871.479	\$ 75.451.824
20	\$	5.061.227	\$ 1.131.680	\$ 3.929.547	\$ 71.522.277
21	\$	5.061.227	\$ 1.072.742	\$ 3.988.485	\$ 67.533.792
22	\$	5.061.227	\$ 1.012.920	\$ 4.048.307	\$ 63.485.485
23	\$	5.061.227	\$ 952.201	\$ 4.109.026	\$ 59.376.459
24	\$	5.061.227	\$ 890.571	\$ 4.170.656	\$ 55.205.802
25	\$	5.061.227	\$ 828.016	\$ 4.233.211	\$ 50.972.591
26	\$	5.061.227	\$ 764.523	\$ 4.296.704	\$ 46.675.888
27	\$	5.061.227	\$ 700.078	\$ 4.361.149	\$ 42.314.739
28	\$	5.061.227	\$ 634.667	\$ 4.426.560	\$ 37.888.179
29	\$	5.061.227	\$ 568.274	\$ 4.492.953	\$ 33.395.226
30	\$	5.061.227	\$ 500.885	\$ 4.560.342	\$ 28.834.884
31	\$	5.061.227	\$ 432.486	\$ 4.628.741	\$ 24.206.143
32	\$	5.061.227	\$ 363.061	\$ 4.698.166	\$ 19.507.977
33	\$	5.061.227	\$ 292.595	\$ 4.768.632	\$ 14.739.345
34	\$	5.061.227	\$ 221.071	\$ 4.840.156	\$ 9.899.189
35	\$	5.061.227	\$ 148.475	\$ 4.912.752	\$ 4.986.437
36	\$	5.061.227	\$ 74.790	\$ 4.986.437	\$ 0

Fuente: Creación propia

Capítulo Final | Conclusiones y Referencias

Conclusiones

A lo largo de los capítulos presentados, ha quedado claro que la industria de la ciberseguridad demanda ayuda. No solo se trata de proporcionar soluciones B2B, sino también de formar individuos capacitados para enfrentar cualquier eventualidad tanto en su vida personal como laboral. El estudio de mercado ha demostrado cómo los ciberdelincuentes afectan de manera significativa a todos los sectores de la industria. Ante este panorama, se pensaba un plan empresarial el cual ofreciera servicios especializados como análisis de vulnerabilidad, un Centro de Operaciones de Seguridad (SOC), ejercicios de phishing y otras propuestas que contribuyeran a la seguridad integral de cada empresa.

No obstante, la investigación reveló que llevar a cabo este tipo de iniciativas demanda un capital considerable y una experticia en el campo, experiencia con la cual aún no se cuenta y recursos de los cuales no se disponen. Fue entonces que me llamó la atención una frase encontrada en línea: "Enamórate del problema, no de la solución". Esta afirmación dio inicio a la exploración de nuevas perspectivas para abordar el verdadero desafío. Descubrí que más allá de brindar servicios de ciberseguridad, la verdadera necesidad radica en formar individuos apasionados por el sector, dotados de habilidades esenciales para gestionar cualquier tipo de incidente.

Este nuevo enfoque se torna altamente viable, ya que no requiere una inversión considerable para iniciar, y su potencial impacto en el sector es innegable. Al proveer a las personas con las habilidades y el interés necesarios para asumir un papel activo en la ciberseguridad, no solo se crea una solución más asequible, sino que también se contribuye de manera más efectiva a la protección digital.

Referencias

- [1] Semana, «Aumentan 605% ciberamenazas relacionadas con covid-19,» 07 Noviembre 2020. [En línea]. Available: <https://www.semana.com/tecnologia/articulo/cuanto-subieron-las-ciberamenazas-en-el-segundo-trimestre/305962/>. [Último acceso: 13 Diciembre 2022].
- [2] Kaspersky, «¿Qué es una brecha de seguridad?,» Kaspersky, sf. [En línea]. Available: <https://www.kaspersky.es/resource-center/threats/what-is-a-security-breach>. [Último acceso: 22 Diciembre 2022].
- [3] G. Berna, «Retos y recomendaciones de ciberseguridad para empresas,» Seguros Bolívar, 29 Julio 2020. [En línea]. Available: <https://www.segurosbolivar.com/blog/mundo-empresarial/retos-y-recomendaciones-de-ciberseguridad-para-empresas/>. [Último acceso: 13 Diciembre 2022].
- [4] Fortinet, «FortiGuard Labs presenta reporte de ciberataques en América Latina,» Fortinet, 2021. [En línea]. Available: <https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortiguards-labs-reporte-ciberataques-america-latina-2021>. [Último acceso: 13 Diciembre 2022].
- [5] OWASP , «OWASP Top Ten,» OWASP , 2022. [En línea]. Available: <https://owasp.org/www-project-top-ten/>. [Último acceso: 13 Diciembre 2022].
- [6] Profitline, «Actualmente Como se encuentra Colombia en Seguridad Informática,» Business Process Outsourcing - Profitline, 26 Febrero 2019. [En línea]. Available: <https://profitline.com.co/actualmente-como-se-encuentra-colombia-en-seguridad-informatica/>. [Último acceso: 13 Diciembre 2020].
- [7] Portafolio, «Aumentan en 30% los ataques cibernéticos en Colombia,» Portafolio, 8 Julio 2021. [En línea]. Available: <https://www.portafolio.co/tendencias/aumentan-en>

- 30-los-ataques-ciberneticos-en-colombia-553803. [Último acceso: 13 Diciembre 2022].
- [8] CCIT, «Tendencias cibercrimen Colombia 2019-2020,» Cámara Colombiana de Informática y Telecomunicaciones, 29 Octubre 2019. [En línea]. Available: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf. [Último acceso: 13 Diciembre 2022].
- [9] ACIS, «Lista de Empresas de Seguridad Informática en Colombia | ACIS,» ACIS, 2022. [En línea]. Available: <https://acis.org.co/portal/content/lista-de-empresas-de-seguridad-inform%C3%A1tica-en-colombia>. [Último acceso: 14 Diciembre 2022].
- [10] Empresite Colombia, «Desarrollo De Software en Colombia. Listado de empresas de Desarrollo De Software en Colombia,» Empresite Colombia, 2022. [En línea]. Available: <https://empresite.economistaamerica.co/Actividad/DESARROLLO-DE-SOFTWARE/>. [Último acceso: 15 Diciembre 2022].
- [11] La República, «La industria del software representa alrededor de US\$10.000 millones en Colombia,» Diario La República, 28 Marzo 2022. [En línea]. Available: <https://www.larepublica.co/internet-economy/la-industria-del-software-representa-alrededor-de-us-10-000-millones-en-colombia-3330546>. [Último acceso: 15 Diciembre 2022].
- [12] M. Jiménez, «Uber sufre un ataque informático: un 'hacker' de 18 años vulnera sus sistemas informáticos,» Cinco Días, 16 Septiembre 2022. [En línea]. Available: https://cincodias.elpais.com/cincodias/2022/09/16/companias/1663328711_079738.html. [Último acceso: 16 Diciembre 2022].
- [13] L. H. Newman, «The Uber Hack's Devastation Is Just Starting to Reveal Itself,» WIRED, 16 Septiembre 2022. [En línea]. Available: <https://www.wired.com/story/uber-hack-mfa-phishing/>. [Último acceso: 16 Diciembre 2022].
- [14] V. García, «Hackearon Twitch: revelan las ganancias millonarias de Ibai, Auronplay y Rubius,» 442, 6 Octubre 2021. [En línea]. Available: <https://442.perfil.com/noticias/noticias/hackearon-twitch-hackeo-masivo-a-su-base->

- de-datos-y-revelan-ganancias-millonarias-de-ibai-auronplay-rubius.phtml. [Último acceso: 16 Diciembre 2022].
- [15] LISA Institute, «Diferencia entre Ciberseguridad, Seguridad Informática y Seguridad de la Información,» LISA Institute, 3 Marzo 2021. [En línea]. Available: <https://www.lisainstitute.com/blogs/blog/diferencia-ciberseguridad-seguridad-informatica-seguridad-informacion>. [Último acceso: 20 Diciembre 2022].
- [16] Kaspersky, «¿Qué es la ciberseguridad?,» Kaspersky Latam, Diciembre 2021. [En línea]. Available: <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>. [Último acceso: 18 Diciembre 2022].
- [17] Centro de Estudios Superiores, «¿Qué hace un profesional de la ciberseguridad?,» Centro de Estudios Superiores, 4 Julio 2022. [En línea]. Available: <https://www.centroafuera.es/que-hace-un-profesional-de-la-ciberseguridad/>. [Último acceso: 18 Diciembre 2022].
- [18] Le VPN, «¿QUÉ ES LA CIBERSEGURIDAD? ¿CÓMO AFECTA NUESTRA VIDA PRIVADA?,» Le VPN, 22 Mayo 2018. [En línea]. Available: <https://www.le-vpn.com/es/ciberseguridad-afecta-vida-privada/>. [Último acceso: 18 Diciembre 2022].
- [19] Next Move Strategy Consulting, «Cyber Security Market Size, Share and Trends Analysis Report by Type (Enterprise, Consumer), Product (Security Consulting, Managed Service Providers, Identity and Access Management), Vertical, Enterprise Size, Region, and Segment Forecasts, 2021-2026,» Next Move Strategy Consulting, 2022. [En línea]. Available: <https://www.nextmsc.com/report/cyber-security-market>. [Último acceso: 18 Diciembre 2022].
- [20] Bit Life Media, «El mercado de ciberseguridad ingresará 334.000 millones en 2026,» Bit Life Media, 28 Septiembre 2022. [En línea]. Available: <https://bitlifemedia.com/2022/09/mercado-de-la-ciberseguridad/>. [Último acceso: 22 Diciembre 2022].

- [21] A. D. Aurenty, «Ciberseguridad: una industria en crecimiento,» BBVA, 22 Octubre 2021. [En línea]. Available: <https://www.bbva.ch/noticia/ciberseguridad-una-industria-en-crecimiento/>. [Último acceso: 22 Diciembre 2022].
- [22] Semana, «Este es el ‘malware’ que más está afectando la seguridad digital de las empresas,» Semana, 10 Diciembre 2022. [En línea]. Available: <https://www.semana.com/economia/empresas/articulo/este-es-el-malware-que-mas-esta-afectando-la-seguridad-digital-de-las-empresas/202214/>. [Último acceso: 22 Diciembre 2022].
- [23] Portafolio, «El 73% de las empresas en el mundo ha sufrido ciberataques,» Portafolio, 31 Agosto 2022. [En línea]. Available: <https://www.portafolio.co/economia/finanzas/ciberseguridad-el-73-de-las-empresas-en-el-mundo-ha-sufrido-ciberataques-570387>. [Último acceso: 25 Diciembre 2022].
- [24] WeLiveSecurity, «Ransomware como servicio (RaaS): qué es y cómo funciona este modelo,» WeLiveSecurity, 23 Febrero 2022. [En línea]. Available: <https://www.welivesecurity.com/la-es/2022/02/23/ransomware-as-a-service-raas-que-es-como-funciona/>. [Último acceso: 22 Diciembre 2022].
- [25] Cloudflare, «¿Qué es el ransomware como servicio (RaaS)?,» Cloudflare, 2021. [En línea]. Available: <https://www.cloudflare.com/es-es/learning/security/ransomware/ransomware-as-a-service/>. [Último acceso: 22 Diciembre 2022].
- [26] CyberSecure, «Panorama de Amenazas :: Primer Trimestre 2022,» CyberSecure, 2022. [En línea]. Available: https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1234/. [Último acceso: 22 Diciembre 2022].
- [27] P. R. M. S. Jeffrey Caso, «New survey reveals \$2 trillion market opportunity for cybersecurity technology and service providers,» McKinsey & Company, 27 Octubre 2022. [En línea]. Available: <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market->

- opportunity-for-cybersecurity-technology-and-service-providers. [Último acceso: 24 Diciembre 2022].
- [28] Grandviewresearch, «Cyber Security Services Market Size Report, 2021-2028,» Grandviewresearch, 2021. [En línea]. Available: <https://www.grandviewresearch.com/industry-analysis/cyber-security-service-market>. [Último acceso: 20 Diciembre 2022].
- [29] Itreseller, «Los ataques de malware sobre dispositivos IoT crecieron un 123% en 2022,» Itreseller, 30 Noviembre 2022. [En línea]. Available: <https://www.itreseller.es/seguridad/2022/11/los-ataques-de-malware-sobre-dispositivos-iot-crecieron-un-123-en-2022>. [Último acceso: 30 Diciembre 2022].
- [30] C. Luna, «Las amenazas de Ciberseguridad de las que el Software "Nx" permanece seguro,» Tecnoseguro, 25 Enero 2022. [En línea]. Available: <https://www.tecnoseguro.com/analisis/cctv/amenazas-ciberseguridad-software-nx-permanece-seguro>. [Último acceso: 12 Diciembre 2022].
- [31] IBM Security , «Informe del Coste de la vulneración de datos 2022,» IBM, 2022. [En línea]. Available: <https://www.ibm.com/downloads/cas/WOLL1DX3>. [Último acceso: 25 Diciembre 2022].
- [32] Computerworld, «El 80% de los ataques de 'phishing' tienen éxito,» Computerworld, 25 Abril 2022. [En línea]. Available: <https://cso.computerworld.es/cibercrimen/el-80-de-los-ataques-de-phishing-tienen-exito>. [Último acceso: 29 Diciembre 2022].
- [33] AAG IT Support, «The Latest 2022 Phishing Statistics,» AAG IT Services, 12 Diciembre 2022. [En línea]. Available: <https://aag-it.com/the-latest-2022-phishing-statistics-updated-october-2022/>. [Último acceso: 29 Diciembre 2022].
- [34] G. Mondaca, «36 Phishing Statistics in 2022: Don't Take the Bait!,» Eftsure, 17 Octubre 2022. [En línea]. Available: <https://get.eftsure.com.au/statistics/phishing-statistics-2022/>. [Último acceso: 25 Diciembre 2022].
- [35] ICEX España, «Ciberseguridad,» ICEX España, 2021. [En línea]. Available: <https://www.emarketservices.es/emarketservices/ProcesarDescarga?dDocName=>

DOC2021893645&urlIsesion=/emarketservices/es/mi-cuenta/inicio-sesion/index.html?. [Último acceso: 20 Diciembre 2020].

- [36] CCIT, «Estudio trimestral: Ciberseguridad en redes de telecomunicaciones móviles,» CCIT - Cámara Colombiana de Informática y Telecomunicaciones, 18 Noviembre 2022. [En línea]. Available: <https://www.ccit.org.co/wp-content/uploads/ciberseguridad-en-redes-de-tel-2022-2.pdf>. [Último acceso: 30 Diciembre 2022].
- [37] ACIS, «Más de 7 billones de intentos de ciberataques afectaron a Colombia en 2020 | ACIS,» ACIS, 2020. [En línea]. Available: <https://acis.org.co/portal/content/noticiisdelsector/m%C3%A1s-de-7-billones-de-intentos-de-ciberataques-afectaron-colombia-en-2020>. [Último acceso: 30 Diciembre 2022].
- [38] H. D. Granados, «Presupuesto en ciberseguridad aumenta en empresas, pese a recortes por COVID-19,» Kaspersky, Octubre Febrero 2021. [En línea]. Available: <https://latam.kaspersky.com/blog/presupuesto-en-ciberseguridad-aumenta-en-empresas-pese-a-recortes-por-covid-19/21022/>. [Último acceso: 20 Diciembre 2022].
- [39] Semana, «Si usted está afiliado a Sanitas y Colsanitas preocúpese: sigue el secuestro de los hackers, que estarían publicando información de pacientes para presionar pago,» Semana, 21 Diciembre 2022. [En línea]. Available: <https://www.semana.com/salud/articulo/se-agrava-situacion-de-sanitas-hackers-que-hicieron-ciberataque-estarian-publicando-datos-de-los-pacientes/202226/>. [Último acceso: 22 Diciembre 2022].
- [40] Portafolio, «Ataque informático a Sanitas no comprometió información de usuarios,» Portafolio, 21 Diciembre 2022. [En línea]. Available: <https://www.portafolio.co/negocios/empresas/eps-sanitas-detalles-del-ciberataque-que-sufrio-grupo-keralt-575968>. [Último acceso: 22 Diciembre 2022].
- [41] GlobalData UK Ltd., «Colombia Bakery and Cereals Market Size by Categories, Distribution Channel, Market Share and Forecast, 2021-2026,» Market Research

- Reports & Consulting | GlobalData UK Ltd., 16 Junio 2022. [En línea]. Available: <https://www.globaldata.com/store/report/colombia-bakery-and-cereals-market-analysis/>. [Último acceso: 03 Enero 2023].
- [42] Mordorintelligence, «Colombia Cybersecurity Market - Growth, Trends, COVID-19 Impact, and Forecasts (2023 - 2028),» Mordorintelligence, 2022. [En línea]. Available: <https://www.mordorintelligence.com/industry-reports/colombia-cybersecurity-market>. [Último acceso: 03 Enero 2023].
- [43] MINTIC , «MINTIC Colombia - Inicio,» MINTIC , 2022. [En línea]. Available: <https://www.mintic.gov.co/portal/inicio/>. [Último acceso: 04 Enero 2023].
- [44] Mintic, «CSIRT Gobierno,» Mintic, 2021. [En línea]. Available: <https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/CSIRT-Gobierno/>. [Último acceso: 04 Enero 2023].
- [45] CCIT, «Estudio trimestral de ciberseguridad: Ataques a entidades de gobierno,» CCIT - Cámara Colombiana de Informática y Telecomunicaciones, 06 Abril 2022. [En línea]. Available: <https://www.ccit.org.co/wp-content/uploads/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno-safe-bp.pdf>. [Último acceso: 03 Enero 2023].
- [46] Kionetworks, «Conoce las tendencias en ciberseguridad para este 2022,» Kionetworks, 2022. [En línea]. Available: <https://www.kionetworks.com/blog/ciberseguridad/conoce-las-tendencias-en-ciberseguridad-para-este-2022>. [Último acceso: 06 Enero 2023].
- [47] J. Howarth, «8 Huge Cybersecurity Trends (2023),» Exploding Topics, 08 Septiembre 2021. [En línea]. Available: <https://explodingtopics.com/blog/cybersecurity-trends>. [Último acceso: 06 Enero 2023].
- [48] Deloitte Chile, «Las 10 tendencias en ciberseguridad que marcarán el 2021,» Deloitte, 12 2 2021. [En línea]. Available:

<https://www2.deloitte.com/cl/es/pages/risk/articles/diez-tendencias-ciberseguridad-2021.html>. [Último acceso: 06 Diciembre 2023].

- [49] El blog de Orange, «Así cambiará la ciberseguridad: las diez tendencias de 2023,» El blog de Orange, 21 Diciembre 2022. [En línea]. Available: <https://blog.orange.es/navegacion-segura/ciberseguridad-tendencias-2023/#>. [Último acceso: 06 Enero 2023].
- [50] Kaspersky, «Top Ten Cybersecurity Trends,» Kaspersky, 18 Febrero 2022. [En línea]. Available: <https://www.kaspersky.com/resource-center/preemptive-safety/cyber-security-trends>. [Último acceso: 06 Enero 2023].
- [51] Semana, «Las nuevas tendencias que se esperan en 2023 en materia de ciberseguridad,» Semana, 29 Noviembre 2022. [En línea]. Available: <https://www.semana.com/economia/empresas/articulo/las-nuevas-tendencias-que-se-espera-en-2023-en-materia-de-ciberseguridad/202245/>. [Último acceso: 06 Enero 2023].
- [52] N. Duggal, «Top 10 Cybersecurity Trends to Watch Out For in 2023,» Simplilearn, 11 Marzo 2020. [En línea]. Available: <https://www.simplilearn.com/top-cybersecurity-trends-article>. [Último acceso: 06 Diciembre 2023].
- [53] Spiceworks, «12 Cybersecurity Trends Every CISO Must Prepare for in 2023 |,» Spiceworks, 22 Noviembre 2022. [En línea]. Available: <https://www.spiceworks.com/it-security/cyber-risk-management/interviews/top-cybersecurity-trends-2023/>. [Último acceso: 06 Enero 2023].
- [54] C. C. Alonso, «Zero trust, tendencia en el entorno de seguridad cloud,» Think Big | Telfónica Tech, 14 Noviembre 2022. [En línea]. Available: <https://empresas.blogthinkbig.com/zero-trust-tendencia-entorno-seguridad-cloud/>. [Último acceso: 07 Enero 2023].
- [55] Netronome , «Zero-Trust Security for Cloud Data Centers – How Much Does it Cost?,» Netronome , 09 Agosto 2016. [En línea]. Available:

- <https://www.netronome.com/blog/zero-trust-security-for-cloud-data-centers-how-much-does-it-cost/>. [Último acceso: 07 Enero 2023].
- [56] R. Toledo, «Principales tendencias de ciberseguridad del 2022,» Grupocibernos, 28 Julio 2022. [En línea]. Available: <https://www.grupocibernos.com/blog/principales-tendencias-de-ciberseguridad-del-2022>. [Último acceso: 07 Enero 2023].
- [57] Mordorintelligence, «Mercado de seguridad de confianza cero: crecimiento, tendencias, impacto de COVID-19 y pronósticos (2022 - 2027),» Mordorintelligence, 2022. [En línea]. Available: <https://www.mordorintelligence.com/es/industry-reports/zero-trust-security-market>. [Último acceso: 07 Enero 2023].
- [58] Itdigitalsecurity, «El 80% de las empresas opta por la seguridad Zero Trust como alternativa a las VPN,» Itdigitalsecurity, 17 Octubre 2022. [En línea]. Available: <https://www.itdigitalsecurity.es/endpoint/2022/10/el-80-de-las-empresas-opta-por-la-seguridad-zero-trust-como-alternativa-a-las-vpn>. [Último acceso: 17 Enero 2023].
- [59] J. Gregory, «Cybersecurity Trends: IBM's Predictions for 2023,» Security Intelligence, 13 Diciembre 2022. [En línea]. Available: <https://securityintelligence.com/articles/cybersecurity-trends-ibm-predictions-2023/>. [Último acceso: 07 Enero 2023].
- [60] Lumu Technologies, «Cybersecurity 2023: Recession Opens Opportunities for Criminals and Defenders,» Lumu Technologies, Diciembre 2022. [En línea]. Available: https://lumu.io/blog/predictions-cybersecurity-2023/?utm_source=linkedin&utm_medium=organic&utm_campaign=ao1418_02122022_b2b_lin_org_trf_predicitons_2023_sm. [Último acceso: 07 Enero 2023].
- [61] B. Marr, «The Top Five Cybersecurity Trends In 2023,» Forbes, 14 Noviembre 2022. [En línea]. Available: <https://www.forbes.com/sites/bernardmarr/2022/11/11/the-top-five-cybersecurity-trends-in-2023/?sh=509a12871785>. [Último acceso: 07 Enero 2023].
- [62] INCIBE, «Tendencias,» INCIBE, 07 Junio 2023. [En línea]. Available: <https://www.incibe.es/enise/tendencias>. [Último acceso: 07 Enero 2023].

- [63] Kaspersky, «Internet of Things Security Threats,» Kaspersky, 13 Enero 2021. [En línea]. Available: <https://www.kaspersky.com/resource-center/threats/internet-of-things-security-risks>. [Último acceso: 08 Enero 2023].
- [64] Knowledgehut, «IoT Cyber Security: Trends, Challenges and Solutions,» Knowledgehut, 2022. [En línea]. Available: <https://www.knowledgehut.com/blog/security/lot-cyber-security>. [Último acceso: 08 Enero 2023].
- [65] R. Ramiro, «Recomendaciones de ciberseguridad en IoT,» CIBERSEGURIDAD | Blog, 03 Junio 2018. [En línea]. Available: <https://ciberseguridad.blog/recomendaciones-de-ciberseguridad-en-iot/>. [Último acceso: 08 Enero 2023].
- [66] INCIBE, «TemáTICas IoT,» INCIBE, 13 Enero 2021. [En línea]. Available: <https://www.incibe.es/protege-tu-empresa/tematicas/iot>. [Último acceso: 08 Enero 2023].
- [67] Portafolio, «La demanda de servicios de ciberseguridad creció 40%,» Portafolio, 08 Febrero 2022. [En línea]. Available: <https://www.portafolio.co/innovacion/la-demanda-de-servicios-de-ciberseguridad-crecio-40-561523>. [Último acceso: 09 Enero 2023].
- [68] A. Noguerras, «La demanda de talento en Ciberseguridad doblará a la oferta en 2024,» EALDE Business School, 23 Mayo 2022. [En línea]. Available: <https://www.ealde.es/demanda-de-talento-en-ciberseguridad/>. [Último acceso: 09 Enero 2023].
- [69] «Demanda de Profesionales de Ciberseguridad Durante la Pandemia | Latam University,» LATAM University, 19 Abril 2021. [En línea]. Available: <https://blog.latam.university/blog/demanda-de-profesionales-de-ciberseguridad-durante-la-pandemia/>. [Último acceso: 09 Enero 2023].
- [70] INCIBE, «La demanda de talento en ciberseguridad doblará a la oferta en 2024, hasta alcanzar la cifra de más de 83.000 profesionales necesarios en el sector,» INCIBE, Marzo 2022. [En línea]. Available: <https://www.incibe.es/sala-prensa/notas->

prensa/demanda-talento-ciberseguridad-doblara-oferta-2024-alcanzar-cifra-mas-83000. [Último acceso: 09 Enero 2023].

- [71] Ciberseguridad, «EMPRESAS DE CIBERSEGURIDAD EN COLOMBIA,» Ciberseguridad, 30 Octubre 2020. [En línea]. Available: <https://ciberseguridad.com/empresas/colombia/>. [Último acceso: 09 Enero 2023].
- [72] A. Datalab, «El 62% de las pymes colombianas no tiene acceso a financiamiento | Colombiafintech,» Colombiafintech, 2020. [En línea]. Available: <https://www.colombiafintech.co/lineaDeTiempo/articulo/el-62-de-las-pymes-colombianas-no-tiene-acceso-a-financiamiento>. [Último acceso: 09 Enero 2023].
- [73] Portafolio, «Ciberseguridad, clave para la industria de los eventos en el 2021,» Portafolio, 11 Febrero 2021. [En línea]. Available: <https://www.portafolio.co/tendencias/ciberseguridad-clave-para-la-industria-de-los-eventos-en-el-2021-549070>. [Último acceso: 09 Enero 2023].
- [74] Portafolio, «Los sectores en los que más se han creado empresas en Colombia en 2022,» Portafolio, 23 Agosto 2022. [En línea]. Available: <https://www.portafolio.co/negocios/empresas/los-sectores-en-los-que-mas-se-han-creado-empresas-en-colombia-en-2022-569928>. [Último acceso: 09 Enero 2023].
- [75] INCIBE, «INCIBE Emprende, el nuevo programa para emprendedores y start-ups de ciberseguridad dotado con 191 millones de euros,» INCIBE, 09 Septiembre 2012. [En línea]. Available: <https://www.incibe.es/sala-prensa/notas-prensa/incibe-emprende-el-nuevo-programa-emprendedores-y-start-ups-ciberseguridad>. [Último acceso: 09 Enero 2023].
- [76] INCIBE, «INCIBE promueve el emprendimiento en ciberseguridad con una inversión de 30 millones de euros de fondos europeos,» INCIBE, 29 Diciembre 2022. [En línea]. Available: <https://www.incibe.es/sala-prensa/notas-prensa/incibe-promueve-el-emprendimiento-ciberseguridad-inversion-30-millones>. [Último acceso: 09 Enero 2023].

- [77] IPSEC Colombia, «Inicio - IPSEC Colombia - Ciberseguridad y Tecnologías de la Información,» IPSEC Colombia, 2023. [En línea]. Available: <https://ipsec.com.co/esp/>. [Último acceso: 10 Enero 2023].
- [78] Gtd Colombia, «Gtd Colombia: Expertos en Soluciones Digitales para tu Empresa - Colombia-Corporaciones - GTD,» GTD Colombia, 2022. [En línea]. Available: <https://www.gtdcolombia.com/inicio>. [Último acceso: 10 Enero 2023].
- [79] B-SECURE, «Perfin LinkedIn B-SECURE,» LinkedIn, sf. [En línea]. Available: <https://www.linkedin.com/company/b-secure/>. [Último acceso: 10 Enero 2023].
- [80] B-SECURE , «B-SECURE | Pasión por la Seguridad,» B-SECURE , 2021. [En línea]. Available: <https://www.b-secure.co/>. [Último acceso: 10 Enero 2023].
- [81] B-SECURE, «¿Quiénes somos? | B-SECURE,» B-SECURE, 2015. [En línea]. Available: <https://www.b-secure.co/nosotros/quienes-somos>. [Último acceso: 10 Enero 2023].
- [82] 360 Security Group, «Soluciones-360 Security Group,» 360 Security Group, sf. [En línea]. Available: <https://www.360sec.com/soluciones.html>. [Último acceso: 23 Enero 2023].
- [83] 360 Security Group, «360 Security Group,» LinkedIn, sf. [En línea]. Available: <https://www.linkedin.com/company/360-security-group/>. [Último acceso: 10 Enero 2023].
- [84] SIGUARD, «Seguridad Informática en Colombia,» Seguridad Informática | SIGUARD, 18 Mayo 2021. [En línea]. Available: <https://seguridadinformatica.com.co/>. [Último acceso: 10 Enero 2023].
- [85] DragonJAR, «DragonJAR - Servicios de Seguridad Informática,» DragonJAR, 25 Mayo 2021. [En línea]. Available: <https://www.dragonjar.org/>. [Último acceso: 11 Enero 2023].
- [86] Appgate, «Appgate | People-Defined Zero Trust Security,» Appgate, [En línea]. Available: <https://www.appgate.com/>. [Último acceso: 11 Enero 2023].

- [87] Grupo Oruss, «Grupo Oruss | Ciberseguridad & Ethical Hacking,» Grupo Oruss, 05 Mayo 2016. [En línea]. Available: <https://grupooruss.com/home/>. [Último acceso: 11 Enero 2023].
- [88] 2Secure S.A.S, «2Secure S.A.S, Productos y Servicios en seguridad de la información,» 2Secure S.A.S, 16 Junio 2016. [En línea]. Available: <https://2secure.co/>. [Último acceso: 11 Enero 2023].
- [89] Gamma Ingenieros S.A.S, «Web site Gamma,» Gamma Ingenieros S.A.S, 22 Abril 2022. [En línea]. Available: <https://www.gammaingenieros.com/>. [Último acceso: 11 Enero 2023].
- [90] SecPro Security Professionals, «Inicio - SecPro Security Professionals,» SecPro Security Professionals, 11 Septiembre 2020. [En línea]. Available: <https://secpro.co/>. [Último acceso: 11 Enero 2023].
- [91] A3sec, «A3Sec - Operación Unificada de Seguridad,» A3sec, 2019. [En línea]. Available: <https://www.a3sec.com/>. [Último acceso: 11 Enero 2023].
- [92] Hack-Inn, «Inicio | Hack-Inn,» Hack-Inn, 2011. [En línea]. Available: <https://www.hack-inn.com/>. [Último acceso: 11 Enero 2023].
- [93] Identian, «Identian -Beyond Information - Identian,» Identian, 10 Enero 2021. [En línea]. Available: <https://www.identian.co/>. [Último acceso: 11 Enero 2023].
- [94] Isecauditors, «Internet Security Auditors,» Isecauditors, 2022. [En línea]. Available: <https://www.isecauditors.com/>. [Último acceso: 11 Enero 2023].
- [95] J2K Security Group, «Inicio - J2K Security Group,» J2K Security Group, 22 Noviembre 2021. [En línea]. Available: <https://www.j2ksec.com/>. [Último acceso: 11 Enero 2023].
- [96] NewNet S.A., «Especialista en Gestión de Riesgos de Tecnología - NewNet S.A.,» NewNet S.A., 22 Junio 2021. [En línea]. Available: <https://www.newnetsa.com/>. [Último acceso: 11 Enero 2023].

- [97] Securesoft, «Inicio - securesoft,» Securesoft, 2015. [En línea]. Available: <https://www.securesoftcorp.com/>. [Último acceso: 11 Enero 2023].
- [98] Up Connection, «Up Connection – Ciberseguridad Escalando la Nube,» Up Connection, sf. [En línea]. Available: <https://upconnection.co/>. [Último acceso: 11 Enero 2023].
- [99] ITforensic, «IT FORENSIC COMPANY - Ciberseguridad,» ITforensic, sf. [En línea]. Available: <https://www.itforensic-la.com/index.html>. [Último acceso: 11 Enero 2023].
- [100] S2 Grupo, «S2 Grupo | Especializada en Ciberseguridad,» S2 Grupo, 2022. [En línea]. Available: <https://s2grupo.es/>. [Último acceso: 11 Enero 2023].
- [101] Canadian College, «Análisis DOFA: una herramienta fundamental para evaluar tu empresa,» Canadian College, 17 Diciembre 2020. [En línea]. Available: <https://canadiancollege.edu.co/analisis-dofa-una-herramienta-fundamental-para-evaluar-tu-empresa/>. [Último acceso: 13 Enero 2023].
- [102] Sistema TDC, «¿Cómo hacer un análisis DOFA?,» Sistema TDC, 03 Junio 2020. [En línea]. Available: <https://sistematdc.com/blog/sistema/como-hacer-un-analisis-dofa/>. [Último acceso: 13 Enero 2023].
- [103] Harvard Business , «Why the Lean Start-Up Changes Everything,» Harvard Business Review, Mayo 2013. [En línea]. Available: <https://hbr.org/2013/05/why-the-lean-start-up-changes-everything>. [Último acceso: 20 Enero 2023].
- [104] M. Bonzón, «¿Qué es Lean Startup? ¿Para qué sirve?,» Designthinking, sf. [En línea]. Available: <https://www.designthinking.es/comparte/view.php?id=305&tipo=>. [Último acceso: 20 Enero 2023].
- [105] R. Alberdi, «The Lean Startup Methodology Cycle: 4 Steps to Risk-Free Success,» ThePower Business School, 25 Marzo 2023. [En línea]. Available: <https://www.thepowermba.com/en/blog/lean-startup-methodology>. [Último acceso: 22 Enero 2023].

- [106] «The Lean Startup | Methodology,» Theleanstartup, sf. [En línea]. Available: <https://theleanstartup.com/principles>. [Último acceso: 22 Enero 2023].
- [107] University Lab Partners, «What Is the Lean Startup Methodology?,» University Lab Partners, 2020. [En línea]. Available: <https://www.universitylabpartners.org/blog/what-is-lean-startup-methodology>. [Último acceso: 22 Enero 2023].
- [108] J. C. Alcalde, «¿En qué consiste el método lean startup?,» Economipedia, sf. [En línea]. Available: <https://economipedia.com/definiciones/metodo-lean-startup.html>. [Último acceso: 22 Enero 2023].
- [109] D. Torres, «¿Qué es el método Lean Startup? Definición, pasos y ejemplos,» Hubspot, 24 Mayo 2022. [En línea]. Available: <https://blog.hubspot.es/sales/metodo-lean-startup>. [Último acceso: 29 Enero 2023].
- [110] E. E. Samaniego, «5 ejemplos de Lean Startup para inspirar su propio negocio,» LinkedIn, 19 Agosto 2021. [En línea]. Available: <https://www.linkedin.com/pulse/5-ejemplos-de-lean-startup-para-inspirar-su-propio-el%C3%BAa-samaniego/>. [Último acceso: 29 Enero 2023].
- [111] CertiProf, «Authorized Training Partner 2023 was issued by CertiProf to Beef Up Tech.,» Credly, 06 Julio 2023. [En línea]. Available: https://www.credly.com/badges/68cfc168-8fcc-469d-a928-0846e5db101b/public_url. [Último acceso: 06 Julio 2023].
- [112] Cámara de Comercio de Bogotá | CCB, «Pasos para crear tu empresa para que tu negocio funcione con todas las de la ley,» Cámara de Comercio de Bogotá | CCB, 2022. [En línea]. Available: <https://www.ccb.org.co/Cree-su-empresa/Programa-Juntos/Quieres-crear-tu-empresa>. [Último acceso: 06 Marzo 2023].
- [113] Cámara de Comercio de Bogotá | CCB, «Formas jurídicas para crear tu empresa,» Cámara de Comercio de Bogotá | CCB, 2022. [En línea]. Available: <https://www.ccb.org.co/Cree-su-empresa/Programa-Juntos/Quieres-crear-tu-empresa>. [Último acceso: 06 Marzo 2023].

- [114] Cámara de Comercio de Bogotá | CCB, «Trámites para registrar y constituir su empresa,» Cámara de Comercio de Bogotá | CCB, 2022. [En línea]. Available: <https://www.ccb.org.co/Cree-su-empresa/Programa-Juntos/Quieres-crear-tu-empresa>. [Último acceso: 06 Marzo 2023].
- [115] Cámara de Comercio de Bogotá | CCB, «Ley de Emprendimiento Juvenil,» Cámara de Comercio de Bogotá | CCB, 2022. [En línea]. Available: <https://www.ccb.org.co/Inscripciones-y-renovaciones/Normativa-Registros-Publicos/Ley-de-Emprendimiento-Juvenil>. [Último acceso: 08 Marzo 2023].
- [116] Modelo Canvas, «Diferencia entre Lean Canvas y Modelo Canvas,» Modelo Canvas, 28 Septiembre 2020. [En línea]. Available: <https://modelo-canvas.com/diferencia-entre-lean-canvas-y-modelo-canvas/>. [Último acceso: 1 Julio 2023].
- [117] A. R. Ferrer, «Cap 25: Como convertir mi idea en producto o servicio,» Boss Tank: Ser Tu Propio Jefe [Podcast de audio], 15 Agosto 2019. [En línea]. Available: <https://open.spotify.com/episode/2h6BKUka3R1Ofo6G9qwkqL?si=VgriF1J8RBmYeNC8UkBxAQ>. [Último acceso: 1 Julio 2023].
- [118] Actualícese, «Costos de contratar un trabajador con el salario mínimo,» Actualícese, 28 Marzo 2023. [En línea]. Available: <https://actualicese.com/costos-de-contratar-un-trabajador-con-el-salario-minimo/>. [Último acceso: 06 Julio 2023].