Plan de negocio para la creación de la empresa Bluedice

Claudia Liliana Carreño

Juan David Parra

Fabian Humberto Vergara

Universidad EAN

Facultad de ingeniería

Maestría en gerencia de sistemas de información y proyectos de tecnológicos

Bogotá, Colombia

Mayo 24 2024

Plan de negocio para la creación de la empresa Bluedice

Juan David Parra

Claudia Liliana Carreño

Fabian Humberto Vergara

Trabajo de grado presentado como requisito para optar al título de:

Magister en Gerencia de sistemas de información y proyectos tecnológicos

Director (a):

León Darío Parra Bernal

Modalidad:

Creación de Empresa

Facultad de ingeniería

Maestría en gerencia de sistemas de información y proyectos tecnológicos

Bogotá, Colombia

Mayo 24 2024

Nota de aceptación

_____

_____

_____

_____

_____

_____

Firma del jurado

_____

Firma del jurado

_____

Firma del director del trabajo de grado

Bogotá, Mayo 24 2025

Agradecimientos

Agradezco sinceramente a mi familia, amigos y profesores por su apoyo inquebrantable durante este proceso de investigación y redacción de mi trabajo de grado. Su aliento fue fundamental para lograr este logro.

Frase:

"En el camino hacia la maestría en gerencia de sistemas de información, cada desafío es una oportunidad para demostrar tu capacidad de liderazgo y excelencia. Como un maestro en formación, enfrenta cada obstáculo con determinación, ya que cada paso te acerca a la maestría. ¡Tu tesis no solo es un proyecto, es el reflejo de tu dedicación y conocimiento! Eleva tus habilidades, alcanza la cima de la maestría y deja una huella duradera en el mundo de los sistemas de información."

Resumen

En un mundo caracterizado por un rápido avance tecnológico y una creciente dependencia de la innovación digital, las amenazas cibernéticas se han convertido en un desafío significativo. La falta de énfasis en la seguridad informática debido a la aceleración en el desarrollo de software ha dejado a muchas organizaciones vulnerables. En respuesta a esta necesidad, surge la idea de crear una empresa especializada en seguridad de la información.

Esta empresa se dedica a realizar análisis exhaustivos de vulnerabilidades y riesgos de seguridad para fortalecer la ciberseguridad de otras organizaciones. Su enfoque proactivo anticipa posibles amenazas, realiza pruebas de penetración éticas y ayuda a implementar estrategias de mitigación.

Para lograr este objetivo se llevará a cabo un proceso de investigación con diferentes tipos de herramientas las cuales permitirán identificar ventajas competitivas, factores internos y externos, diversificación de productos, viabilidad financiera y desarrollar diferentes indicadores que den una visión global y especifica en la ejecución y seguimiento en el tiempo de este proyecto.

En conclusión, este estudio de grado aporta al ámbito de los análisis corporativos al investigar un enfoque de negociación innovador y contemporáneo, centrado en las demandas de la actualidad y poder contribuir y solucionar una problemática que cada vez es más frecuente y critica de cara a la protección de los datos de los clientes y organizaciones.

De los iniciadores de proyectos y adquisidores en un entorno virtual. Asimismo, proporciona sugerencias concretas para los emprendedores que desean acceder al sector de las ventas en línea, resaltando la relevancia de la propuesta de beneficios, la estrategia global y la interacción especializada con los consumidores.

Palabras clave: Seguridad, Ciberseguridad, ISO27001, criticidad, activos de información, análisis de vulnerabilidad, Amenazas.

Abstract

In a world characterized by rapid technological advancement and an increasing reliance on digital innovation, cyber threats have become a significant challenge. The lack of emphasis on computer security due to the accelerated pace of software development has left many organizations vulnerable. In response to this need, the idea of creating a specialized information security company has emerged.

This company is dedicated to conducting thorough vulnerability and security risk analyses to strengthen the cybersecurity of other organizations. Its proactive approach anticipates potential threats, conducts ethical penetration testing, and assists in implementing mitigation strategies.

To achieve this goal, a research process will be carried out using several types of tools that will enable us to identify competitive advantages, internal and external factors, product diversification, financial feasibility, and develop different indicators that provide a comprehensive and specific insight into the execution and ongoing monitoring of this project.

In conclusion, this degree study contributes to the field of corporate analysis by investigating an innovative and contemporary business approach, focused on current demands and the ability to contribute to and address an increasingly common and critical issue regarding the protection of customer and organizational data. This pertains to project initiators and acquirers in a virtual environment. Additionally, it provides specific recommendations for entrepreneurs looking to

enter the online sales sector, emphasizing the relevance of value proposition, global strategy, and specialized interaction with consumers.

Keywords: Security, Cybersecurity, ISO27001, criticality, information assets, vulnerability analysis, Threats.

}

Tabla de Contenidos

1. Introducción 16

Objetivo general 21

Objetivos específicos 21

2. Naturaleza del Proyecto 22

2.1. Origen de la idea de negocio 22

2.2. Descripción del modelo de negocio 24

2.3. Objetivos empresariales 26

2.4. Estado actual del negocio 27

2.5. Descripción de productos o servicios 28

2.6. Razón social, tamaño y ubicación de la empresa 30

2.7. Potencial del mercado en cifras 30

2.8. Ventajas competitivas del producto y/o servicio 32

2.9. Resumen de las inversiones requeridas 33

2.10. Proyecciones de ventas y rentabilidad 33

2.11. Conclusiones financieras y evaluación de viabilidad 34

2.12. Equipo de trabajo 35

3. Análisis del sector 37

3.1. Análisis PESTEL 38

3.2. Análisis Porter 52

4. Estudio piloto de mercado 66

4.1. Análisis y estudio de mercado 66

4.2. Perfil de persona 70

4.3. Descripción de los consumidores Ficha técnica de encuesta 74

4.4. Análisis de la Competencia 84

4.5. Estrategia y plan de introducción de mercado 88

4.6. Estrategia de producto y servicios 89

4.7. Estrategia de precio 91

5. Aspectos técnicos 92

5.1. Ficha técnica del producto o servicio 92

6. Recursos tecnológicos e infraestructura 99

7. Proceso para la prestación del servicio 100

7.1. Mapa de Procesos Bluedice 100

7.2. Flujograma proceso de prestación del servicio 101

7.3. Capacidad de prestación del servicio 103

8. Aspectos organizacionales y legales 107

8.1. Misión: 107

8.2. Visión 107

8.3. Análisis DOFA 107

8.4. Análisis cruzado Matriz DOFA BLUEDICE 109

8.5. Normatividad empresarial 111

9. Aspectos financieros 114

9.1. Estados financieros Básicos proyectados 121

9.2. Evaluación financiera y punto de equilibrio 124

10. Sostenibilidad 126

11. Conclusiones 130

Referencias **132**

A. Anexos **135**

Tabla de Imágenes

Pág.

Imagen 1 - Delitos informáticos en Colombia - Fuente Asuntos legales. *17*

Imagen 2 - Lado derecho Lienzo *19*

Imagen 3 - Lado Derecho del Lienzo *20*

Imagen 4 - Mapa sistema de negocio *24*

Imagen 5 - Modelo de Negocio *25*

Imagen 6 - Punto de equilibrio *34*

Imagen 7 - Tabla de Ingresos y crecimiento porcentual *34*

Imagen 8 - Grafico análisis PESTEL *50*

Imagen 9 - Esquema acciones estrategia Océano azul *63*

Imagen 10 - Mapa de Empatía *67*

Imagen 11 - Perfil de Persona *70*

Imagen 12 - Árbol de problemas *73*

Imagen 13 - Cargos encuestados *77*

Imagen 14 - Características para contratar servicios de Seguridad de la información y ciberseguridad *78*

Imagen 15 - Factores de compra servicios de seguridad de la información y ciberseguridad *79*

Imagen 16 - Marcas u oferentes de servicios de ciberseguridad *80*

Imagen 17 - disposición para pagar servicios de seguridad de la información y ciberseguridad *81*

Imagen 18 - Preocupación por los datos en línea *82*

Imagen 19 - Incidentes de seguridad de la información y ciberseguridad 83

Imagen 20 - Mapa de proceso Bluedice - Fuente propia 100

Imagen 21 - Proceso Prestación de servicios Bluedice 102

Imagen 22-Análisis Dofa 108

Imagen 23 - Análisis cruzado matriz DOFA 109

Imagen 24 - Análisis cruzado matriz DOFA Amenazas 110

Imagen 25 - Estructura organizacional Bluedice 114

Imagen 26 - Ingresos- Ventas año 1 115

Imagen 27 - Costos por servicio 116

Imagen 28 - Proyecciones por año 116

Imagen 29 - Crecimiento en ventas 117

Imagen 30 - Inversión inicial 118

Imagen 31 - Presupuestos Marketing Mix 119

Imagen 32 - Gastos fijos 119

Imagen 33 - Inversión total 120

Imagen 34 - Estado de resultados 121

Imagen 35 - Balance 122

Imagen 36 - Flujo de caja 123

Imagen 37 -Calculo de flujo de caja 123

Imagen 38 - Punto de equilibrio 124

Imagen 39 - TIR 124

Imagen 40 - Punto de equilibrio 125

Lista de tablas

Pág.

Tabla 1 - Análisis PESTEL - Político 38

Tabla 2 - Análisis PESTEL - Económico 40

Tabla 3 -Análisis PESTEL - Social 44

Tabla 4 - Análisis PESTEL - tecnológico Fuente: Elaboración propia 46

Tabla 5 - Análisis PESTEL - Ecológico 48

Tabla 6 - Análisis PESTEL - Legal 49

Tabla 7- Fuerzas de Porter – Poder de los compradores 53

Tabla 8 - Fuerzas de Porter – Competidores Potenciales 55

Tabla 9- Fuerzas de Porter – Rivalidad entre los competidores 57

Tabla 10 - - Fuerzas de Porter - Poder de negociación con los Proveedores 59

Tabla 11 - Fuerzas de Porter - Productos sustitutos 61

Tabla 12 - Análisis de la competencia 85

Tabla 13 - Plan de introducción en el mercado 88

Tabla 14 - Ficha técnica Auditoría Interna SGSI ISO 27001 92

Tabla 15 - Ficha Técnica Implementación sistemas de gestión 94

Tabla 16 - Ficha Técnica Auditoría interna SGCN 22301 95

Tabla 17 - Ficha técnica servicios Ethical Hacking - Pentesting - Análisis de vulnerabilidades 96

Tabla 18 - Tabla de infraestructura bluedice 99

Tabla 19 - Capacidad Prestación de Servicios Horas/Mes - Fuente propia 103

Tabla 20 - Capacidad Prestación de Servicios Horas/Empleado 104

Tabla 21 - Requerimiento de conocimiento técnico prestación del servicio 105

Tabla 22 - Normatividad aplicable 111

Tabla 23 - Requerimientos Constitución de empresa 112

Tabla 24 - Estrategias de Sostenibilidad Bluedice 126

1. Introducción

Se evidencia la necesidad del cumplimiento normativo de las empresas colombianas que cuenten con las certificaciones en ISO tales como (27001, 22301, 27032), para la prestación de sus servicios a otras organizaciones.

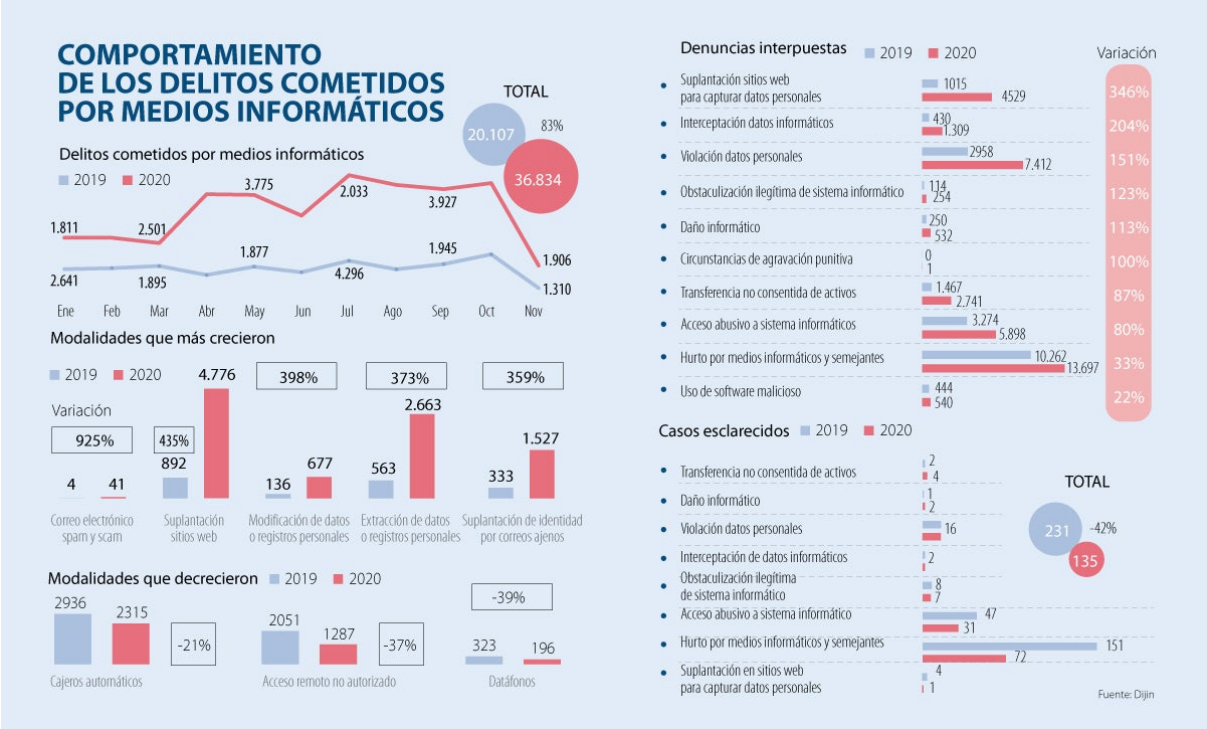
Se evidencia en empresas como la DIAN que para ser proveedor tecnológico y poder prestar servicios de Facturación electrónica requieren contar con la certificación ISO 27001; otro escenario que se evidencia es que muchas empresas para la contratación de servicios se hacen exigible el cumplimiento con estándares de seguridad de la información.

Desde el inicio de la pandemia hasta la fecha se evidencia como las empresas colombianas están sufriendo una transformación tecnológica y están cambiando sus sistemas y procesos a la nube, con esto también se evidencia la vulnerabilidad que se tiene por el desconocimiento y mejora de sistema seguros, las empresas con el paso del tiempo están comprendiendo la importancia de asegurar sus sistemas pues con el paso el tiempo se evidencia la importancia que tiene asegurar los datos de sus clientes ya que estos pueden ser el activo más crítico para su negocio .

La ley 1581 del 2012 (Protección de datos personales), Ley 1273 del 2009 (Medidas mínimas para prevenir delitos informáticos), Decreto 1078 del 2015 (Regula la seguridad de la información en el sector público), y la circular externa 052 2017 (lineamiento para la gestión de riesgos) son unas de las reglamentaciones más importantes el cumplimiento de estas son carácter obligatorio y por ende muchas de las organizaciones que se encuentran en el mercado no cumplen a cabalidad con esta normatividad, ya sea porque no cuentan con el personal capacitado o con el conocimiento para la implementación de estas normas, y se ven en la necesidad de contratar servicios externos “consultoría”, para dar cumplimiento a sus contratos.

En la *Imagen 1* se evidencia el panorama de Seguridad y Ciberseguridad de las empresas colombianas.

Imagen 1 - Delitos informáticos en Colombia - Fuente Asuntos legales.



Los delitos cometidos por medios informáticos crecieron 83% por cuenta de la pandemia. (s/f). Com.co. Recuperado el 30 de enero de 2024, de https://www.asuntoslegales.com.co/consumidor/los-delitos-cometidos-por-medios-informaticos-crecieron-83-por-cuenta-de-la-pandemia-3099101

Según un estudio en donde se hace una comparación del año 2019 y 2020 basado en el comportamiento de los delitos cometidos por medios informáticos, se puede evidenciar un crecimiento de hasta el 453% en suplantación sitios web, 398% en modificación de datos o registros personales, 373% en extracción de datos o registros personales y 359% en suplantación de identidad por correos ajenos y el aumento de estas modalidades son directamente

proporcionales a las denuncias hechas por personas quienes de alguna forma se vieron involucradas.

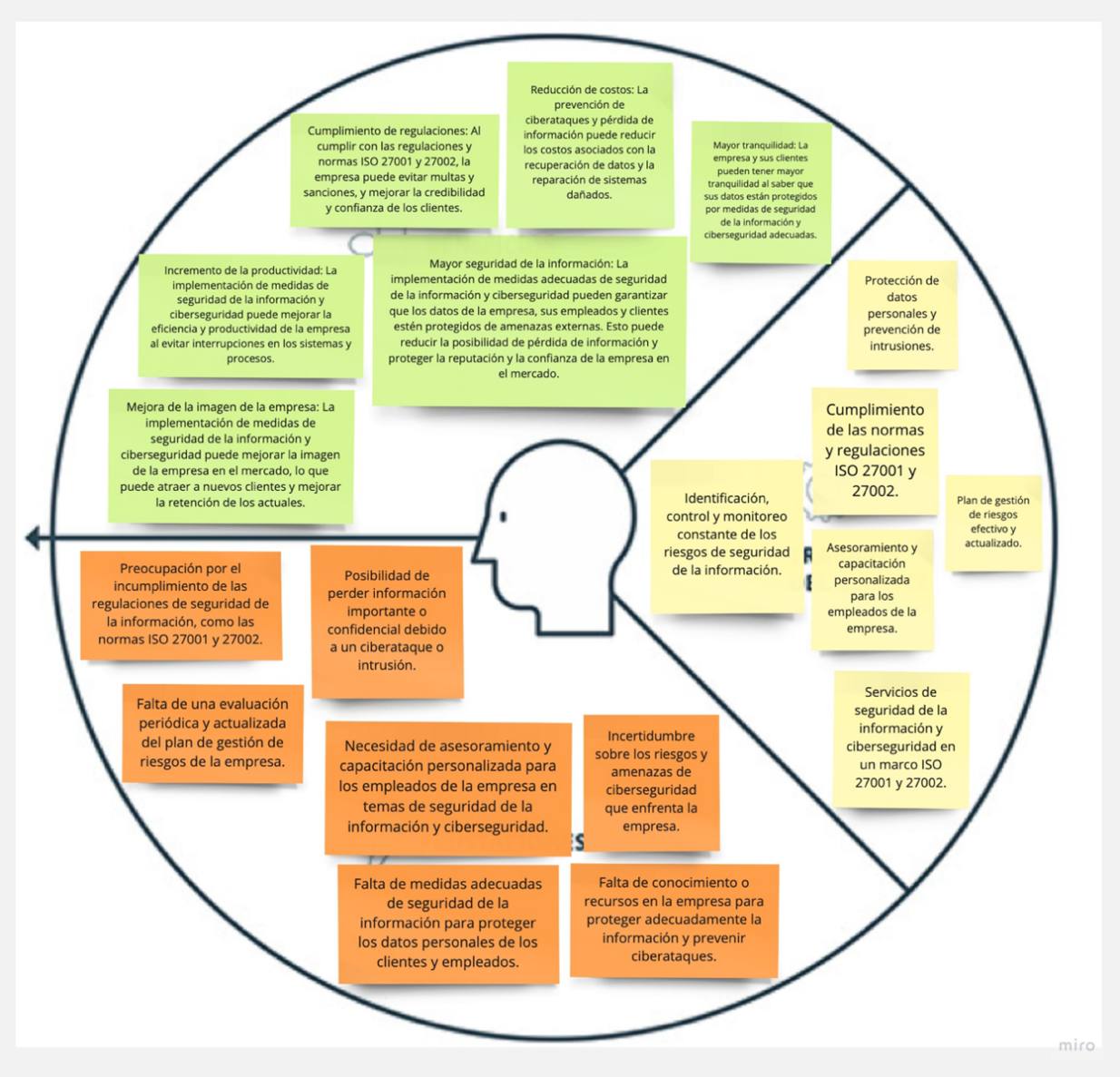
Con el incremento de este tipo de amenazas y el auge que cada vez aumenta por el consumo de aplicaciones móviles, web, y el consumo de la tecnología aumenta la demanda de ofrecer este tipo de servicios y cada vez se hace más importante la protección de los datos personales.

Lienzo de propuesta de Valor

La ilustración del lienzo de la propuesta de valor permite visualizar la necesidades y expectativas de los clientes, al igual que permite representar la oferta de valor que la empresa quiere ofrecer, allí se definirán los beneficios o las promesas de valor que la organización quiere realizar para con sus interesados.

Lado derecho del lienzo

Imagen 2 - Lado derecho Lienzo



Fuente: Elaboración propia

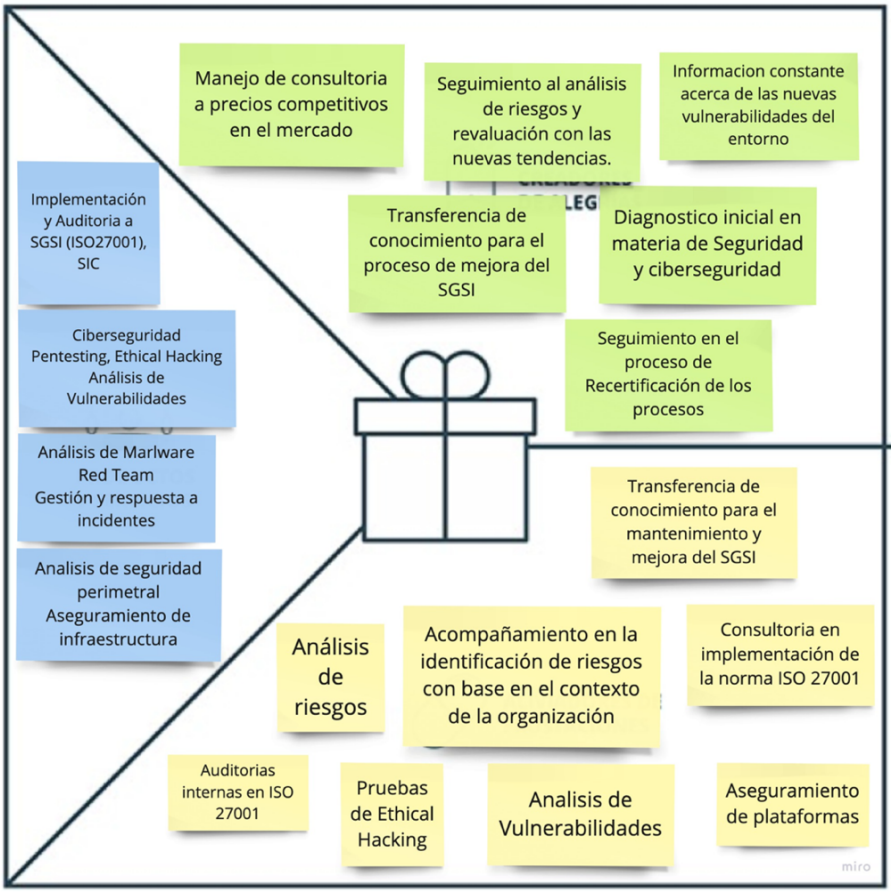
En este lado del lienzo se percibieron las necesidades, miedos y deseos de los clientes en torno al manejo de la seguridad de la información y la ciberseguridad en sus organizaciones, una vez que se conoció al cliente mediante entrevistas realizadas, se procedió a plasmar la información

recibida en este lado del lienzo para visualizar de forma Gráfica y clara que siente el interesado frente a la problemática identificada.

Lado izquierdo del lienzo

El lado del lienzo permite identificar cuál es la propuesta de valor que desea ofrecer la empresa a sus clientes, una vez identificada la problemática presentada por los clientes prospectos, se identificaron los aliviadores del dolor de los clientes, los beneficios que la organización plantea ofrecer y, por último y no menos importante, los servicios que ofrecerá la empresa, para poder garantizar y satisfacer las necesidades del cliente.

Imagen 3 - Lado Derecho del Lienzo



Fuente: Elaboración propia

Durante el plan de investigación se planteó realizar una serie de encuestas y entrevistas a personas que pertenecen al segmento de empresas en las cuales se han realizado unas preguntas con el fin de poder validar la hipótesis planteada.

Objetivo general

Desarrollar un plan de negocio para la creación de la empresa "Bluedice", para la prestación de servicios de implementación, certificación y continuidad de los sistemas de seguridad de la información, ciberseguridad y gestión integral de riesgos.

Objetivos específicos

- Realizar un análisis de mercado para identificar posibles competidores y oportunidades de crecimiento de la empresa Bluedice.
- Analizar los riesgos y amenazas técnico-Operativas de la prestación de servicios de Seguridad de la información, ciberseguridad y riesgos para la creación de la empresa referenciada.
- Realizar un análisis financiero que incluya costos, gastos, proyecciones, análisis de precios y fuentes de ingresos iniciales para la empresa a crear.
- Identificar los recursos administrativos y legales necesarios para la puesta en marcha de la empresa que se está creando.
- Plantear estrategias de sostenibilidad que permitan que Bluedice genere beneficios a la sociedad de manera ética y responsable.

2. Naturaleza del Proyecto

2.1. Origen de la idea de negocio

En el contexto actual, caracterizado por un auge tecnológico sin precedentes, el mundo se encuentra en un estado de constante transformación impulsada por la innovación digital. La tecnología ha alterado radicalmente la forma en que las empresas operan interactúa y gestionan su información. Este escenario, aunque prometedor, ha traído consigo un desafío creciente y preocupante: la vulnerabilidad de los sistemas ante las crecientes amenazas cibernéticas.

El vertiginoso ritmo al que se desarrollan y adoptan nuevas tecnologías ha dejado en su estela a muchas organizaciones incapaces de mantener el paso necesario para implementar buenas prácticas en seguridad informática. Los procesos de desarrollo de software se han vuelto cada vez más acelerados, y la presión por llevar al mercado productos y servicios de manera más rápida ha resultado en una falta de énfasis en la seguridad cibernética. En este contexto, la seguridad de la información se ha convertido en un aspecto crítico que no puede ser ignorado.

Fue en este escenario de vulnerabilidad y riesgo constante que surgió la idea de crear una empresa especializada en abordar los desafíos de seguridad de la información. Esta empresa se dedica a realizar análisis exhaustivos de vulnerabilidades y a identificar riesgos de seguridad con el propósito de fortalecer la ciberseguridad de otras empresas que buscan salvaguardar sus activos digitales y garantizar la confidencialidad, integridad y disponibilidad de su información.

La premisa fundamental de Bluedice es abordar la seguridad cibernética desde un enfoque proactivo. En un mundo donde las amenazas digitales son persistentes y evolucionan constantemente, e equipo de expertos se dedica a anticipar posibles brechas y debilidades en los sistemas de los clientes. Realizamos pruebas de penetración éticas, identificamos vulnerabilidades

y ayudamos a establecer estrategias de mitigación que permitan a las organizaciones estar un paso adelante en la protección de sus activos digitales.

La propuesta de valor de la empresa radica en la capacidad de ofrecer soluciones integrales de seguridad cibernética en un mundo altamente interconectado. Reconocemos que la seguridad de la información es una prioridad estratégica para las organizaciones, ya que cualquier brecha puede tener un impacto devastador en sus operaciones, reputación y relaciones con los clientes.

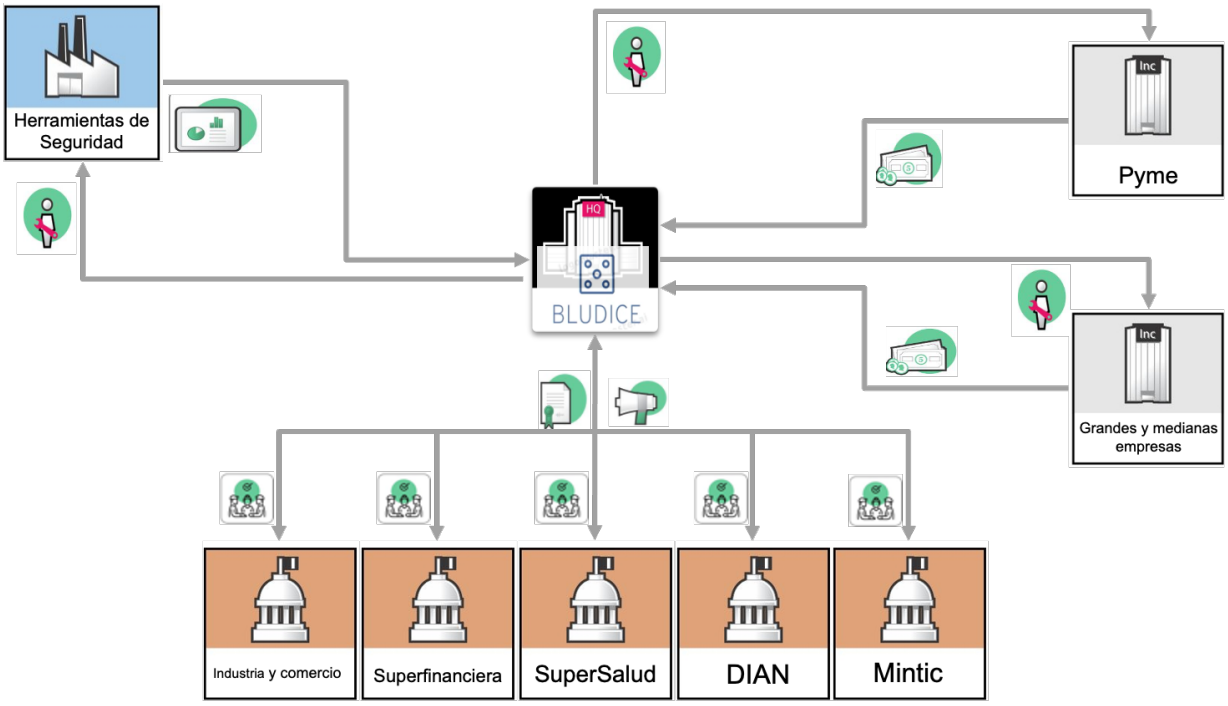
El compromiso de Bluedice con la ciberseguridad va más allá de la mera identificación de vulnerabilidades. Bluedice se esfuerza por proporcionar a los clientes un panorama completo de sus riesgos y la asesoría necesaria para fortalecer su postura de seguridad. Trabajamos codo a codo con ellos para implementar soluciones efectivas y garantizar que estén preparados para enfrentar las amenazas cibernéticas en constante evolución.

La idea de negocio de la empresa no solo responde a la creciente necesidad de ciberseguridad en un mundo digitalizado, sino que también contribuye a la protección de la información crítica de las empresas y a la construcción de la confianza de sus clientes. En un entorno donde la seguridad de la información es esencial, Bluedice se posiciona como un aliado estratégico para aquellos que buscan fortalecer su resiliencia cibernética y mantenerse a salvo en la era digital. La empresa está comprometida a ser líder en el campo de la ciberseguridad, proporcionando un servicio de alta calidad que brinde tranquilidad y seguridad a los clientes en este mundo digitalmente conectado y siempre cambiante.

2.2. Descripción del modelo de negocio

El mapa del sistema de negocio permite identificar visualmente los actores claves del negocio, allí se visualizan las partes interesadas que están en el proceso de Bluedice, y se evidencian los elementos de valor.

Imagen 4 - Mapa sistema de negocio



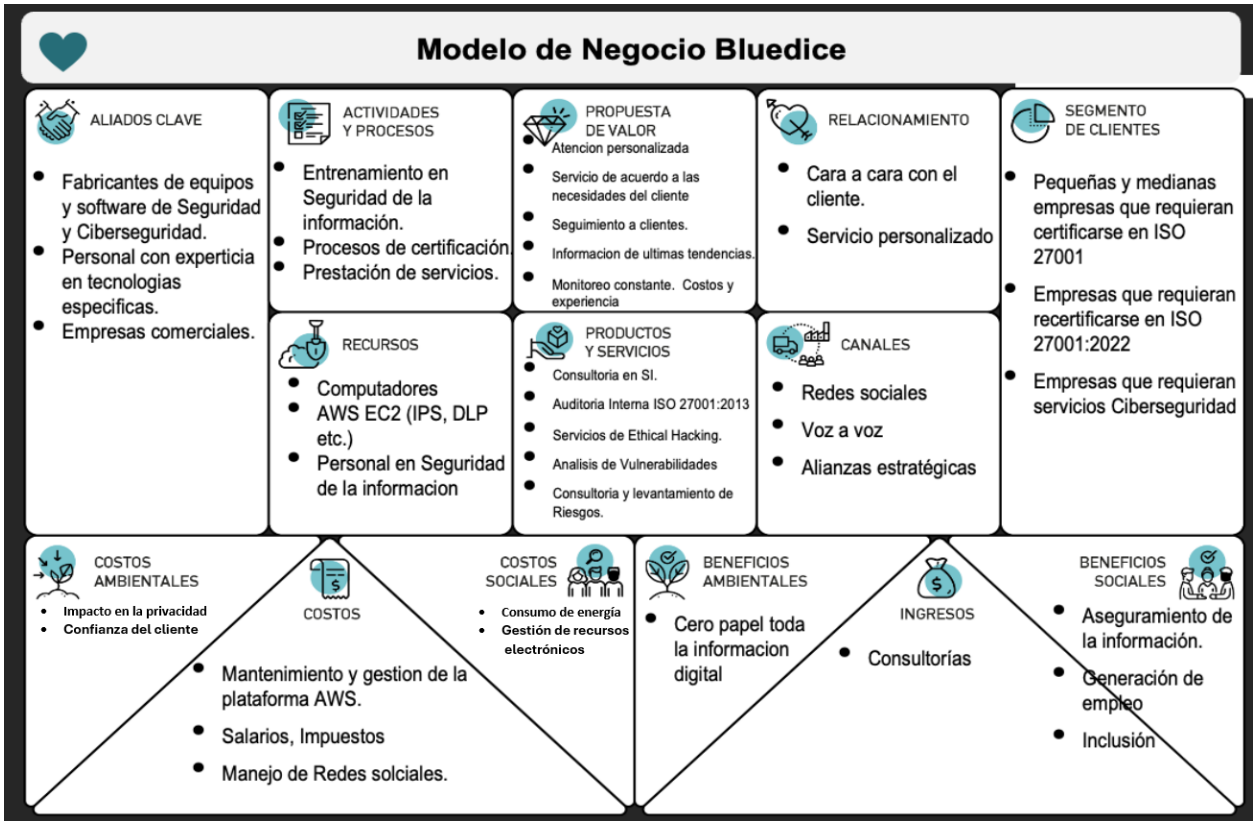
Fuente: Elaboración propia

En la *Imagen 4* se evidencia como eje principal los principales clientes (pymes, grandes y mediana empresas) a los cuales se les ofrecerán los servicios ofertados por Bluedice y en contraprestación se recibirá un pago. En la parte inferior se logra dimensionar los entes reguladores o normativos que se deben tener en cuenta, la parte Gubernamental impulsa el crecimiento del negocio ya que son los encargados de apalancar las directrices de Seguridad de la información y ciberseguridad, por parte de estos entes se pueden tener derechos y exposición los cuales ayudan

al posicionamiento de marca de la compañía, Bluedice entregara a los entes reguladores un trabajo colaborativo para el análisis y/o mesas de trabajo para el cumplimiento de la nueva normatividad que se valla a realizar.

Bluedice generara una conexión bidireccional con los proveedores de herramientas de seguridad, ciberseguridad y riesgos en la que cada una de las personas que trabajan para Bluedice se certificarán y aprenderán de las diferentes tecnologías del proveedor actuando como socio estratégico de negocio con el fin de poder realizar la entrega del servicio y poder obtener un reconocimiento.

Imagen 5 - Modelo de Negocio



Fuente: Elaboración propia

En el siguiente modelo de negocio se puede evidenciar de manera grafica las estrategias del emprendimiento, como lo son los servicios, propuesta de valor, partes interesadas, clientes, canales, gastos y costos, los cuales permiten ver la interrelación de estos en un mismo modelo.

La propuesta de valor se puede sintetizar en los siguientes términos: “Somos una empresa que ofrece servicios de Seguridad de la información, ciberseguridad y riesgos utilizamos conocimientos especializados y mejores prácticas para garantizar que sus datos estén seguros en todo momento. La experiencia del equipo permite diseñar estrategias de seguridad adaptadas a las necesidades específicas de su empresa buscando satisfacer las necesidades con un enfoque personalizado y escalable.”.

Los servicios que prestara la empresa serán consultorías para la adopción y certificación de normas como la ISO 27001, ISO 31000, ISO 22301 entre otras, también se prestaran servicios de ciberseguridad como lo es el análisis de vulnerabilidad, Ethical Hacking y servicios de educación y concienciación.

2.3. Objetivos empresariales

2.3.1. Objetivos a Corto Plazo

- Durante los dos primeros años de operación, lograr el punto de equilibrio financiero, es decir, que los gastos operativos puedan ser absorbidos por los ingresos sin tener que adquirir ningún tipo de deuda.
- Lograr la venta de servicios y el conocimiento de Bluedice en el mercado nacional.
- Los primeros 3 clientes sean conseguidos mediante una estrategia inbound de mercadeo.

- En el primer año de operaciones crear una alianza con una empresa de ciberseguridad, para tener una mayor cobertura en el mercado y mayor número de clientes.

2.3.2. Objetivos a mediano plazo

- Crear un modelo por suscripción para poder ofrecerlo a clientes y generar una concurrencia en los ingresos más frecuentes.
- Estrategias de fidelización que permitan establecer conexiones y relaciones y no perder ningún cliente por lo menos en los 2 primeros años.
- Realizar o participar como speaker por lo menos 1 conferencia al año con el fin de dar a conocer a la empresa como líder en la prestación de servicios de seguridad de la información y ciberseguridad.

2.3.3. Objetivos a largo plazo

- Realizar 1 investigación al año para estar a la vanguardia de la tecnología de seguridad de la información y ciberseguridad con el fin de desarrollar soluciones innovadoras.
- Lograr consolidar financieramente a Bluedice a través de los objetivos financieros estipulados en la proyección generada en el análisis, para 2028 llegar a los 236 millones en utilidad neta (y un punto de equilibro en 1.65 años).
- Ser un referente a nivel nacional como empresa que ofrece servicios de seguridad de la información y gestión de riesgos basados en la normativa ISO27001.

2.4. Estado actual del negocio

El estado actual del negocio básicamente se encuentra en una fase de análisis e investigación. En este momento se está evaluando cuales son los competidores más fuertes en el mercado en Colombia y entendiendo las necesidades de la empresa y/o usuarios finales con el fin de entregar

un servicio basado en las necesidades de los clientes y en el contexto externo de las organizaciones. También la fase de investigación del mercado y así poder diversificar los servicios a partir de una estrategia de inbound marketing con la finalidad de no generar una inversión tan alta en la atracción de clientes desde un frente comercial

2.5. Descripción de productos o servicios

A continuación, se describen los servicios que prestara la empresa con enfoque en Seguridad de la información, Ciberseguridad y Riesgo.

- **Sistemas de gestión**

  Implementación y auditoria a los diferentes sistemas, SGSI (ISO 27001), SGC (ISO 27032), BCP/DRP (ISO 22301), SGS (ISO 20000), SGC (ISO 9000).

- **Normatividad y regulación**

  Apoyo en las diferentes normatividades y regulaciones exigidas en términos de ciberseguridad en el país.

Servicios de Ciberseguridad

- **Pentesting, Ethical Hacking & Análisis de Vulnerabilidades**

  Identificar debilidades en infraestructura, aplicaciones de cualquier tipo y arquitecturas de la organización, todo desde la perspectiva de un atacante real.

- **PCI**

  Pruebas de segmentación y descubrimiento de datos.

- **Pruebas de navegación de servicios (DOS y DDOS)**

Manejo de herramientas de propósito especifico, con el que se busca causar que un recurso informático no esté disponible para los usuarios previstos, inundando una red o un servidor con solicitudes y datos.

- **Análisis de Malware**

  Técnicas avanzadas para la identificación de muestras maliciosas que buscan dañar o comprometer un recurso informático.

- **Red Team**

  Ataques dirigidos, para identificar impactos y superficies de ataque en una compañía.

- **Phishing**

  Ataque que busca capturar por medio de correo electrónico la información confidencial de personas o empresas.

- **Spear Phishing**

  Ataque dirigido por medio de correo electrónico a personas, empresas u organizaciones específicas.

- **Smishing**

  Técnica usada mediante mensajería de texto simulando una organización legitima.

- **Vishing**

  Técnica usada por teléfono, usada para extraer información personal.

- **Tailgating**

  Técnica que busca aprovechar la vulnerabilidad de los empleados de una compañía para ingresar a zonas prohibidas.

- **Aseguramiento de infraestructuras**

  Análisis de las posibles relaciones de los riesgos físicos, los riesgos lógicos y los índices de vulnerabilidades asociados a las amenazas sobre la infraestructura de red y de servidores.

- **Gestión y respuesta a incidentes**

  Responda ante incidentes ejecutados por atacantes avanzados como cibercrimen a gran escala.

2.6. Razón social, tamaño y ubicación de la empresa

Macro-localización:

La empresa se ubicará en el departamento de Cundinamarca, ciudad Bogotá ya que es la capital de país y allí se encuentran la gran mayoría de empresas, esta ciudad cuenta con una buena conectividad de internet ya que este es el servicio de mayor uso por la empresa para la prestación de sus servicios.

Al ser la capital de país y contar con una gran industria la empresa tiene mayor cercanía en la búsqueda y obtención de clientes.

Micro localización

La empresa al estar ubicada en Bogotá, su sitio principal para la prestación de los servicios se encontrará en la localidad de Engativá barrio bonanza, este lugar permite es central y permite un rápido desplazamiento para cualquier parte de la ciudad.

2.7. Potencial del mercado en cifras

El mercado de la seguridad de la información en América Latina está experimentando un crecimiento significativo, impulsado por la creciente digitalización de las empresas y

organizaciones, el aumento de la sofisticación de las amenazas cibernéticas y la creciente concienciación sobre la importancia de la seguridad de la información.

Según el informe "The Cybersecurity Market in Latin America and the Caribbean 2023-2027" de Grand View Research, el mercado de la seguridad de la información en América Latina alcanzará un valor de $28.5 mil millones en 2027, con una tasa de crecimiento anual compuesta (CAGR) del 12,5% durante el período de pronóstico.

Los principales segmentos del mercado de la seguridad de la información en América Latina son la seguridad de endpoints, la seguridad de redes, la seguridad de la nube, la seguridad de aplicaciones y la seguridad de datos. La seguridad de endpoints es el segmento de mayor crecimiento, impulsado por la creciente adopción de dispositivos móviles y BYOD.

América Latina es una región vulnerable a los ataques cibernéticos. En 2022, se registraron más de 100 mil millones de intentos de ciberataques en la región, un aumento del 30% con respecto al año anterior.

Los principales tipos de ataques cibernéticos que afectan a América Latina son el phishing, el ransomware, el malware y el fraude cibernético.

Según un artículo publicado por la republica “la empresa que han sido blando de ciberataques en Colombia en el último año”, Audifarma, Sanitas, Carval y hasta entidades gubernamentales como la fiscalía son algunas de las empresas que han tenido que lidiar con este tipo de ataques. Según el informe de riesgos globales del foro económico mundial, los ataques cibernéticos se incrementaron más del 200% y en Colombia específicamente un 133% en todo el año 2022. En algunos casos varias de estas empresas, 54.121 denuncias entre enero y octubre solo han presentado indisponibilidad de sus servicios, pero muchas de estas también han sufrido por la

pérdida de la información de sus Core y clientes, y se van tenido que enfrentar a grandes sanciones económicas por no garantizar la confidencialidad y transparencia de sus datos.

2.8. Ventajas competitivas del producto y/o servicio

La ventaja competitiva de BLUEDICE se describe desde los siguientes aspectos:

- **Prestación de servicios Integrales**: Se buscará prestar servicios integrales que permitan al cliente cumplir con el objetivo de mantener los sistemas de gestión en el tiempo.
- **Entrega y continuidad de servicio**: Bluedice realizara la entrega del servicio adquirido junto con los resultados y recomendaciones para mantener activo el servicio en el tiempo sin que se tenga que pagar un mayor valor.
- **Precio**: De acuerdo con la investigación de las empresas que compiten en la misma industria, la empresa está por debajo del promedio. La finalidad en tener costos tan bajos es poder ofrecer los servicios a pequeñas empresas que no tienen la solvencia económica para contratar a grandes industrias.
- **Seguridad y certificaciones**: Bluedice garantizará a todos sus clientes respaldo en todos los procedimientos o servicios que se realicen, ya que los entregables a los clientes serán muy bien estructurados y lo primero que realizaremos es la certificación ISO27001y 90001as últimas novedades en torno a los controles de Seguridad, ciberseguridad y Riesgo.

2.9. Resumen de las inversiones requeridas

Se realiza un análisis financiero para la creación de empresa Bluedice en donde se realiza el siguiente análisis y definición:

Para iniciar el proyecto se requiere una inversión inicial de $21.441.666, de los que el equipo de emprendedores aporta $10.000.000 millones, quedando un saldo a solicitar al banco de $27.441.666, para contar con dicho valor se realizará un préstamo con una entidad bancaria para pagarlo en un tiempo de 1 año.

Al ser Bluedice una empresa de presentación de servicios de Seguridad, ciberseguridad y riesgos la inversión inicial no es tan alta ya que no se requiere de infraestructura tecnológica para la prestación de servicios.

La prestación de los servicios de Bluedice está enfocada principalmente en el manejo y conocimiento de los emprendedores, de acuerdo con el tipo de negocio que se pacte con el cliente se verificara la necesidad de contratar ingenieros por prestación de servicios para la ejecución de parte del proyecto lo que tampoco refleja un mayor gasto para la empresa.

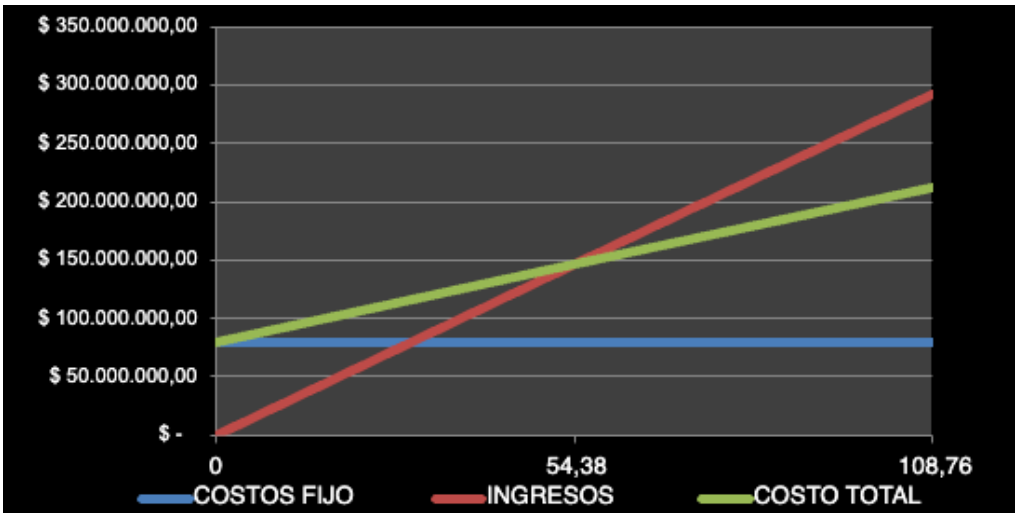
2.10. Proyecciones de ventas y rentabilidad

Se espera una tasa de evaluación de proyecto del 30% y se evidencia que este se lograra en un periodo de recuperación del 1,89 año, el valor presente Neto del emprendimiento se encuentra en $ 61,797.505 millones de pesos y la tasa interna de retorno está en un 84,90% lo indica la viabilidad económica del proyecto.

Según el análisis financiero, el punto de equilibrio se lograría cuando se realicen ventas mínimas de $ 145.993.363 millones de pesos.

En la siguiente imagen se puede visualizar el cruce del punto de equilibrio de la empresa Bluedice.

Imagen 6 - Punto de equilibrio



Fuente :Elaboración propia

En la siguiente tabla se relacionan los Ingresos y crecimiento porcentual de ventas, se detalla la proyección de ventas para el año 1 y el factor de crecimiento para los 4 años posteriores.

Imagen 7 - Tabla de Ingresos y crecimiento porcentual

	NOMBRE DEL PRODUCTO O SERVICIO	CANTIDADES	PRECIO DE VENTA UNITARIO SIN IVA	INGRESOS TOTALES		2025	2026	2027	2028
1	Implementacion de Sistemas de Gestión X proceso	25,00	$ 5.500.000,00	$ 137.500.000	34%	20,0%	30,0%	40,0%	43,0%
2	Bolsas de horas	280,00	$ 300.000,00	$ 84.000.000	21%	7,0%	10,0%	15,0%	20,0%
3	Auditoria por proceso	25,00	$ 1.800.000,00	$ 45.000.000	11%	15%	20%	25%	35%
4	Pruebas de Ciberseguridad alto nivel	25,00	$ 2.800.000,00	$ 70.000.000	17%	27%	35%	40%	50%
5	Pruebas de ingenieria Social	20,00	$ 1.700.000,00	$ 34.000.000	8%	25%	35%	40%	50%
6	Pruebas de Ciberseguridad aplicaciones Moviles	30,00	$ 1.300.000,00	$ 39.000.000	10%	25%	40%	45%	50%
			TOTAL	**$ 409.500.000**	**100%**				

Fuente :Elaboración propia

2.11. Conclusiones financieras y evaluación de viabilidad

Se realiza un análisis de los costos de los servicios de acuerdo con lo que se evidencia en el mercado, es de aclarar que la sustentación de los precios de los servicios ofrecidos por la empresa

se basa en un promedio de horas para la ejecución del servicio. El portafolio de servicios se encuentra estandarizado, una vez se realice el primer contacto con el cliente se evaluarán las necesidades y de allí se generará la propuesta ya que muchos de los servicios se ofrecen en conjunto y como proyecto no de forma individual.

Se espera que los ingresos de la empresa se generen por la ejecución de proyectos de implementación de sistemas de gestión, análisis de vulnerabilidades y ejecución de pruebas de ethical hacking, este tipo de servicios son los que más demanda el mercado y blue dice podría tener una buena partición en el mercado por la competencia de precios.

2.12. Equipo de trabajo

Juan David Parra, Profesional en Ingeniería en telecomunicaciones egresado de la universidad Cooperativa de Colombia con conocimientos en metodologías ágiles, implementación y seguimiento de proyectos en tecnología y análisis de gestión de riesgos. De acuerdo a lo anterior mi experiencia en procesos de implementación con empresas de diferentes industrias me permite tener una visión de la falta de conocimiento de las organizaciones y los controles que actualmente aplican para cerrar brechas tanto de seguridad, vulnerabilidad y cultura dentro de las mismas.

Claudia Liliana Carreño, Profesional en Administración de sistemas de Información, Certificado Auditor Líder ISO 27001:2013, ITIL, con experiencia en Implementación de Sistemas de gestión de Seguridad de la información, Sistemas de Gestión de Calidad, Análisis de riesgos de acuerdo con los lineamientos de la ISO 31000, y Sistemas de continuidad de negocio. La afinidad con este emprendimiento es el conocimiento adquirido y porque se evidencia en el mercado la necesidad de contar con personas con experiencia en la implementación, mantenimiento y mejora continua de sistema de Seguridad de la información, ciberseguridad y análisis de riegos.

Fabian Humberto Vergara, profesional en Ingeniería Eléctrica, con énfasis en Ingeniería de datos y background en la industria farmacéutica, ingestión de datos y procesamiento masivo de información en tiempo real, su afinidad con este proyecto es la capacidad de entender las necesidades de diferentes tipos de mercado y la segmentación de requerimientos basados en las crecientes aspiraciones empresariales de certificarse en diferentes solicitudes gubernamentales y estar protegidos contra amenazas entrantes al mercado y proteger la información de las compañías, su enfoque será el área comercial.

3. Análisis del sector

Colombia ha sido testigo de una extraordinaria evolución tecnológica en los últimos años, protagonizando cambios significativos que abarcan diversos aspectos de la sociedad. En el ámbito de la salud, la telemedicina ha experimentado un notorio incremento del 150%, posibilitando un acceso más eficiente a los servicios médicos, especialmente en regiones remotas. En el mundo laboral, plataformas de colaboración en la nube, como Microsoft Teams y Zoom, han registrado un impresionante aumento del 200%, y un 70% de las empresas han adoptado modelos de trabajo remoto de manera permanente [1].

La inteligencia artificial (IA) ha desempeñado un papel crucial en la mejora de la eficiencia en diversas industrias. La implementación de chatbots impulsados por IA en servicios al cliente ha generado un incremento del 30% en la satisfacción del cliente. Sectores como el financiero, el retail y la manufactura han experimentado transformaciones significativas gracias a la aplicación estratégica de la IA

En lo que respecta al cloud computing, este ha posibilitado que las empresas colombianas escalen sus operaciones de manera excepcional. El mercado de servicios en la nube ha experimentado un crecimiento anual del 25%, con un destacado aumento del 40% en la adopción de soluciones de infraestructura como servicio (IaaS).

- [1] https://www.minsalud.gov.co/Paginas/Colombia-es-pionero-en-transformacio-digital-del-sector-salud.aspx

Las herramientas de Software as a Service (SaaS) han redefinido la gestión empresarial de manera integral. Plataformas líderes como Salesforce, SAP y Slack se han convertido en pilares fundamentales para la gestión eficiente de ventas, recursos humanos y comunicación interna. El uso de herramientas SaaS ha aumentado mucho el 35 % en el último año, generando mejoras sustanciales en la productividad y una reducción significativa en los costos operativos.

Estos datos y cifras respaldan aún más la idea de negocia en la cual la tecnología y su aumento sin precedentes hace que cada vez más exista la posibilidad de una brecha de seguridad, y es importante resaltar que estas cifras son directamente proporcionales, es decir, a mayor número de (Desarrollos, aplicaciones, actualizaciones, cambios de frameworks, códigos), mayor (ataques, riesgos de seguridad, brechas de seguridad) existirán. Esto ratifica aún más que la misión de garantizar la protección y seguridad de todas las personas que utilizan este tipo de productos y servicio.

3.1. Análisis PESTEL

El análisis PESTEL permite identificar las variables a las que la organización se expone, ya que con esto se identifica cuáles son sus de amenazas y oportunidades.

Tabla 1 - Análisis PESTEL - Político

Político		
Descripción	**Amenaza/ Oportunidad**	**Calificación**
Nuevas leyes y/o regulaciones	O	Alto
Políticas gubernamentales	O	Medio
Cambios de gobierno.	A	Bajo

Acuerdos sectoriales.	O	Alto
Impuestos aplicables a empresas de consultoría	A	Medio

Fuente: Elaboración propia

Factor Político y legal: Regulaciones de Ciberseguridad

En Colombia, el factor político desempeña un papel fundamental en la forma en que las empresas operan, especialmente en el ámbito de la ciberseguridad y la protección de la información. En los últimos años, el gobierno colombiano ha intensificado sus esfuerzos para regular y proteger la infraestructura digital y los datos personales de los ciudadanos. Además de la Ley 1581 de 2012, que establece las bases para la protección de datos personales en el país, otra legislación relevante es la Ley 1273 de 2009.

La Ley 1273 de 2009 se centra en los delitos informáticos y establece sanciones y consecuencias legales para quienes realicen actividades delictivas en el ámbito digital, como la piratería informática, el acceso no autorizado a sistemas y la difusión de malware. Esta ley tiene como objetivo proteger la integridad de los sistemas de información y prevenir el ciberdelito. Las empresas en Colombia están obligadas a cumplir con esta ley y tomar medidas para salvaguardar su infraestructura digital.

Ambas leyes, la Ley 1581 de 2012 y la Ley 1273 de 2009, establecen requisitos y normativas específicas que las empresas deben cumplir en el manejo de la información y la seguridad cibernética. Estas regulaciones no solo son una respuesta a la creciente amenaza de la ciberdelincuencia, sino que también tienen como objetivo garantizar la privacidad y la seguridad de los datos en un mundo cada vez más digitalizado.

Aspectos políticos que también se deben tener en cuenta en el desarrollo de este proyecto tales como un cambio de gobierno, lo cual puede generar nuevas legislaciones o cambios estructurales que afecten el desarrollo normal de las operaciones. Adicionalmente el cambio de gobierno no solo en Colombia si no a nivel mundial puede cambiar el horizonte normativo.

Este marco legal ha generado una demanda creciente de servicios de seguridad de la información y ciberseguridad en Colombia. Las empresas buscan cumplir con estas regulaciones, proteger su información y evitar sanciones legales. Bluedice, al ofrecer servicios especializados en seguridad de la información y ciberseguridad, se posiciona de manera única para ayudar a las organizaciones a cumplir con estas regulaciones y proteger sus activos digitales.

Tabla 2 - Análisis PESTEL - Económico

ECONOMICO		
Descripción	**Amenaza/ Oportunidad**	**Calificación**
Fluctuaciones de la economía global	A	Medio
Recesión económica.	O	Alto
Crecimiento de mercado emergentes.	O	Medio
Políticas salariales y contratación.	A	Bajo
Aumento de impuestos.	A	Medio
Tasas de Cambio	O	Alto
Competencia en el mercado y precios de servicios similares	O	Alto

Fuente: Elaboración propia

Factor Económico: Crecimiento en la Demanda de Ciberseguridad

El factor económico en Colombia está experimentando una transformación significativa en el ámbito de la ciberseguridad. En los últimos años, el país ha sido testigo de un aumento constante en la demanda de servicios y soluciones de ciberseguridad. Este aumento en la demanda está impulsado por varios factores económicos clave.

En primer lugar, los costos asociados con los ciberataques se han vuelto más evidentes y significativos. Las empresas en Colombia están reconociendo el impacto financiero de los ciberataques, que incluye la pérdida de datos, la interrupción de las operaciones comerciales, el daño a la reputación y, en algunos casos, sanciones legales. La necesidad de proteger activamente la información y los sistemas digitales se ha vuelto una prioridad financiera y operativa.

Además, la creciente interconexión y digitalización de las empresas han expuesto a más organizaciones a las amenazas cibernéticas. Esto significa que empresas de todos los tamaños y sectores de la industria están buscando soluciones para mitigar estos riesgos. La conciencia sobre la importancia de la ciberseguridad se ha disparado en la comunidad empresarial, y las organizaciones están dispuestas a invertir en servicios especializados.

El sector financiero, la atención médica, el gobierno y las empresas de tecnología son algunos de los sectores clave que están invirtiendo en ciberseguridad. Las empresas se están dando cuenta de que no se trata solo de proteger sus activos digitales, sino también de mantener la confianza de los clientes y cumplir con las regulaciones gubernamentales en constante evolución.

En los últimos años, la demanda de ciberseguridad en Colombia ha experimentado un crecimiento significativo. Este crecimiento se debe a una serie de factores, entre los que destacan el aumento de la digitalización, la sofisticación de los ataques cibernéticos y el incremento de la concienciación sobre la importancia de la ciberseguridad.

Según un estudio publicado por la Cámara Colombiana de Informática y Telecomunicaciones (CCIT), en su artículo Estudio Anual de seguridad 2022-2023: "La demanda de servicios de ciberseguridad en Colombia creció un 40 % en 2022. Este incremento se debe a que las empresas y organizaciones colombianas están cada vez más conscientes de los riesgos cibernéticos y están adoptando medidas para proteger sus datos e infraestructuras.[2]"

Algunos de los factores que han contribuido a este crecimiento son los siguientes:

El aumento de la digitalización: Colombia es un país con una economía digital en crecimiento, lo que conlleva un incremento en la cantidad de datos que se almacenan y procesan en línea. Estos datos son más vulnerables a los ciberataques.

La sofisticación de los ataques cibernéticos: Los ciberdelincuentes están constantemente desarrollando nuevas técnicas y herramientas para atacar a las empresas y organizaciones. Estos ataques son cada vez más sofisticados y difíciles de detectar, lo que hace que sea más importante contar con medidas de ciberseguridad robustas.

El aumento de la concienciación sobre la importancia de la ciberseguridad: Las empresas y organizaciones colombianas están cada vez más conscientes de los riesgos cibernéticos y están tomando medidas para protegerse. Esto se debe, en parte, a las iniciativas gubernamentales y privadas para promover la ciberseguridad.

El crecimiento de la demanda de ciberseguridad en Colombia es un fenómeno positivo, ya que refleja el creciente interés que se le está dando a la ciberseguridad en el país. Sin embargo, también

---

[2] Tomado de: CCIT – Estudio Anual de Ciberseguridad (2023)

https://www.ccit.org.co/estudios/estudio-anual-de-ciberseguridad-2022-2023/

plantea desafíos, ya que el mercado de la ciberseguridad en Colombia es aún incipiente y hay escasez de profesionales capacitados en esta área.

Para abordar estos desafíos, es necesario que las empresas y organizaciones colombianas aumenten su inversión en ciberseguridad. También es necesario que el Gobierno colombiano fomente la formación de profesionales en ciberseguridad y que regule el sector de la ciberseguridad para garantizar que las empresas y organizaciones cuenten con los servicios de ciberseguridad necesarios.

Dentro del análisis y planteamiento inicial también se evaluó y contemplo variables del macroentorno las cuales pueden afectar o desviar el alcance financiero como la inflación la cual según el portal principal de la presidencia de Colombia: "Lo que lleva del año, es decir, de enero 2023 hasta octubre 2023 el porcentaje es del 10,48%[3]".

También se contempló una variación del dólar. Según la revisar "Portafolio", lo que lleva el año 2023 y sus múltiples variaciones se proyecta entre $4.183 y $4.250 pesos colombianos. Si bien, inicialmente el desarrollo de este proyecto será con herramientas Open Source y gratuitos, en el tiempo estas herramientas puede que tengan costos no proyectados.

---

[3] Tomado de: En 10,48% cierre de inflación anual a octubre de 2023, (2023) https://petro.presidencia.gov.co/prensa/Paginas/En-1048--cierre-de-inflacion-anual-a-octubre-de-2023--revel--el-DANE-231108.aspx

Tabla 3 -Análisis PESTEL - Social

Social		
Descripción	**Amenaza/ Oportunidad**	**Calificación**
Aumento de uso de nueva tecnología (Móvil e internet).	O	Alto
Teletrabajo.	O	Alto
Protección de datos personales	O	Medio
Imagen corporativa.	O	Medio
Tendencias y/o conciencia de los clientes potenciales.	O	Medio

Fuente: Elaboración propia

Factor social: concienciación sobre la ciberseguridad

La concienciación sobre la ciberseguridad está creciendo en Colombia. Esto se debe a una serie de factores, entre los que destacan:

El aumento de los ciberataques: En los últimos años, se han registrado un número creciente de ciberataques en Colombia, afectando a empresas, organizaciones y particulares. Estos ataques han tenido un impacto significativo, causando pérdidas económicas, daños a la reputación y violaciones de datos personales.

Ejemplo real: En septiembre de 2023, un ciberataque (Javeriana, 2023), afectó a más de 50 entidades gubernamentales y empresas privadas en Colombia, provocando la interrupción de servicios y el robo de información. El ataque, que se cree que fue llevado a cabo por un grupo de ciberdelincuentes rusos, afectó a la Rama Judicial, el Ministerio de Educación, la Policía Nacional y varias empresas de servicios públicos. El robo de información incluyó datos personales de

millones de ciudadanos colombianos, como números de identificación, direcciones, fechas de nacimiento, números de tarjetas de crédito, cuentas bancarias y direcciones de correo electrónico.

El ataque tuvo un impacto significativo en la vida de los ciudadanos colombianos. Más de 2,5 millones de personas tuvieron que cancelar sus tarjetas de crédito, cambiar sus contraseñas y tomar otras medidas para proteger su información personal. El ataque también provocó un debate sobre la ciberseguridad en Colombia, y llevó al Gobierno a tomar medidas para fortalecer la seguridad de las infraestructuras críticas.

La importancia de la información: La información es un activo cada vez más valioso, tanto para las empresas como para las personas. Los ciberataques pueden comprometer la confidencialidad, integridad y disponibilidad de la información, lo que puede tener consecuencias graves.

En enero del presente año, un grupo de ciberdelincuentes publicó en internet los datos personales de más de 100.000 ciudadanos colombianos, que habían sido robados de una empresa de servicios financieros. Los datos incluían números de tarjetas de crédito, cuentas bancarias y direcciones de correo electrónico. El robo de estos datos tuvo un impacto negativo en la vida de las personas afectadas. Más de 1.000 personas fueron víctimas de fraude, y algunas incluso tuvieron que declararse en bancarrota. El ataque también llevó a un aumento de la desconfianza en las empresas de servicios financieros, y provocó que más de 20.000 personas cambiaran de banco.

De acuerdo con la página de indicadores financieros el portafolio, En septiembre de 2023, una empresa de telecomunicaciones colombiana fue víctima de un ciberataque que provocó la interrupción de sus servicios de internet y telefonía. El ataque afectó a millones de usuarios en todo el país, que se vieron obligados a recurrir a otros medios para comunicarse y conectarse a internet. El ataque tuvo un impacto significativo en la vida de los ciudadanos colombianos. Más

de 10 millones de personas tuvieron que trabajar desde casa, o tuvieron que encontrar otros medios para comunicarse con sus familiares y amigos. El ataque también provocó un debate sobre la ciberseguridad en Colombia, y llevó a la empresa de telecomunicaciones a mejorar sus medidas de seguridad[4].

Tabla 4 - Análisis PESTEL - tecnológico Fuente: Elaboración propia

Tecnológico		
Descripción	**Amenaza/ Oportunidad**	**Calificación**
Innovación	O	Alto
Aumento de uso de la internet.	O	Medio
Uso de IoT	O	Medio
Uso de metadatos.	O	Medio
Inteligencia artificial	O	Alto

Fuente: Elaboración propia

Factor Tecnológico: Avances Tecnológicos y Detección de Amenazas

El factor tecnológico desempeña un papel crítico en el entorno de la ciberseguridad en Colombia. En el contexto de la ciberseguridad, se han producido avances tecnológicos

[4] Portafolio, (2023), A quiénes pertenece IFX, empresa del ciberataque que afecta al país https://www.portafolio.co/negocios/empresas/ifx-networks-quienes-son-los-duenos-de-la-empresa-que-recibio-ciberataque-tue-afecta-a-colombia-589134

significativos que influyen en la forma en que las organizaciones abordan la protección de la información y la mitigación de amenazas cibernéticas.

Un ejemplo destacado de estos avances tecnológicos es el desarrollo y la adopción de soluciones de inteligencia artificial (IA) para la detección de amenazas. Las soluciones de IA utilizan algoritmos avanzados y aprendizaje automático para analizar el tráfico de red y el comportamiento del usuario en busca de patrones sospechosos o anómalos que puedan indicar posibles ataques cibernéticos. Esta tecnología permite una detección más temprana y precisa de amenazas, lo que resulta en una mayor eficacia en la prevención y respuesta a incidentes La automatización también desempeña un papel destacado en el campo de la ciberseguridad. Herramientas como la automatización de respuestas a incidentes permiten a las organizaciones reaccionar de manera más rápida y efectiva ante las amenazas, reduciendo el tiempo de inactividad y el impacto de los ataques. La incorporación de tecnologías avanzadas en los servicios de seguridad de la información puede mejorar la capacidad de una empresa como Bluedice para brindar protección proactiva a sus clientes.

La evolución de las amenazas cibernéticas es un factor tecnológico adicional. A medida que los ciberdelincuentes desarrollan nuevas tácticas y herramientas más sofisticadas, las empresas deben mantenerse al día con las últimas tendencias en ciberseguridad. Esto incluye la detección y mitigación de amenazas emergentes, como el ransomware, los ataques de día cero y el phishing, que requieren soluciones tecnológicas avanzadas para contrarrestarlos.

Bluedice puede aprovechar estos avances tecnológicos al ofrecer servicios de seguridad de la información que estén a la vanguardia de la ciberseguridad. Al mantenerse al día con las últimas tecnologías y tendencias en ciberseguridad, la empresa puede brindar a sus clientes soluciones efectivas y avanzadas que les ayuden a proteger sus activos digitales en un entorno tecnológico en

constante evolución. El factor tecnológico influye en la necesidad de servicios de ciberseguridad de vanguardia y en la oferta de Bluedice inicialmente en el mercado colombiano.

Tabla 5 - Análisis PESTEL - Ecológico

Ecológico		
Descripción	**Amenaza/ Oportunidad**	**Calificación**
Desastres naturales	O	Medio
Eventos climáticos.	O	Medio
Responsabilidad social empresarial	O	Alto
Conciencia social sobre el impacto ambiental y la importancia de la sostenibilidad	O	Bajo

Fuente: Elaboración propia

Factor ecológico: La ciberseguridad y el cuidado del medio ambiente

La protección del medio ambiente en la actualidad está en crecimiento y es allí en donde las empresas dedicadas al cuidado y mantenimiento del medio ambiente desde sus diferentes perspectivas velan por el cuidado de sus sistemas en los cuales la preservación de la información es de gran importancia ya que el análisis histórico puede ayudar a predecir cambios en el comportamiento climático que apalanquen el beneficio y cuidado de las industrias y las personas.

Es allí en donde la Ciberseguridad juega un papel importante pues los sistemas de las empresas de predicción climática, de suministro de agua, energía y petróleo debe cuidar de los datos que manejan en los sistemas con el fin de no generar ningún tipo de perdida ya que pueden afectar su sostenibilidad y preservación, un ejemplo de ello es lo que dice ***cronup*** en su blog ***Ciberataques con consecuencias reales: ¿cómo la ciberdelincuencia afecta al medio ambiente?***

(Ciberseguridad, 2023), se debe tener en cuenta que los ciberdelincuentes ya no solo buscan generar un cobro por un ataque cibernético, sino que van un poco más allá y lo que buscan es desestabilizar los sistemas por medio del robo de información.

Tabla 6 - Análisis PESTEL - Legal

Legal		
Descripción	**Amenaza/ Oportunidad**	**Calificación**
Leyes de Seguridad de la información y ciberseguridad.	O	Alto
Leyes de protección de datos personales.	O	Alto
Cláusulas de cumplimiento a nivel de seguridad y Ciberseguridad.	O	Alto
Regulaciones específicas de las industrias de los clientes.	O	Alto

Fuente: Elaboración propia

Factor Legal: Creación de nueva normatividad

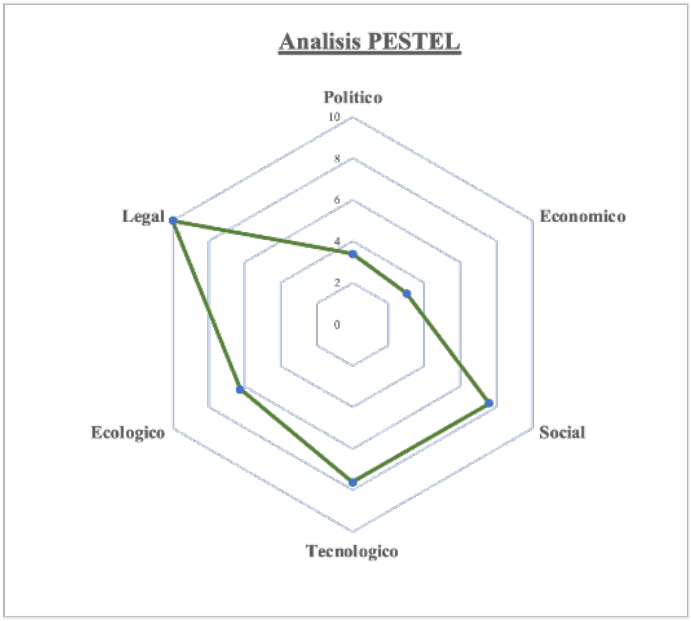
Hoy día en Colombia es importante que todas las organizaciones cumplan con el reporte de la Base de datos que indica la ley 1582 en temas de datos personales, después de la pandemia se ha evidencia como para mucha organización es de gran importancia el cumplimiento normativo en temas de Seguridad de la información, Ciberseguridad y Riesgos.

Hoy día es importante que las organizaciones que prestan algún tipo de servicio se encuentren certificadas en ISO 27001, para ello se puede evidenciar actividades como lo es ser proveedor tecnológico para servicios de facturación electrónica lo cual se describió inicialmente en la

resolución 2242 de 2015, la superintendencia Financiera a las entidades vigiladas les exige el cumplimiento de los descrito en la circular 029 y en la circular 007. Es por ello por lo que se evidencia el crecimiento y la oportunidad de la prestación de servicios de seguridad de la información, ciberseguridad y riesgos.

En la actualidad fue radicado frente al congreso de Colombia un proyecto de Ley en el cual se busca la creación de la Agencia Nacional de Seguridad Digital y Asuntos Espaciales (Mintic, 2023)[5], en caso de que este proyecto de ley sea aprobado, se observa la importancia y el crecimiento que está dando el país para buscar estrategias que permitan a las organizaciones cumplir con la protección de la información.

Imagen 8 - Grafico análisis PESTEL



Fuente: Elaboración propia

[5] https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/277156:Ante-el-Congreso-fue-radicado-el-Proyecto-de-Ley-para-crear-la-Agencia-Nacional-de-Seguridad-Digital-y-Asuntos-Espaciales

De acuerdo con lo que se observa en *Imagen* 8 se resaltan fortalezas en los siguientes factores:

Factor social: Se identifica que los crecientes ataques de ciberseguridad en Colombia, y la necesidad que tienen las empresas de proteger los datos claves de negocio y sus activos ofrecen una ventaja competitiva en la que Bluedice puede tener participación ya que ayudara a las empresas y a sus entornos a proteger los activos más valiosos, así como controlar lo riesgos a los que estos se ven expuestos.

Factor Legal: Se evidencia que el marco legal en Colombia está en aumento y apalanca el crecimiento de las organizaciones que ofertan servicios de Seguridad de la Información, Ciberseguridad, riesgos y continuidad de negoció ya que se apalanca en la normatividad vigente como lo es la Ley 1581 de 2012, Ley 1273 de 2009, Circular 009, 005 y 007 de la Superintendencia Financiera, Resolución 2242, entre otras, La importancia de la protección de datos en Colombia, que ha llevado a las empresas a una creciente necesidad de certificarse para cumplir los requisitos mínimos que estas leyes declaran para la operación y prestación de servicios.

Factores tecnológico: El Uso de tecnologías Emergentes como lo es los servicios SAS, PASS, LASS y la Inteligencia Artificial han desarrollado nuevas amenazas para las organizaciones, Bluedice ha tomado estas nuevas tecnologías a su favor con la adopción de soluciones de inteligencia artificial (IA) para la detección de amenazas, la automatización de respuestas a incidentes, y la adaptación a la evolución de las amenazas cibernéticas, adicionalmente buscara apalancarse con diferentes proveedores de herramientas de seguridad que permitan controlar y asegurar la información y la continuidad del negocio cumplimento con los controles indicados en la Norma ISO 27001:2022, ISO 31000:2015 y la NIST.

El factor económico se ve como un punto a considerar para Bluedice, debido a Fluctuaciones de la economía global, recesión económica y el aumento de impuestos, los cuales impactan directamente el modelo de negocio de Bluedice y sus aspiraciones de crecimiento acelerado

De acuerdo con el análisis anterior se puede evidenciar que el valor generado por cada uno de los factores de la Matriz PESTEL son clasificados como una oportunidad para el crecimiento y posicionamiento de Bluedice en la prestación de servicios de seguridad, ciberseguridad y riesgos.

3.2. Análisis Porter

Las 5 fuerzas de Porter es un componente estratégico de gran importancia para Bluedice ya que permite analizar e identificar la negociación que hay entre proveedores, clientes, competidores y productos sustitutos.

Durante el análisis se valorarán las oportunidades y amenazas que presenta la empresa frente a cada una de las fuerzas con el fin de plasmar estrategias que permitan apalancar el crecimiento y posicionamiento del negocio en el mercado, el ofrecimiento de servicios seguridad y la ciberseguridad cuenta con competidores de alto nivel que no son de fácil alcance para la pequeñas y medianas empresas que son el mercado en el cual Bluedice desea ingresar.

Es importante determinar que en la actualidad existe un gran mercado para el ofrecimiento de servicios de Seguridad de la información, Ciberseguridad, análisis de riesgos entre otros teniendo en cuenta que los entes regulatorios han establecido requisitos y estándares de seguridad para el ofrecimiento de servicios específicos los cuales deben contar con sistemas seguros y que tenga dentro de su oferta de valor la seguridad de los datos.

En la siguiente *Tabla 7* se evidencia las oportunidades y Amenazas en las que se encuentra la empresa frente a estas 5 Fuerzas.

Tabla 7- Fuerzas de Porter – Poder de los compradores

Definición y Valoración de Oportunidades y Amenazas

5 FUERZAS DE PORTER		**Oportunidades**		**Amenazas**	
Poder de los compradores	**Los compradores tienen más poder cuando:** Los vendedores son pocos y pequeños y los compradores pocos y grandes. Los compradores adquieren grandes cantidades. Un comprador individual es un gran cliente. Los compradores pueden cambiar proveedores a bajo costo. Los compradores compran de múltiples vendedores a la vez. Los compradores pueden	**1**	Precios a la medida de las necesidades del cliente	**1**	Competencia desleal entre canales
		2	Buen relacionamiento entre el comercial y el cliente	**2**	Análisis de cliente para el ofrecimiento del servicio VS el precio
		3	Soporte personalizado de la empresa al cliente	**3**	El cliente puede buscar soluciones de seguridad y ciberseguridad más económicas, lo que podría generar presión para reducir precios y márgenes de ganancia.

integrarse fácilmente hacia atrás.	**4**	Entregables del servicio al cliente, informes de mejores prácticas, diseños, recomendaciones y oportunidades de mejora.	**4**	solicitud de condiciones contractuales desfavorables, como garantías extensas o plazos de pago prolongados que permiten que la empresa tenga que conseguir más cliente para subsidiar las condiciones del cliente.
	5	Customización de servicios.	**5**	Posibilidad de que el cliente cambie a otros competidores si no están satisfechos con los servicios o soluciones ofertados por BlueDice.

Fuente: Elaboración propia

Poder de los compradores en la actualidad existe un gran número de clientes potenciales, se observa como una oportunidad poder brindar servicios de Seguridad de la información, ciberseguridad y análisis de riesgos ya que Bluedice ofrece este tipo de soluciones de forma costo efectivas en el cual se busca garantizar la satisfacción del cliente y la recontratación de nuevos servicios.

También es importante visualizar la poca facilidad que pueden tener los compradores para poder integrar servicios de seguridad, ya que en algunas ocasiones la implementación exitosa de estrategias de seguridad cibernética requiere conocimientos especializados que la organización no va a poder solucionar de forma integral y requerirá la contratación de este tipo de servicios.

Tabla 8 - Fuerzas de Porter – Competidores Potenciales

Definición y Valoración de Oportunidades y Amenazas

5 FUERZAS DE PORTER	Oportunidades		Amenazas	
Nuevos competidores / potenciales	**Los competidores entrantes (a la industria) amenazan a las compañías establecidas.** Barreras al ingreso: Lealtad de marca Ventajas absolutas de costo	**1**	Experiencia en el mercado de Seguridad de la información, ciberseguridad y análisis de riesgos	**1** Competidores con los mismos servicios a precios más bajos
		2	Generar alianzas estratégicas	**2** Ingreso de nuevas empresas tecnológicas con

Economías de escala Costos ínter cambiantes Normativas Gubernamentales		con otros competidores para contar con mayores servicios.		soluciones innovadoras que puedan competir en precio y calidad.
Las barreras al ingreso reducen la amenaza de nueva competencia	**3**	No existe un sesgo de producto de Software	**3**	Posibilidad de que los nuevos competidores aprovechen la tecnología emergente y desafíen la experiencia y reputación de las pequeñas empresas en seguridad y ciberseguridad.

Fuente: Elaboración propia

Bluedice visualiza como oportunidad la experiencia que se tiene a nivel general en la implementación de sistemas de seguridad, ciberseguridad y análisis de riesgos, al igual que está en la búsqueda de alianzas estratégicas que permitan ofrecer servicios de forma integral de acuerdo a las necesidades y expectativas de los clientes, también es importante mencionar que Bluedice

busca tener soluciones efectivas que permitan mitigar las diferentes amenazas a las que se puede ver expuesta por la llegada de nuevos competidores.

Tabla 9- Fuerzas de Porter – Rivalidad entre los competidores

Definición y Valoración de Oportunidades y Amenazas

5 FUERZAS DE PORTER		Oportunidades		Amenazas
Rivalidad entre los Competidores	**La intensidad de la rivalidad competitiva en una industria surge de:** La estructura competitiva de la industria. Las condiciones de la demanda (crecimiento o declinación) en la industria. El tamaño de las barreras de salida en la industria.	**1** Experiencia en temas especializados	**1**	Competidores más grandes y establecidos que pueden ofrecer una gama más amplia de soluciones y tener una mayor capacidad para bajar los precios o invertir en marketing.
		2 Consultoría a la medida del cliente	**2**	Presión en los márgenes de ganancia debido a la intensa competencia en precios y servicios.

3	Aumento de mercado de clientes.	**3**	Riesgo de perder clientes existentes ante competidores que ofrecen soluciones similares o superiores.
4	Generar alianzas estratégicas que permitan ampliar la cantidad de servicios prestados por Bluedice con el fin de consolidar mercado.	4	Pérdida de clientes por competencia desleal.

Fuente: Elaboración propia

Bluedice dentro de las oportunidades que observa para la penetración en el mercado en cuanto a la rivalidad con sus competidores, buscara generar alianzas estratégicas que permitan ampliar los servicios ofrecidos en su portafolio brindado integralidad a las solicitudes de los clientes, también genera servicios especializados y consultoría de acuerdo con cada una de las necesidades y requerimientos.

En la actualidad en Colombia existen varias empresas que ofrecen servicios de seguridad de la información, ciberseguridad y riesgos, se observa que al ser servicios especializados el costo tiene a ser altos y las pymes no cuentan con el rubro económico para poder implementar estos sistemas de información.

Tabla 10 - - Fuerzas de Porter - Poder de negociación con los Proveedores

Definición y Valoración de Oportunidades y Amenazas

5 FUERZAS DE PORTER		Oportunidades		Amenazas	
Poder de Negociación con los Proveedores	**Los proveedores tienen poder de negociación si:** Sus productos tienen pocos sustitutos y son importantes para los compradores. La industria del comprador no es un cliente importante para el proveedor. La diferenciación hace costoso que los compradores cambien de proveedor. Los proveedores pueden integrarse hacia delante y competir con los compradores, y estos no pueden integrarse hacia atrás para llenar sus necesidades.	**1**	Pocos Proveedores con precios a demanda	**1**	Precios Fijos
		2	realizar relaciones con múltiples proveedores con el fin de dar lugar a opciones de precios más competitivas y un acceso más amplio a tecnologías y servicios de seguridad de la información,	**2**	Riesgo de depender de un número limitado de proveedores para tecnologías o servicios clave, lo que podría resultar en un mayor costo o falta de disponibilidad en caso de conflictos con los proveedores.

	ciberseguridad y riesgos.		
3	Construir acuerdos a largo plazo con los proveedores. permitiendo que se tengan colaboraciones en la innovación y el desarrollo de soluciones de seguridad personalizadas.	**3**	Posibilidad de enfrentar aumentos de precios por parte de proveedores dominantes, lo que puede reducir los márgenes de ganancia de la PYME.
4	Buscar nuevas oportunidades de mercado en regiones geográficas no explotadas.	**4**	Dificultad para encontrar proveedores alternativos que cumplan con los requisitos específicos de seguridad y ciberseguridad.

Fuente: Elaboración propia

Es de gran importancia que la empresa busque alternativas confiables y seguras para negociar con los proveedores y poder generar servicios con desarrollos personalizados de acuerdo a las necesidades y expectativas de los clientes, la búsqueda nuevas oportunidades de mercado en diferentes zonas que no se cuenten servicios de seguridad de la información, ciberseguridad y riesgos se observa como una oportunidad para la exploración de nuevos mercados, que son zonas en las cuales los competidores no tiene una alta acogida por los costos altos que se manejan.

Tabla 11 - Fuerzas de Porter - Productos sustitutos

Definición y Valoración de Oportunidades y Amenazas

5 FUERZAS DE PORTER		Oportunidades	Amenazas
Productos sustitutos	**La amenaza competitiva de los productos sustitutos incrementa conforme se acercan en su capacidad de llenar necesidades de los clientes.**	**1** Consultoría especializada y a la medida del cliente	**1** Sustitutos a nivel de precio
		2 Diversificación de servicios para abordar no solo las amenazas cibernéticas, sino también otras necesidades como seguridad física, formación de empleados en ciberseguridad, auditoría de cumplimiento, cumplimiento normativo, entendimiento y análisis de riesgos SARE, SARO entre otros.	**2** Riesgo de que los clientes opten por soluciones alternativas de seguridad y ciberseguridad, como el software de código abierto o enfoques menos convencionales.
		3 Generar procesos de formación y sensibilización en cultura de seguridad prevención de amenazas cibernéticas y el	**3** Posibilidad de que surjan nuevas tecnologías o métodos que ofrezcan una forma más efectiva o económica de abordar los desafíos de seguridad, lo que

	cumplimiento de políticas internas de seguridad de la información y protección de datos.	podría disminuir la demanda de los servicios de la PYME.

Fuente: Elaboración propia

El campo de la seguridad de la información ha venido en aumento, la implementación de tecnologías emergentes por parte de la organización al migrar gran parte de los servicios a la nube, ha permitido que se desprendan una gran cantidad de oportunidades para ampliar los servicios con los que Bluedice puede apalancar el crecimiento de clientes en el mercado, buscar cerrar la brechas de seguridad por medio de servicios de entrenamiento y simulaciones de seguridad pueden permitir que gran parte de las organizaciones pequeñas vean como una oportunidad para implementar estrategias seguras en sus organizaciones.

Realizar alianzas estrategias con diferentes sectores y con el ministerio de las TIC con el fin de buscar procesos de innovación y nuevas alternativas de aprendizaje permitirán que la Bluedice pueda garantizar su permanencia en el mercado con la adquisición de nuevos conocimiento y nuevas experiencias.

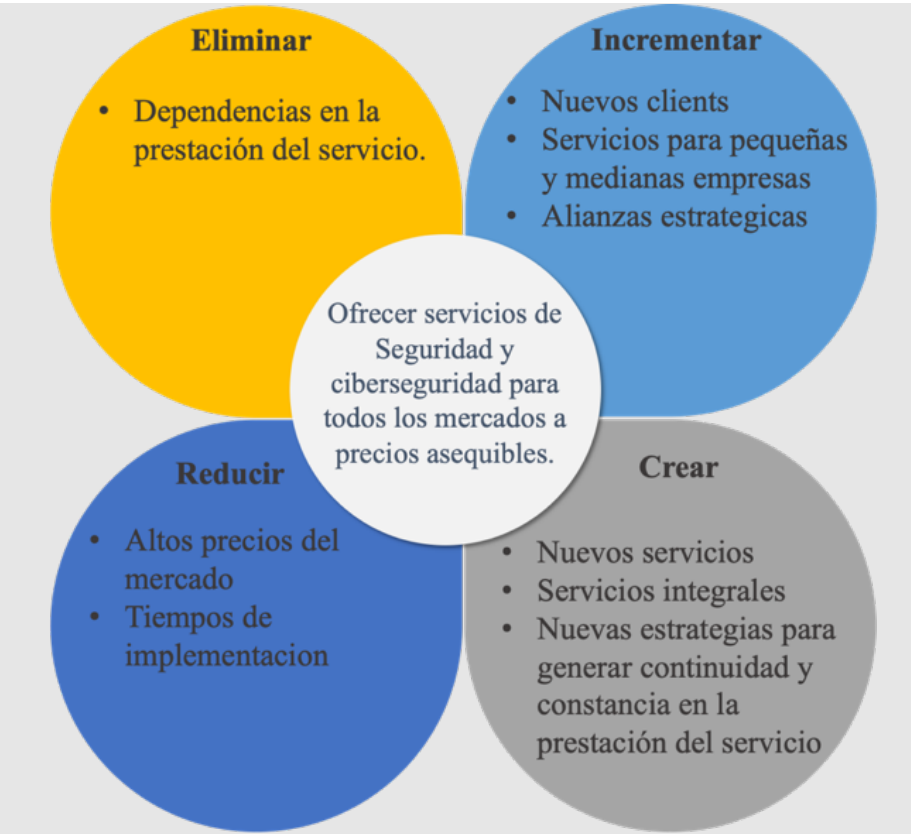
Para concluir se puede decir que la aplicabilidad de las 5 fuerzas de PORTER permite identificar que la empresa no cuenta con un alto poder de negociación con proveedores, ya que no se manejan muchos proveedores, en cuanto al poder de negociación con los clientes se identifica que los servicios que presta la empresa a sus clientes son hechos a la medida de acuerdo con las necesidades y requerimientos de sus clientes.

En Bluedice se planea implementar estrategias que permitan la entrada de la empresa en el mercado Colombiano teniendo como oferta de valor el permitir que todas las organizaciones

puedan acceder a servicios de seguridad, ciberseguridad y análisis de riesgos a precios asequibles, actualmente se evidencia como se puede dar apertura al mercado de las pequeñas y medianas empresas con el manejo de diferentes servicios para que puedan ir cumpliendo los requisitos regulatorios e ir al paso de mercado sin que puedan ser descalificados por no cumplir requisitos de protección de datos personales, cuidados de información de cliente, continuidad de negocio o análisis de riesgos.

A continuación, se puede identificar el esquema de los cuatros acciones de la estrategia de BLUEDICE

Imagen 9 - Esquema acciones estrategia Océano azul



Fuente: Elaboración propia

De acuerdo a la estrategias de Océano azul Bluedice busca reducir los altos costos que existen en el mercado por parte de los otros competidores pues actualmente pagar por consultorías en servicios de seguridad y ciberseguridad son bastantes altos ya que la mayoría de empresas que implementan estos tipos de sistemas son aquellas que cuentan con alto flujo de caja en las que sus procesos requieren inversiones para proteger sus sistemas, es importante tener en cuenta que no solo es la reducción de costos sino la reducción de tiempos de implementación.

Bluedice busca crear servicios integrales que permitan al cliente asegurar de una manera completa sus sistemas o los servicios contratados, se espera poder eliminar la dependencia para la prestación de los servicios es decir que si el cliente contrata análisis de vulnerabilidades se pueda ofrecer un paquete completo que permita realizar todo el ciclo completo desde el análisis hasta la mitigación de este ofreciendo calidad en la prestación de los servicios a precios costo- eficientes.

En la implementación de la estrategia del océano azul Bluedice creara estrategias para fortalecer la creación de empresa en el mercado de la seguridad de la información, ciberseguridad y Riesgos con las siguientes acciones:

A. Crear nuevos espacios de mercado que permitan reconocer a Bluedice como una empresa que presta servicios de Seguridad de la información, ciberseguridad y Riesgos.
B. Generar propuestas con el portafolio de servicio inicial (Assesment) y una vez se generen oportunidades contractuales con los clientes se mostrará los nuevos servicios ofertados por Bluedice que generar sentido con las necesidades del negocio y del entorno en los que se mueve el cliente actualmente.

C. Generar procesos de atracción de cliente por medio de Sensibilizaciones que permitan a los clientes conocer las nuevas tendencias de Seguridad de la información, Ciberseguridad y riesgos.

D. Durante el proceso de la creación de la empresa se buscará fortalecer el relacionamiento con entidades gubernamentales con el fin de generar conciencia (talleres, Mesas de trabajo colaborativas) sobre el manejo de la ciberseguridad en el cuidado de los datos personales.

E. Participar activamente en los talleres de formación generados por los proveedores de soluciones de seguridad con el fin de ampliar conocimiento para el mejoramiento e innovación del portafolio actual de servicios ofrecidos por Bluedice.

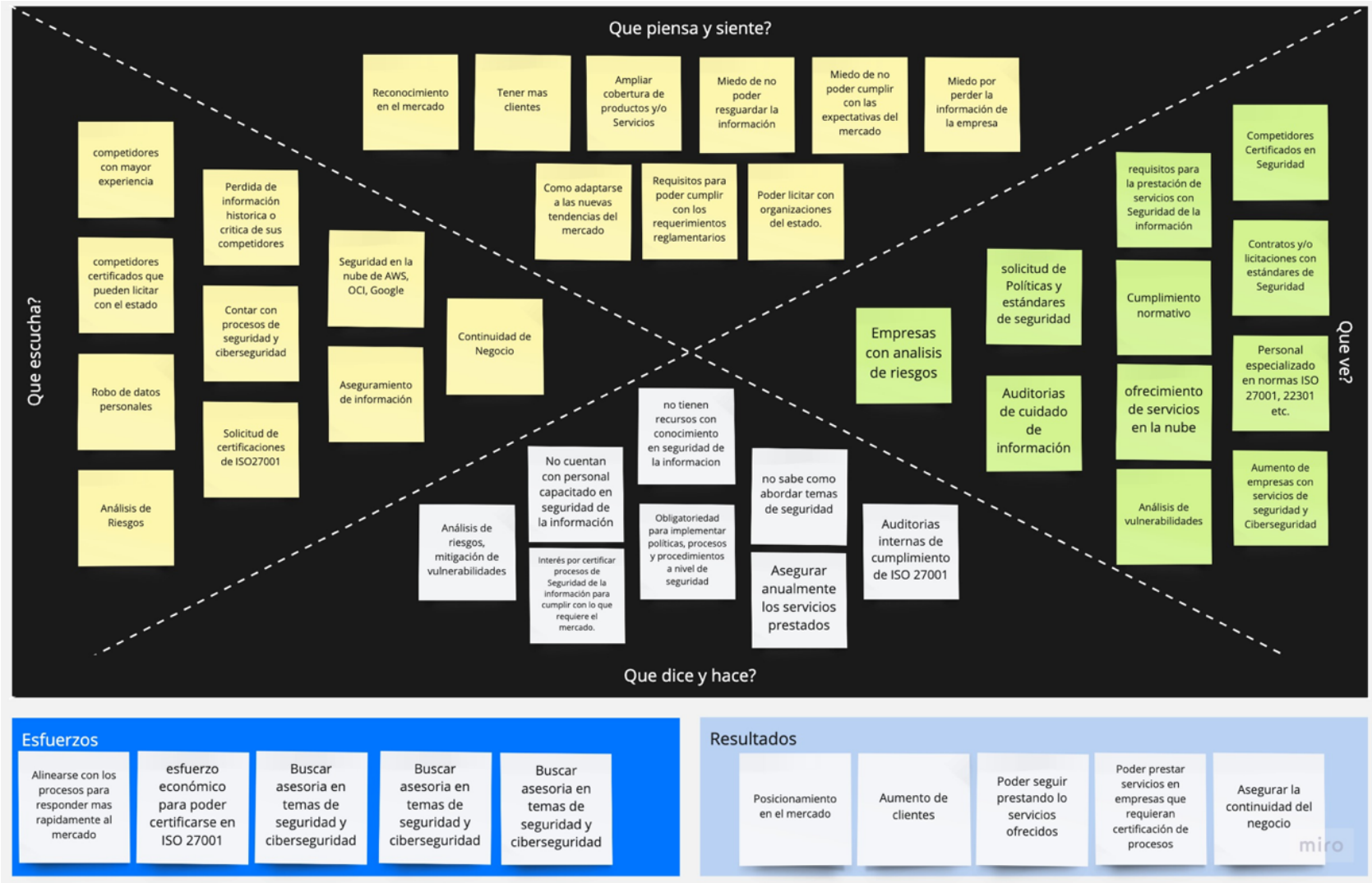
4. Estudio piloto de mercado

4.1. Análisis y estudio de mercado

El aumento de los ciberataques a los que están expuestas las organizaciones hacen que busquen de forma constante estrategias para proteger su información, sin duda alguna el Covid-19 ha influido en el mercado de la seguridad de la información , la ciberseguridad y el análisis de riesgos, el incrementó el Teletrabajo, la migración de los servicios a Internet y la aceleración del mercado ha hecho que las organizaciones busquen la forma de fortalecer sus sistemas y protegerlos de robo o perdida de información.

De acuerdo a lo anterior se realiza la creación de un mapa de Empatía en el cual se puede identificar que escucha, piensa y cree las organizaciones en torno a la implementación de la políticas, procesos , procedimientos de Seguridad de la información, ciberseguridad y riesgos, es allí en donde se evidencia que Las empresas actuales buscan tener dentro de su presupuesto una parte para la protección de datos y así poder robustecer sus sistemas y protegerlos de modalidades como Vishing, suplantación de identidad y smishing las cuales son una de las principales formas usadas por los delincuentes cibernéticos para el robo de información, tanto las empresas como las personas naturales cada día buscan más alternativas para controlar la pérdida o robo de información

Imagen 10 - Mapa de Empatía



Fuente: Elaboración propia

El cliente ideal para BlueDice, se define en las siguientes características:

Necesidades y Metas

- Garantizar la seguridad de los datos confidenciales de la empresa.
- Cumplir con las regulaciones y estándares de seguridad del sector financiero.
- Identificar y mitigar vulnerabilidades en la infraestructura de TI.
- Obtener certificaciones reconocidas para validar la seguridad de la empresa.

Frustraciones y Dificultades:

- Falta de tiempo para dedicarse a la gestión exhaustiva de la seguridad.
- Presión para cumplir con los requisitos normativos en constante evolución.
- Incertidumbre sobre cuál es el mejor enfoque para abordar las vulnerabilidades.
- Preocupación por la posibilidad de sufrir un ciberataque que afecte la reputación de la empresa.

Influencias Externas:

- Directivos de la empresa que priorizan la seguridad como un elemento clave del negocio.
- Presión competitiva de otras empresas del sector que están mejorando su postura de seguridad.
- Noticias sobre violaciones de datos y ciberataques en empresas similares.

Fuentes de Información:

- Revistas especializadas en seguridad informática.

- Conferencias y eventos de ciberseguridad.
- Recomendaciones de colegas en la industria de la seguridad.
- Consultores externos en ciberseguridad.

Emociones y Sentimientos:

- Ansiedad por la posibilidad de sufrir una brecha de seguridad.
- Determinación por proteger los activos digitales de la empresa.
- Expectativa de encontrar un socio de confianza en seguridad cibernética.
- Necesidad de tranquilidad y certeza en cuanto a la protección de los datos de la empresa.

4.2. Perfil de persona

Imagen 11 - Perfil de Persona

Fuente: Elaboración propia

De Acuerdo con la *Imagen 11* el perfil de persona permite identificar gustos, intereses y necesidades con el fin de adaptar los productos y servicios de la empresa hacia

Se realizan entrevistas realizadas con el experto técnico, aliado clave, empresario y clientes se pudieron identificar los siguientes hallazgos para tener en cuenta para el desarrollo del emprendimiento:

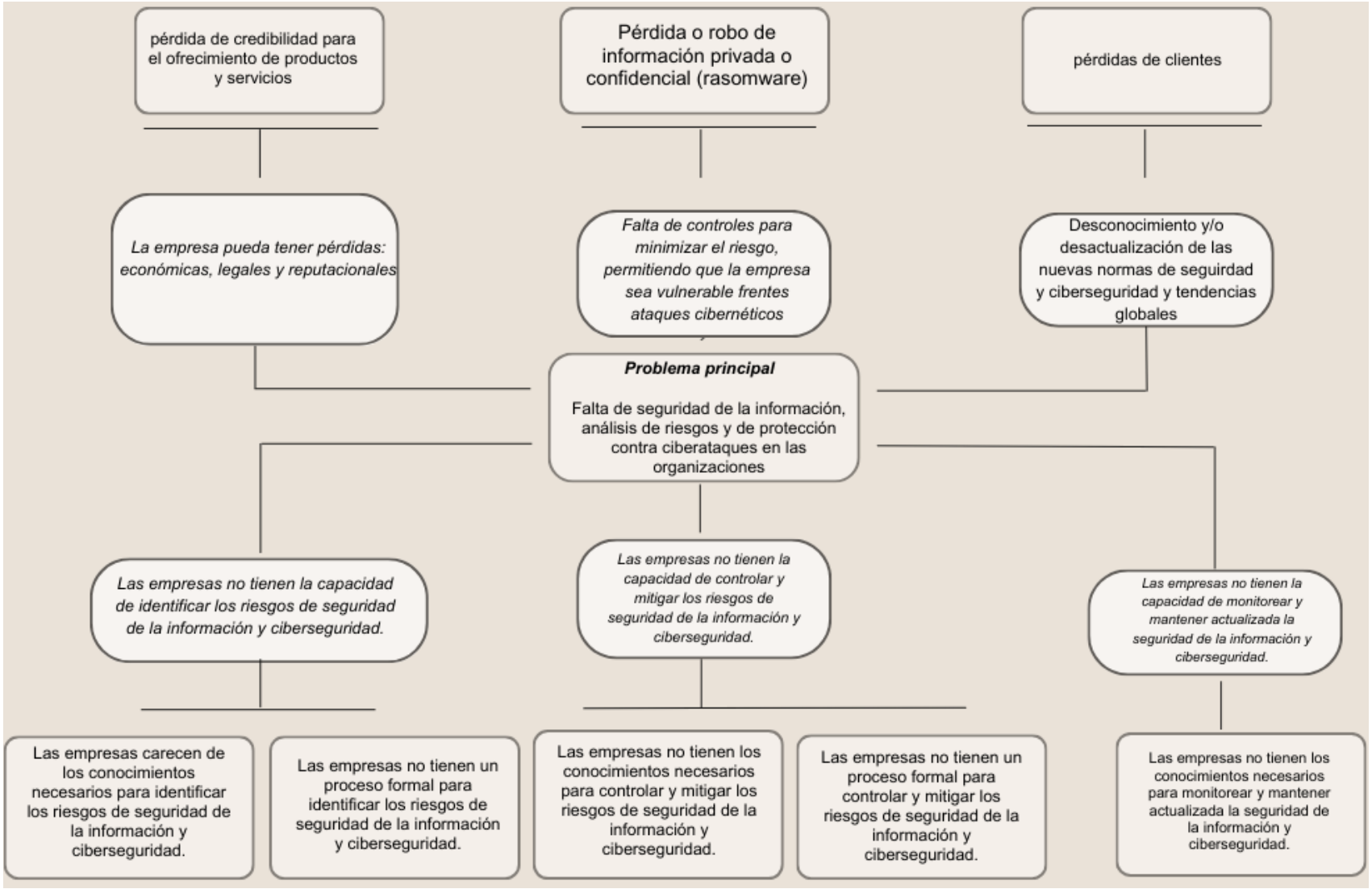
A. El experto técnico considera que la idea de negocio está bien encaminada, considera que para iniciar se pueden manejar los servicios planteados, pero es importante a
B. Actuar frente a los requerimientos del cliente.
C. Se debe tener en cuenta que inicialmente el conocimiento del negocio será por la voz a voz de las personas del medio conocidas.
D. El experto técnico realiza una observación en cuanto a los costos de los servicios ya que inicialmente Bluedice piensa realizar cobro por hora de consultoría, lo cual se debe replantear teniendo en cuenta que los costos por hora son muchos más altos y la consultoría se puede volverse un proyecto el cual es viable realizar un cobro por la totalidad más no por horas para tener mayor control de cliente.
E. En la sesión realizada con el aliado clave se identificó que es de gran importancia contar con aliados clave para los procesos de seguridad y ciberseguridad, en el planteamiento inicial no se identificó el manejo de aliados claves como empresas para el análisis de riesgos en temas de Seguridad de la información.
F. A nivel general con todos los entrevistados se identifica que es importante ofrecer servicios de capacitación y/o sensibilización con el fin de apalancar la postura de seguridad de la información.

G. En la sesión con el cliente se logró identificar que para las organizaciones la tercerización de algunos procesos de seguridad de la información y ciberseguridad es de gran importancia ya que lo que realmente que buscan es especializarse en su nicho de negocio y no asignar otros roles que son apoyo y requieren una recarga laboral bastante amplia.

H. Durante el proceso de entrevistas se identifica que muchas empresas, personas, aliados buscan compañías que manejen servicios de forma integral a nivel de seguridad de la información y Ciberseguridad ya que en algunas ocasiones se evidencia especialización y no ampliación de portafolio de servicios.

I. Se evidencio durante el proceso de entrevistas a nivel general que el dolor más grande que presentan las organizaciones está en el dominio de la sensibilización del Talento humano y en la materialización de incidentes de Seguridad y ciberseguridad ya que las empresas por lo general temen al daño reputacional o a la penalización por el incumplimiento de los acuerdos de servicio planteados entre empresa y cliente ya que no manejan esquemas de crisis para dar a conocer este tipo de incidencias.

Imagen 12 - Árbol de problemas



Fuente: Elaboración propia

Para la validación de la hipótesis se planteó el siguiente árbol de problemas en el que de manera grafica permite representar e identificar claramente el problema, allí se desglosan las causas y los efectos generados en los interesados por la no solución a tiempo de los problemas presentados

4.3. Descripción de los consumidores Ficha técnica de encuesta

Se realiza una descripción de los consumidores por medio de una encuesta con el fin de realizar un sondeo de Mercado de servicios de Seguridad de la Información y Ciberseguridad, se evidencia que en Colombia se espera un crecimiento en promedio del 80% de servicios de seguridad de la información, ciberseguridad y riesgos, esto teniendo él cuenta que el uso de la inteligenciar artificial, la exposición de datos personales en la red, el uso de los servicios SAAS y las nubes esta crecimiento lo que hace que cada vez las organizaciones estén expuestas a cambios tecnológicos y gubernamentales lo que los obliga a mantener su información protegida.

Dentro del segmento o las características que se tuvieron en cuenta para la selección de las empresas, se contemplaron los siguientes ítems:

- Pequeñas y medianas empresas
- Empresas en la ciudad de Bogotá
- Empresas enfocadas o especializadas en tecnología
- Prestadoras de servicios tecnológicos

Por correo electrónico se lograron contactar a más de 100 empresas con estas mismas características. Del total de las empresas se logró tener una tasa de apertura del 58% y solo un 31% del segmento logró finalizar las encuestas.

Objetivo de la encuesta
Identificar las diferentes variables del mercado por las cuales se guían las empresas para seleccionar un proveedor que ofrezca servicios de Seguridad de la información, ciberseguridad y riesgos.
Tamaño de la muestra
31 compañías que requieren contratar servicios de Seguridad de la información, ciberseguridad y riesgos, las personas encuestadas hacen parte del equipo de Seguridad y son aquellas que harían el proceso de contratación. .
Técnica de Recolección
Cuestionario electrónico
Fecha de Recolección
23/8/2023 al 24/2/2024
Diseño y Realización
La encuesta fue diseñada y realizada por Juan David Parra, Claudia Liliana Carreño y Fabian Humberto Vergara Rojas, estudiantes de la Maestría en Gerencia de Sistemas de información y proyectos de Tecnológicos de la Universidad EAN con el objetivo de conocer el mercado objeto para la adquisición de servicios de Seguridad de la información, Ciberseguridad y riesgos.
Universo
Personal técnico encargado de contratar y/o realizar seguimiento a los procesos de Seguridad de la información, ciberseguridad y riesgos de diferentes organizaciones
Preguntas formuladas

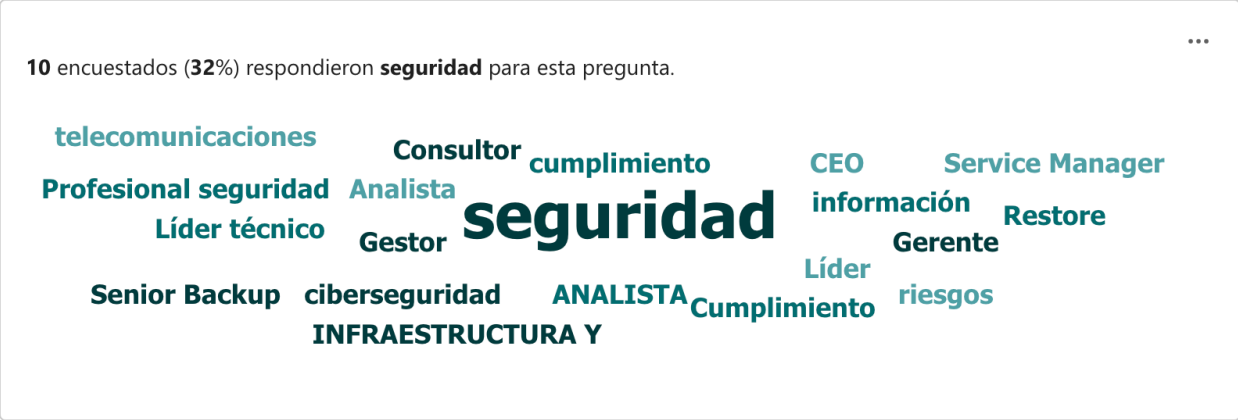
- Nombres y apellidos
- Cargo
- Sexo
- Sector
- Escolaridad
- La característica más importante que como consumidor final le exige a un servicio de seguridad de la información o Ciberseguridad es:
- Al adquirir servicios de seguridad de la información o ciberseguridad, ¿qué factores influyen en su decisión de compra? (Puede seleccionar más de uno)
- ¿Qué marcas u oferentes de servicios de seguridad de la información o Ciberseguridad le vienen a la mente cuando piensa en este tipo de servicios?
- ¿Estaría dispuesto/a pagar más por un servicio de seguridad de la información o ciberseguridad si garantiza características avanzadas o mayor protección?
- ¿Qué tan preocupado/a está por la seguridad de sus datos en línea?
- ¿Ha experimentado algún incidente de seguridad o Ciberseguridad en el último año?

A continuación, se evidenciarán los resultados y análisis de la encuesta:

En las primeras 5 preguntas se puede identificar que las personas encuestadas en su mayoría fueron hombres con un total de 19 encuestados frente a mujeres las cuales solo fueron 12, la

mayoría de las personas que respondieron son personas que cuenta con nivel de escolaridad en posgrado y el sector de trabajo es el empresarial entre los que se encuentran los cargos descritos en la *Imagen 13*:

Imagen 13 - Cargos encuestados

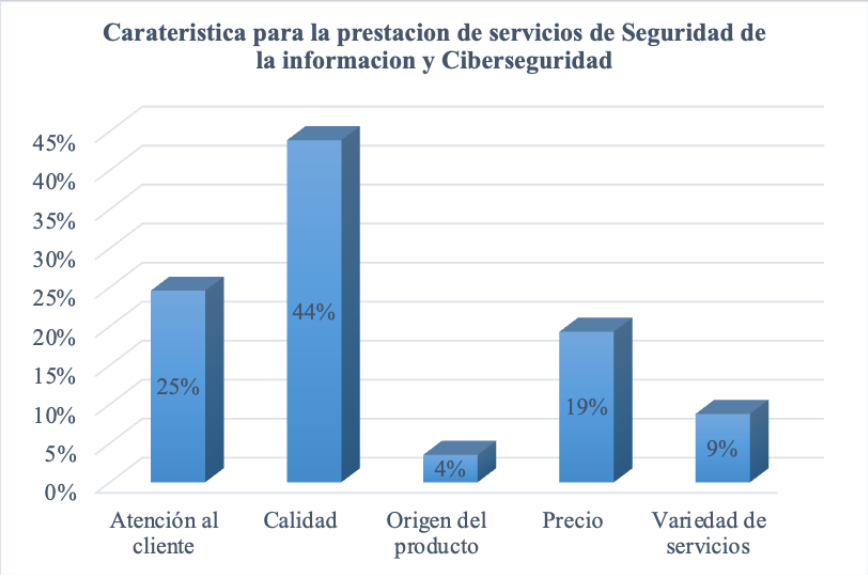


Fuente: Elaboración propia

De acuerdo a la *Imagen* 13 se evidencia que las personas encuestadas se encuentran dentro del área empresarial de Tecnología, Ciberseguridad y riesgos tomando como base fundamental que la encuesta se realizó a las personas que se encargan de los procesos de contratación de este tipo de servicios.

Frente a la pregunta No.6 "La característica más importante que como consumidor final le exige a un servicio de seguridad de la información o Ciberseguridad es", se puede apreciar lo siguiente:

Imagen 14 - Características para contratar servicios de Seguridad de la información y ciberseguridad



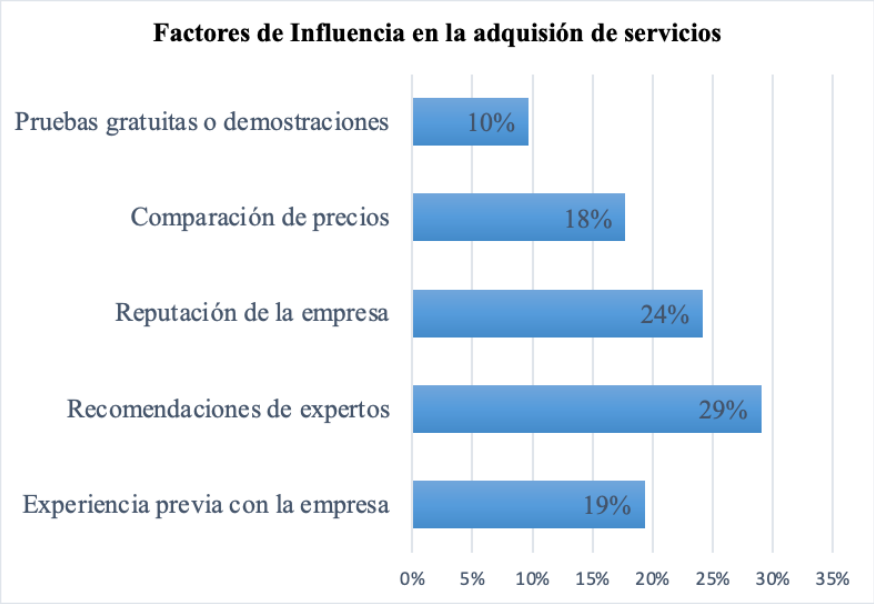
Fuente: Elaboración propia

De acuerdo a la *Imagen* 14 se identifica que las personas encuestadas consideran que al momento de adquirir un servicios de Seguridad de la información, ciberseguridad se fijan mucho en la calidad (44%) y en el servicio al cliente (25%), siendo este uno de los puntos más relevantes para el proceso de adquisición de servicios, es allí en donde Bluedice tiene la oportunidad brindar servicios integrales, de calidad enfocándose en el desarrollo continuo de servicios de vanguardia que permitan que los clientes se sientan seguros y respaldados en términos de seguridad de la información, Ciberseguridad y Riesgos, por medio de la propuesta de valor la cual se enfoca en apoyar de forma constante a la organización para que se encuentren alienadas a las estrategias de

mercado y actuar de forma proactiva a las tendencias digitales en términos de seguridad de la información y ciberseguridad del mercado.

Frente a la pregunta No.7 *"Al adquirir servicios de seguridad de la información o ciberseguridad, ¿qué factores influyen en su decisión de compra?"*, se evidencia lo siguiente:

Imagen 15 - Factores de compra servicios de seguridad de la información y ciberseguridad



Fuente: Elaboración propia

En la *Imagen* 15 se evidencia que las personas encuestadas consideran que para contratar una empresa que brinde servicios de Seguridad de la información, ciberseguridad el 29% se fija en la reputación de la empresa, el 24% en la recomendación de expertos y el 19% en la experiencia previa con la empresa, estos factores resaltados por los encuestados son de gran importancia ya que allí es a donde Bluedice buscara estrategias que permitan apoyarse en la recomendación de los clientes en los cuales se evidencien la prestación de servicios confiables y de calidad y que puedan recomendar a la empresa para posicionarse en el mercado.

Frente a la pregunta No.8 "¿Qué marcas u oferentes de servicios de seguridad de la información o Ciberseguridad le vienen a la mente cuando piensa en este tipo de servicios?", y como se evidencia en la Imagen 16 las personas encuestadas tienen recordación en empresas grandes que brindan herramientas de protección de ciberseguridad, la cuales tienen una gran reputación y renombre en la creación de controles que permiten alertar de forma proactiva la exposición y vulnerabilidades de las organizaciones. Bluedice cuenta con la experiencia y conocimiento en este tipo herramientas lo que permitirá ofrecer al cliente servicios integrales para mejorar los controles de las configuraciones ya realizadas en estos sistemas parametrizando los sistemas para que generen alertas anticipadas de la exposición de la información en la red, con el fin de generación protección frente a los ciberdelincuentes.

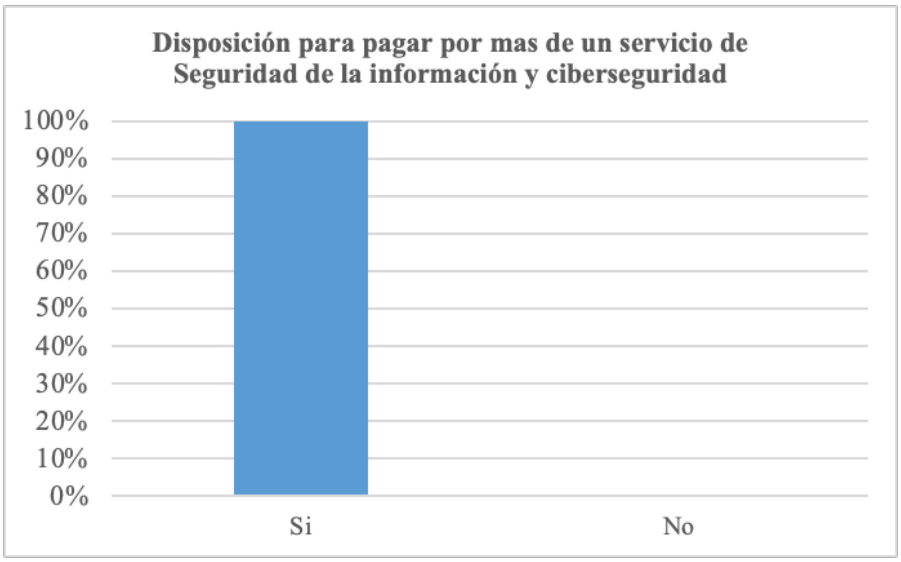
Imagen 16 - Marcas u oferentes de servicios de ciberseguridad

Fuente: Elaboración propia

Frente a la pregunta No.9 "¿Estaría dispuesto/a a pagar más por un servicio de seguridad de la información o ciberseguridad si garantiza características avanzadas o mayor protección?", se evidencia en la Imagen 17 que el 100% de las personas encuestadas estarían dispuestas a contratar más de un servicio de seguridad de la información y ciberseguridad, teniendo como premisa principal que las empresas y las personas están preocupadas por salvaguardar la información

confidencial y privada de sus partes interesada. Bluedice apoya a las organizaciones en la protección y privacidad de la información por medio de la implementación de políticas, procesos, procedimientos, análisis de riesgos, capacitaciones de seguridad de la información y ciberseguridad con el fin de dar cumplimiento normativo y que puedan cumplir con el manejo de estándares de seguridad.

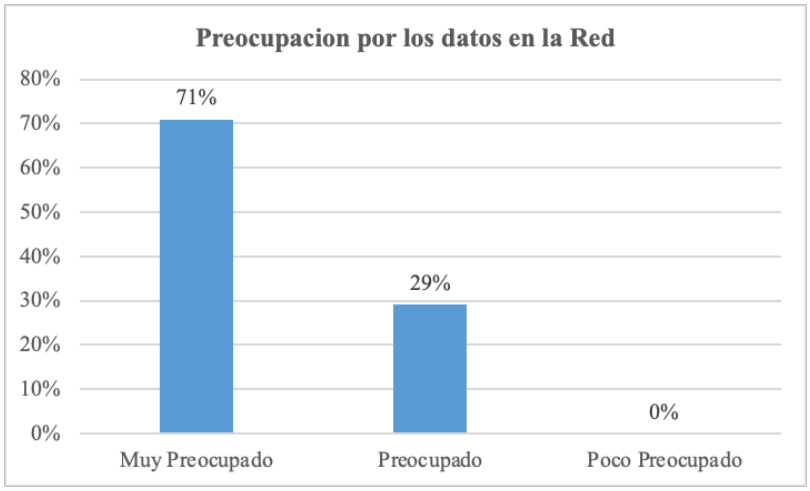
Imagen 17 - disposición para pagar servicios de seguridad de la información y ciberseguridad



Fuente: Elaboración propia

Frente a la pregunta No.10 *"¿Qué tan preocupado/a está por la seguridad de sus datos en línea?"*, se evidencia lo siguiente:

Imagen 18 - Preocupación por los datos en línea

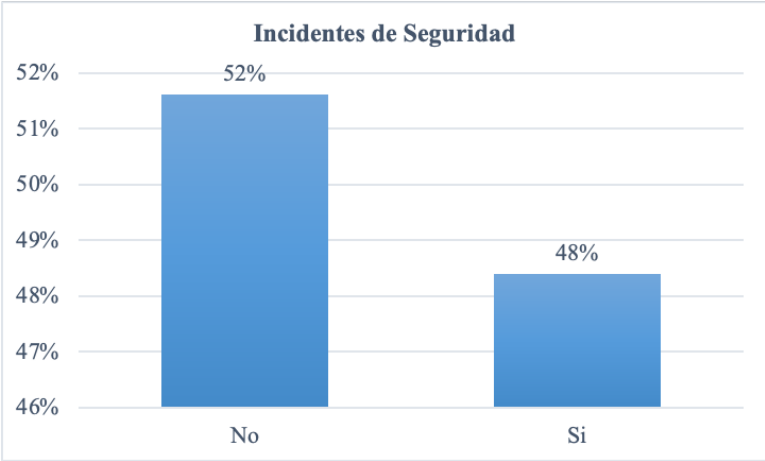


Fuente: Elaboración propia

De acuerdo con la *Imagen 18* se observa que el 71% de las personas encuestadas se encuentran muy preocupados por los datos que se encuentran en la línea y el 29% se encuentran solo manifiesta un poco de preocupación, es allí en donde se evidencia que la información que transita por la red es de gran preocupación por las empresas, los procesos de fraude y perdida sobre la red cada vez son más sencillos de realizar, Bluedice quiere asegurar dentro de su oferta de valor la protección de la información del cliente garantizando siempre la disponibilidad, confidencialidad e integridad de la misma.

Frente a la pregunta No.11 *"¿Ha experimentado algún incidente de seguridad o Ciberseguridad en el último año?"* se identifica lo siguiente*:*

Imagen 19 - Incidentes de seguridad de la información y ciberseguridad



Fuente: Elaboración propia

De acuerdo a la *Imagen 19* se identifica en las personas encuestadas que solo el 48% de los encuestados ha experimentado incidentes de seguridad y ciberseguridad. Es importante que las organizaciones tengan conocimiento y conceptos claros sobre que puede ser incidente o evento de seguridad para que sepan como mitigar, controlar y detener las diferentes incidencias a las que se pueden ver expuestos, es por ello que Bluedice dentro de su oferta de valor ofrece oportunidades a los clientes para estar alineados, tener conocimiento y manejo de las ultimas brechas de seguridad que se presentan en la actualidad, es fundamental que tanto los clientes como usuarios tengan conocimiento y buen manejo de la información.

Frente a las encuestas anteriores se puede concluir que las empresas que realizan los procesos de contratación de servicios de Seguridad de la información y ciberseguridad muestran preocupación por la exposición de datos en línea, al igual que se evidencia que casi la mitad de los encuestados han manifestado que han presentado incidentes de seguridad de la información y ciberseguridad, puede ser que el otro porcentaje de los encuestados no los hayan presentado o no tengan el conocimiento de los que es un incidente de seguridad, el entendimiento de las empresas

por asegurar su información demuestra la importancia que se tiene para la prestación de este tipo de servicios y aseguramiento por medio de procesos, procedimientos que permitan que los métodos de intrusión que usan los ciberdelincuentes sean más difíciles.

A continuación, se adjuntan los enlaces de evidencia de las entrevistas y encuestas realizadas a las diferentes partes interesadas ***Anexo 1*** ***Encuestas y Entrevistas.zip***.

Con respecto a las encuestas y entrevistas realizadas se puede concluir que la prestación de servicios de Seguridad de la información, ciberseguridad y gestión de riesgos presenta un panorama de crecimiento robusto y en evolución permanente. El manejo de conciencia y cultura en el manejo de amenazas cibernéticas y la importancia de proteger la información confidencial ha impulsado una demanda sostenida de servicios especializados, todo esto teniendo en cuenta que ahora las empresas han ido evolucionando y cuentan con tecnologías emergentes en las cuales se evidencia una expansión de las amenazas de los entornos de ciberseguridad, destaca la necesidad de implementar soluciones innovadoras y el manejo de servicios adaptados a las necesidades de los clientes.

4.4. Análisis de la Competencia

El análisis de la competencia de empresas que brindan servicios de seguridad, ciberseguridad y riesgos le permitirá a Bluedice conocer los competidores existentes en el mercado al igual que los productos y/o servicios que estos ofrecen, clientes y sectores objetivo, precios, modelos de negocio entre otros, esto con el fin de identificar en que se parece la empresa versus sus competidores y cuál puede ser su punto diferenciador.

Tabla 12 - Análisis de la competencia

Competencia				
Descripción	**Cloud**	**ETEK**	**ART2SEC**	**2Secure**
Plaza	Bogotá Zona Norte	Bogotá Zona Norte México Perú Estados Unidos India	Bogotá Zona Norte	Bogotá zona norte México D.F.
Productos y servicios (atributos)	Consultoría en Seguridad de la información, Servicios de Auditoria, análisis de vulnerabilidades, pruebas de Ética Hacking.	Portafolio de servicios de Ciberseguridad, implementación y soporte de hardware y soluciones de ciberseguridad	Servicios de Control y gestión de riesgos, detección y control de amenazas, protección de ambientes cloud	Servicios de Ciberseguridad, Análisis de vulnerabilidades, Pruebas internas y externas de Ethical Hacking, computación forense, monitoreo y Sistemas SOC, otros servicios de seguridad
Precios	Los precios se ajustan dependiendo el cliente y el servicio a realizar. Precios bajos	Los precios se ajustan dependiendo el cliente y el servicio a realizar. Precios Altos en el mercado	Los precios se ajustan dependiendo el cliente y el servicio a realizar. Precios bajos	Los precios se ajustan dependiendo el cliente y el servicio a realizar. Precios Altos en el mercado

Posicionamiento	Cloud Seguro tiene un buen posicionamiento en el mercado, ya que ha desarrollado proyectos a nivel de gobierno y a empresas privadas en Colombia.	Alto posicionamiento en el mercado, reconocida y con gran trayectoria en la prestación de servicios de seguridad de la información y ciberseguridad. Etek cuenta con alta gama de clientes y con certificaciones internaciones.	Art2sec es una empresa que aún está en proceso de posicionamiento ya que su fundación fue hacia el año 2016	Empresa con alto reconocimiento en el mercado para la prestación de servicios a nivel de seguridad informática, seguridad de la información y ciberseguridad, 2secure cuenta con reconocimiento y más de 10 alianzas estratégicas, en Colombia cuenta con una gran cantidad de clientes muchos

Fuente: Elaboración propia

Para concluir con el análisis de la competencia de acuerdo de lo descrito en la *Tabla 12* se puede determinar lo siguiente:

A. En el mercado actual se encuentra grandes competidores que ofrecen los mismos servicios a nivel de seguridad, ciberseguridad y riesgos, se observa que los servicios ofrecidos por Etek y 2secure están más orientados a servicios de Ciberseguridad.
B. El principal diferencial de Bluedice va a ser el uso de una metodología que permita combinar diferentes tipos de análisis para realizar el proceso de diagnóstico de vulnerabilidades, enfocado a pequeñas y medianas empresas pensando en lo siguiente:
    - Personalización de servicios dependiendo el cliente y su necesidad.

- La ventaja competitiva que ha diseñado y/o desarrollado Bluedice con la finalidad de poder generar diferenciación con otros proveedores que pueden ofertar los mismos servicios.
- Se desarrollaron fichas técnicas de la prestación del servicio las cuales le permitirán a los clientes identificar los servicios que ofertan y su interés. Cada una de estas fichas están desarrolladas con base en unos alcances y condiciones determinadas.
- Dentro de su oferta de servicios Bluedice entregará un informe de resultados enfocados a los planes de remediación que la organización debe accionar para el cumplimiento de las normas 31000 y 27001
- Se ofrecerán servicios bajo demanda que permitan asegurar la continuidad de los sistemas de gestión y también se asegure que las organizaciones puedan cumplir con los estándares de protección de datos y las buenas prácticas para gestionar los riesgos
- Se proporcionará la capacidad de ser un servicio integral, no solo un portafolio en Pentesting y ciberseguridad, si no que la empresa también está alineada al análisis constante de riesgos y el cumplimiento de estándares actuales de certificación mínima que se requiere hoy en día a nivel legal. El precio de los servicios ofertado por Bluedice es un diferenciador importante ya que dentro de la estrategia general se encuentra en el ganar posicionamiento y reconocimiento en el mercado. Si bien sus competidores ya cuentan con este reconocimiento también es importante destacar que el nicho de mercado que busca atacar Bluedice inicialmente son las pequeñas y medianas empresas las cuales buscan la protección de sus datos y el

cumplimiento normativo y no cuenta con alto flujo de caja para el pago de servicios a un costo tan alto como lo ofrecen empresas de reconocimiento y trayectoria.

Actualmente se observa un crecimiento alto en la adquisición de servicios de seguridad de la información, ciberseguridad y análisis de riesgos por las empresas pequeñas y medianas ya que para poder prestar ciertos tipos de servicios a otras compañías del sector gobierno y financiero deben ser certificados es ISO 27001, si bien para este tipo de organizaciones es un costo y no cuentan con el personal capacitado, Bluedice tiene dentro de sus portafolio de servicios presta servicios de consultoría y/o asesoría en la implementación y certificación de sistemas de Seguridad la información y ciberseguridad con el fin de dar cumplimiento normativo a requerimientos que la empresa contratante.

4.5. Estrategia y plan de introducción de mercado

Bluedice ejecutará el plan de introducción de mercado en el servicio que permitan a las organizaciones poder identificar el status de vulnerabilidades cibernéticas con el fin de realizar diferentes estrategias que permitan a las pequeñas organizaciones mitigar la exposición al riesgo en seguridad y ciberseguridad, bajo esa misma línea de trabajo la estrategia será la siguiente:

Tabla 13 - Plan de introducción en el mercado

Estrategia:	**Posicionamiento y atracción de nuevos clientes**		
Propósito:	Garantizar que los clientes conozcan a Bluedice		
Actividad	Recursos requeridos	Mes de ejecución	Responsable
Inbound Marketing	Branding: Marca, logos, equipos tecnológicos, contenido digital, material publicitario	6	Área de Gerencia y área comercial

Creación de contenido para la atracción de los clientes	
Creación del perfil de LinkedIn corporativo	
Optimización de motores de búsqueda (SEO)	
Costo:	$5.000.000

Fuente: Elaboración propia

Objetivo: Tener un posicionamiento de Bluedice y alcanzar a atraer a partir de pauta y estrategias de mercadeo digital para el primer año de funcionamiento

Resultado: Atraer por estrategias de mercadeo digital el cierre de 5 clientes durante el primer año**.**

4.6. Estrategia de producto y servicios

Desarrollo y creación de una página web para que los clientes puedan conocer a Bluedice y la oferta de valor

- Creación de una estrategia de Inbound Marketing para la atracción de clientes: En inbound marketing implica atraer y convertir a nuevos clientes con estrategias como correos electrónicos, marketing cloud para atraer prospectos, mediante tácticas de cierre que conviertan leads en clientes, y posteriormente centrarse en la satisfacción del cliente para fomentar la lealtad y la voz a voz positivo.
- Creación de blogs y e-books de temas de tendencias y relevancia: Creación de contenido enfocado en un marco educativo, buenas prácticas y tendencias globales que permitan a los consumidores una descarga de este contenido de valor mediante un formulario el cual se utilizará para la recopilación de los datos personales de los usuarios que descarguen este contenido. A partir de la creación de esta base de datos se crearán diferentes rutas de habilitación, las cuales permitirán comunicar contenido de valor para este usuario
- Crear un perfil de LinkedIn de Bluedice para el posicionamiento con otras empresas: Establecer metas basadas en la creación y visibilidad de la empresa en redes sociales, por ahora centrándonos en LinkedIn, para fortalecer relaciones comerciales y posicionarse en la industria, identificando audiencia, empresas afines, profesionales claves para adaptar el contenido de la página y realizar publicidad estratégica.
- Creación de casos de éxito con los primeros clientes a los cuales se les ha brindado algún tipo de producto, de esta forma podremos resaltar el valor de la compañía.
- Crear una pauta publicitaría en LinkedIn y Google para posicionar Bluedice dentro del motor de búsqueda y en páginas de relevancia e industria.

Implementación de optimizaciones en motores de búsqueda (SEO) a partir de análisis de métricas, interacciones activas, monitoreo de rendimiento y selección de palabras clave en las

publicaciones relevantes lo que permite encontrar la página en búsquedas internas (LinkedIn) y externas (Google)

Se espera que a partir de una estrategia de mercadeo que pueda atraer el 50% de los clientes, y el otro 50% será a partir del vos a vos y/o referidos

4.7. Estrategia de precio

- Los precios que ofrecerá Bluedice serán competitivos y por debajo de la media del mercado, ya que el público objetivo serán esas pequeñas y medianas empresas.
- Lanzar formalmente Bluedice como empresa especializada en consultoría de seguridad, ciberseguridad y gestión de riesgos con enfoque tecnológico con el objetivo de generar permanencia. Adicionalmente, crearemos por lanzamiento unos descuentos y servicios complementarios y adicionales con la finalidad de incentivar a los clientes que hagan parte de Bluedice.
- Participación a diferentes eventos asociados a tecnología, riesgos y ciberseguridad para empezar a tener reconocimiento en el mercado.
- Contactar a personas referentes en la industria para realizar alianzas y networking con ellos.

Para concluir se puede considerar esta estrategia de penetración en el mercado como una buena opción para el reconocimiento y posicionamiento de Bluedice ya que sé que evidencia el uso de canales digitales está en constante crecimiento y en Colombia el uso del internet se encuentra en crecimiento, es importante destacar que estas estrategias tienen como base el mínimo costo ya que en este momento la empresa se encuentra en su proceso inicial.

5. Aspectos técnicos

De acuerdo a los aspectos técnicos detallados de cada servicio ofrecidos por Bluedice, es esencial establecer una comprensión general de su portafolio. El cual presenta una variedad de servicios enfocados en la seguridad de la información, la continuidad del negocio y la ciberseguridad. Desde la implementación hasta la auditoría interna y el análisis de riesgos, Bluedice se dedica a proporcionar soluciones integrales que protejan a sus clientes y fortalezcan sus sistemas de gestión; en el numeral 5.1, se generará un detalle la ficha técnica cada uno de los servicios ofertados, lo que proporcionará una visión detallada de los procesos involucrados, los requisitos necesarios y los resultados esperados para cada servicio.

5.1. Ficha técnica del producto o servicio

A continuación, se describe la ficha técnica de los productos que serán ofertados por Bluedice:

Tabla 14 - Ficha técnica Auditoría Interna SGSI ISO 27001

FICHA TÉCNICA	
Nombre del Servicio	Proceso de Auditoría Interna SGSI ISO 27001
Alcance del servicio	Auditoria de los procesos del Sistema de Gestión de Seguridad de la información de acuerdo con lo evidenciado en el Alcance, Objetivos y contexto de la organización.
Descripción del Servicio	Realizar Planeación de auditoría Interna Revisar los numerales de la norma ISO 27001 y sus controles con el fin de poder evidenciar oportunidades de mejora que apalanquen el crecimiento del sistema de Gestión. Identificación de Activos: Definición de los activos de información que están dentro del alcance de la auditoría. Límites Organizacionales: Revisión de los límites organizacionales dentro de los cuales se realizará la auditoría. Puede incluir departamentos específicos, ubicaciones geográficas o unidades de negocio

	particulares. Procesos y Operaciones: Revisión detallada de los procesos y operaciones que serán evaluados, gestión de activos de información, gestión de incidentes de seguridad, gestión de accesos y la adquisición de bienes y servicios. Partes Interesadas: Identificación de las partes interesadas relevantes que estarán involucradas o afectadas por la auditoría entre los cuales están clientes, proveedores, empleados y otros socios comerciales. Tecnología y Sistemas: definición de los sistemas, tecnologías y plataformas que serán objeto de revisión. Cumplimiento Legal y Regulatorio Documentación y Registros: Alcance de la revisión de la documentación del SGSI, procedimientos, registros y cualquier otra documentación relacionada. Alcance de Auditoria Metodología de Auditoría: Se seguirá la metodología de auditoría establecida por la organización basada en las directrices de la norma ISO 19011.
Requisitos para la prestación del servicio	Auditor Interno de SGSI ISO 27001:2013 / 2022 Personal del cliente Acceso a la documentación del cliente.
Entregables del Servicio	Informe de Auditoría detallado con hallazgos, recomendaciones y conclusiones.
Tiempo	Mínimo 5 Días - Depende del alcance y cantidad de procesos
Costos y condiciones Comerciales	Mínimo 5.500.000 por 4 procesos, el valor varía dependiendo el alcance de la Auditoria, Cantidad de procesos
Validez de la Oferta	30 días

Fuente: Elaboración propia

Tabla 15 - Ficha Técnica Implementación sistemas de gestión

FICHA TÉCNICA	
Nombre del Servicio	Proceso de Implementación de Sistemas de Gestión.
Alcance del servicio	Establecer, implementar, mantener y mejorar sistemas de gestión conforme a los estándares ISO 27001 e ISO 22301.
Descripción del Servicio	Identificación de requisitos y expectativas del cliente. Evaluación del contexto organizacional y análisis de riesgos. Desarrollo de un plan de implementación detallado. Asignación de recursos y responsabilidades. Desarrollo de políticas, procedimientos y documentos requeridos. Diseño de procesos para la seguridad de la información y la continuidad de negocio. Capacitación del personal sobre los requisitos y responsabilidades. Establecimiento de controles de seguridad y medidas de continuidad. Implementación de auditorías internas y revisiones periódicas. Mejora continua basada en la retroalimentación y los resultados de las auditorías.
Requisitos para la prestación del servicio	Equipo de Consultores: - Especialistas certificados en ISO 27001 e ISO 22301. - Experiencia en la implementación exitosa en diferentes industrias. Herramientas y Tecnologías: - Herramientas de gestión de proyectos. - Software de gestión documental y de riesgos. - Herramientas de evaluación y monitoreo de la seguridad de la información.
Entregables del Servicio	Implementación de sistemas de Gestión (Alcance, políticas, procesos, procedimientos)
Tiempo	Depende del proyecto, tamaño de organización, cantidad de procesos y alcance a certificar.
Costos y condiciones Comerciales	Por etapa del proyecto, tamaño de organización y alcance a certificar.
Validez de la Oferta	30 días

Fuente: Elaboración propia

Tabla 16 - Ficha Técnica Auditoría interna SGCN 22301

FICHA TÉCNICA	
Nombre del Servicio	Proceso de Auditoría Interna SGCN ISO 22301
Alcance del servicio	Auditoria de los procesos del Sistema de Gestión de continuidad de negocio ISO22301 de acuerdo con lo evidenciado en el Alcance, Objetivos y contexto de la organización.
Descripción del Servicio	Realizar Planeación de auditoría Interna Revisar los numerales de la norma ISO 22301, con el fin de poder evidenciar oportunidades de mejora que apalanquen el crecimiento del sistema de Gestión. Activos Críticos de Negocio: Identificar y evaluar de los activos críticos para la operación de la organización, así como los procesos clave, tecnologías esenciales, personal crítico y recursos críticos. Límites Organizacionales: Se revisará y evaluaran los sistemas informáticos, redes, infraestructuras críticas y cualquier tecnología relevante para la continuidad de negocio. Procesos y Operaciones Incluidos: Se revisarán y evaluarán todos los procesos y operaciones relacionados con la gestión de la continuidad de negocio, desde la identificación de riesgos hasta la recuperación y resiliencia. Ciclo de Vida del Plan de Continuidad: Evaluación de las prácticas de seguridad en cada fase del ciclo de vida del plan de continuidad, desde la planificación hasta la revisión y actualización. Partes Interesadas: Identificación de las partes interesadas relevantes que puedan afectar o ser afectadas por la continuidad del negocio. Evaluación de la efectividad de los ejercicios y pruebas realizados para garantizar la capacidad de respuesta y recuperación del negocio. Documentación y Registros: Revisión de la documentación del SGCN, incluyendo políticas, procedimientos, planes de continuidad y cualquier otra documentación pertinente.

	Cumplimiento Legal y Regulatorio: se realizará la verificación del cumplimiento con todas las leyes y regulaciones aplicables relacionadas con la continuidad de negocio. Metodología de Auditoría: Se seguirá la metodología de auditoría establecida por la organización basada en las directrices de la norma ISO 19011.
Requisitos para la prestación del servicio	Auditor Interno de SGCN ISO 22301 Personal del cliente
Entregables del Servicio	Informe de Auditoría detallado con hallazgos, recomendaciones y conclusiones.
Tiempo	Mínimo 3 Días - Depende del alcance y cantidad de procesos
Costos y condiciones Comerciales	Mínimo 4.000.000 por 3 procesos, el valor varía dependiendo el alcance de la Auditoria, Cantidad de procesos
Validez de la Oferta	30 días

Fuente: Elaboración propia

Tabla 17 - Ficha técnica servicios Ethical Hacking - Pentesting - Análisis de vulnerabilidades

FICHA TÉCNICA

Nombre del Servicio	Servicios de Ethical Hacking / Pentesting / Vulnerabilidades
Alcance del servicio	Identificar y explotar debilidades en la seguridad de los sistemas para evaluar la capacidad de resistencia ante ataques reales. Definir los sistemas, aplicaciones o redes que se incluirán en las pruebas de ethical hacking, así como cualquier limitación o exclusión.
Descripción del Servicio	Ambiente de en el que se va a realizar la prueba: Descripción detallada del entorno, sistemas operativos, aplicaciones, versiones de software y cualquier otro componente relevante. Diagrama de Red: Diagrama detallado de la topología de red, indicando puntos de entrada, segmentación y posibles rutas de movimiento lateral. Credenciales de Acceso: Detalles sobre las credenciales proporcionadas para las pruebas de ethical hacking, incluyendo privilegios y alcance. Técnicas de Hacking Ético: Caja negra, Caja Blanca, Caja Gris.

	Técnicas de Pentesting: Pruebas de inyección, escaneo de puertos, fuzzing, entre otros.
Requisitos para la prestación del servicio	Ingeniero Experto en Ethical Hacking / Pentesting Acceso a sistemas o aplicaciones
Entregables del Servicio	Informe con todas las vulnerabilidades identificadas, incluyendo su clasificación, evidencia y posibles impactos. Informe de registro detallado de las actividades realizadas durante las pruebas de ethical hacking, incluyendo fechas, horas y acciones específicas.
Tiempo	Depende de los sistemas, Aplicaciones y/o redes en donde se requiera realizar la prueba. Tiempo 1 aplicación simple sin recurrencia 3 días
Costos y condiciones Comerciales	Depende de los sistemas, Aplicaciones y/o redes en donde se requiera realizar la prueba. Valor inicial 1 aplicación simple sin recurrencia: 2.500.000
Validez de la Oferta	30 días

Fuente: Elaboración propia

Bluedice prestara servicios de acuerdo con el portafolio de servicios que se encuentra descrito en las tablas anteriores de la siguiente forma:

Servicios de Seguridad de la información, continuidad de negocio y ciberseguridad, Bluedice ofrecerá Implementación, consultoría, auditoría interna y análisis de riesgos que permitan mantener y proteger a los clientes en términos de seguridad de la Información y ciberseguridad adicionalmente se ofrecerán servicios adicionales de acuerdo a un proceso de SiteAudit que permitirá identificar los procesos en los cuales los clientes requieren asistencia para mejorar o mantener los Sistemas de gestión.

El ofrecimiento de servicios para pruebas de Ethical Hacking, análisis de vulnerabilidad e ingeniera social se ofertarán de acuerdo con la cantidad de aplicaciones que el cliente requiera hacer la revisión y de acuerdo con esto se generan informes que puedan soportar los hallazgos encontrados y su nivel de criticidad, esto con el fin entregar servicios de calidad y que permita mantener la tranquilidad de los clientes.

Adicionalmente si el cliente lo requiere se podrá proporcionar un paquete de horas mensuales o anuales con el fin de que el cliente pueda mantener y realizar la mejora continua de los sistemas de gestión implementados en la organización.

6. Recursos tecnológicos e infraestructura

Para la prestación del servicio es importante contar con el siguiente Talento Humano:

- Asesor Comercial
- Auditor
- Especialista en Seguridad de información (Emprendedor y personal subcontratado)
- Especialista en Ciberseguridad (Emprendedor y personal subcontratado)

A nivel de Infraestructura para la prestación del servicio se requiere lo siguiente:

Tabla 18 - Tabla de infraestructura Bluedice

Tipo de Activo	Descripción	Cantidad	valor Unitario	Requisitos técnicos
Infraestructura	Conexión a Internet	3	$ 300.000	100 MB
	Equipos Portátiles	3	$ 10.000.000	Intel Core i5 - i7 RAM 16 GB Disco SSD 512GB / 1 TB
	Office 365 (60USD)	3	$ 780.000	
	Software Qualys para análisis de vulnerabilidades y Pentesting.	2	$12.000.000 -	SAAS

Fuente: Elaboración propia

Actualmente para la prestación de servicios de seguridad, ciberseguridad y riesgos no será necesario contar con instalaciones de oficina ya que la prestación de los servicios se realizará en las instalaciones físicas del cliente o en su defecto de forma virtual.

7. Proceso para la prestación del servicio

7.1. Mapa de Procesos Bluedice

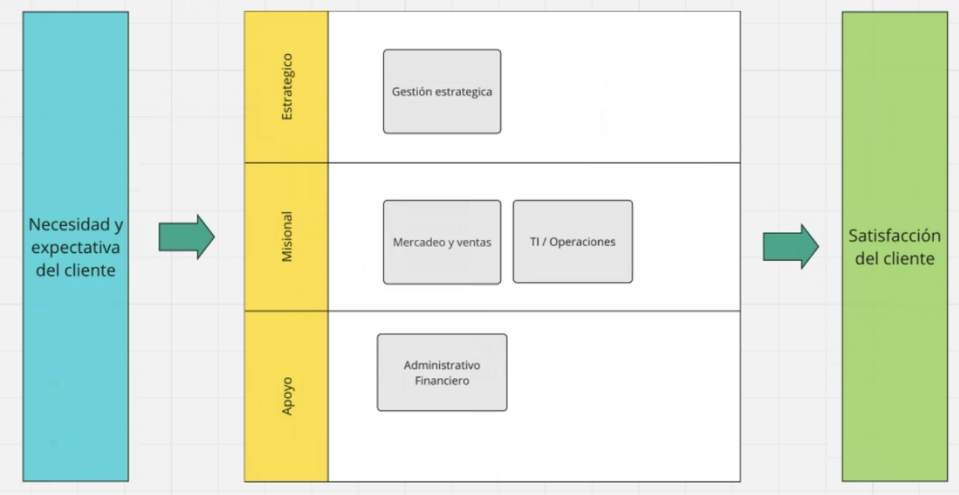
En la siguiente imagen se puede evidenciar el mapa de procesos de BLUEDICE:

Entrada: Se identifican las necesidades y expectativas del cliente

Procesos: Se evidencia procesos estratégicos, Misionales y de Apoyo

Salida: Se busca la satisfacción del Cliente en la entrega de la prestación del servicio

Imagen 20 - Mapa de proceso Bluedice - Fuente propia



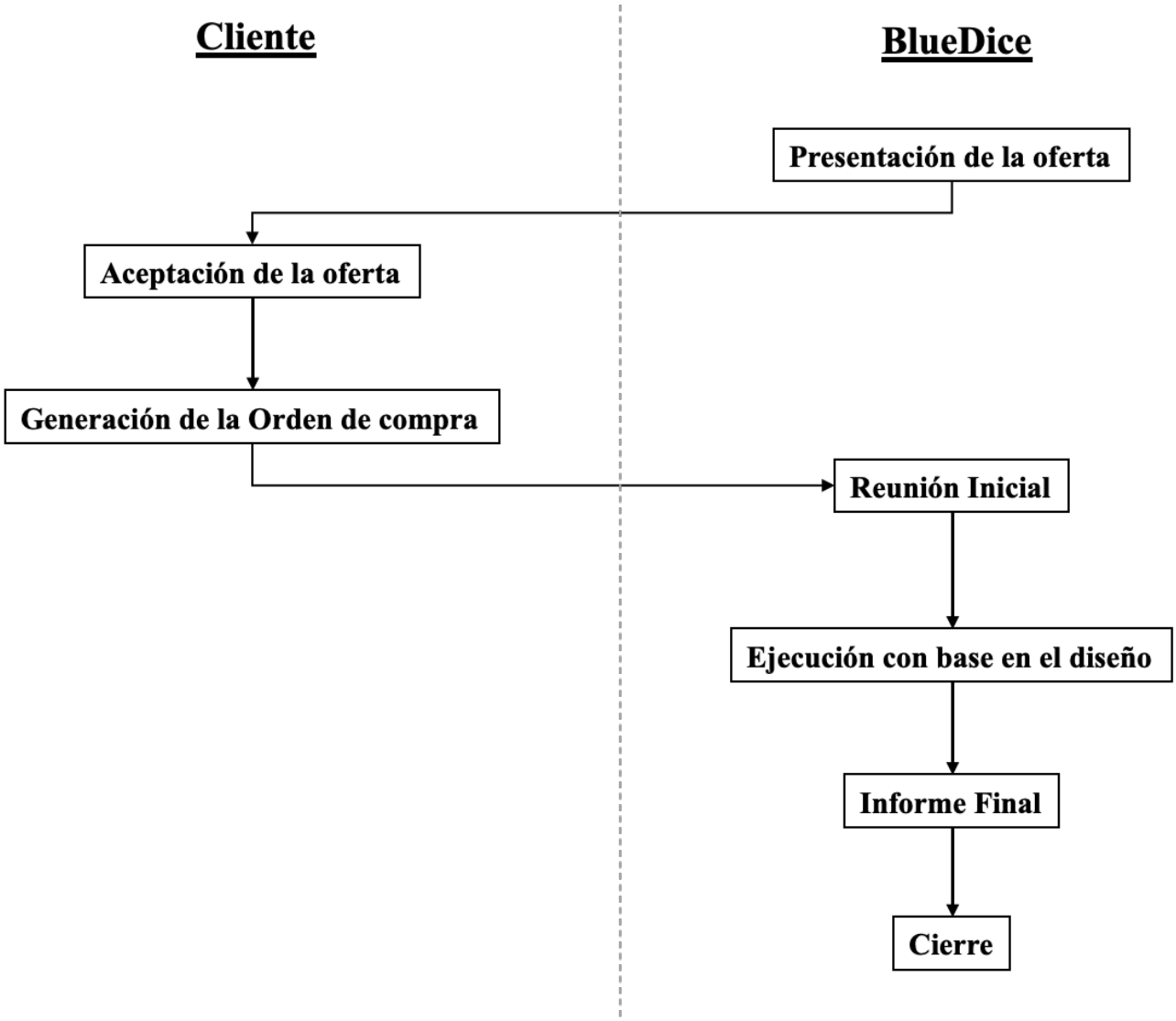
Fuente: Elaboración propia

El mapa de procesos de BLUDICE está compuesto en 3 etapas principales, la primera en donde se identifica la necesidad del cliente; posterior a ello se subdivide en 4 procesos que son la columna vertebral de la organización, gestión estratégica de tipo estratégico, mercadeo y ventas, TI/Operaciones: Misional, y administrativo financiera: Apoyo.

7.2. Flujograma proceso de prestación del servicio

A continuación se describe el proceso a realizar para la prestación del servicio el cual inicia con la presentación de la oferta al cliente el cual se enmarcan en las necesidades y/o requerimientos del cliente, este proceso es realizado por el proceso Misional área de Mercadeo y ventas , una vez se genere y se entregue la oferta de servicio al cliente este revisara y en caso de que esta sea aceptada se generara una Orden de compra o de servicio el cual es generado por el proceso de Apoyo Administrativo y financiero, posteriormente se realizara una reunión inicial con el fin de indicarle al cliente todo el proceso de ejecución con base en un cronograma que llevara el tiempo y los recursos a utilizar todo esto pactado con el cliente, al terminar todas la actividades y cumplir con lo requerido por el cliente Bluedice generara una informe final con los resultados realizados y se procederá al cierre y entrega final al cliente, esta etapa del proceso es atendida por el proceso Misional el cual está a cargo del área de TI/operaciones y la satisfacción del cliente será medida en el proceso de Apoyo por parte del área administrativa y financiera.

Imagen 21 - Proceso Prestación de servicios Bluedice



Fuente: Elaboración propia

7.3. Capacidad de prestación del servicio

Tabla 19 - Capacidad Prestación de Servicios Horas/Mes - Fuente propia

Servicios	Cantidad de Horas Mes
Implementación de Sistemas de Gestión X proceso	200
Bolsas de horas	30
Auditoria por proceso	50
Pruebas de Ciberseguridad alto nivel	28
Pruebas de ingeniería Social	12
Pruebas de Ciberseguridad aplicaciones Móviles	10
Total, de Horas	330

Fuente: Elaboración propia

De acuerdo con lo descrito en la Tabla 19 - Capacidad Prestación de Servicios Horas/Mes, dentro del proceso inicial de la creación de empresa se estima prestar un total de 330 Horas al mes, para los diferentes servicios ofrecidos por Bluedice

Inicialmente para la prestación del servicio, se evalúa una capacidad instalada en horas hombre de 324 en el cual la prestación del servicio de la empresa se realizará por los 3 emprendedores, el cual podrá variar con el tiempo debido a cambios en la composición del equipo, las políticas de trabajo, la demanda de proyectos, entre otros factores. Es importante revisar y ajustar estos cálculos periódicamente para reflejar con precisión la capacidad real de trabajo del equipo y así poder dar cumplimiento a promesa de valor de la organización.

Tabla 20 - Capacidad Prestación de Servicios Horas/Empleado

Personal	Horas de trabajo Mes
Ingeniero 1	160
Ingeniero 2	100
Ingeniero 3	64
Total 3 ingenieros equipo emprendedor	324

Fuente: Elaboración propia

Tabla 21 - Requerimiento de conocimiento técnico prestación del servicio

Nombre del Cargo	Funciones principales	Formación	Experiencia General (años)	Experiencia específica (años)	Tipo de contratación (jornal, prestación de servicios, nómina)	Dedicación de tiempo (tiempo completo /tiempo parcial)	Unidad	Valor remuneración*
Auditor	Realizar reunión de Apertura / Cierre de Auditorias.	Ingeniero de Sistemas Certificado Auditor Líder ISO 27001	5Años	2 años Auditor Líder	Prestación de Servicios	Tiempo Parcial	Horas	$ 70.000
Especialista Ciberseguridad	Realiza pruebas de ciberseguridad	Ingeniero de Sistemas Certificado Auditor	10 años	5 años Ethical Hacking, análisis de vulnerabilidades, Pentesting	Prestación de Servicios	Tiempo Parcial	Horas	$ 80.000

Especialista Seguridad de la información	Procesos de Auditoria, implementación de sistemas de gestión, consultoría de Seguridad de la Información, continuidad de negocio, Análisis de Riesgos	Ingeniero de Sistemas Certificado Auditor Líder ISO 27001 / ISO 32001, ISO 22301	10 años	4 años de experiencia como implementador de sistemas de gestión de Seguridad de la información, análisis de riesgos.	Prestación de Servicios	Tiempo Parcial	Horas	$ 80.000
Asesor comercial	Realizar ofertas comerciales	Administrador de empresas	2 años	1 año realizando Ofertas	Prestación de Servicios	Tiempo Parcial	Horas	$ 45.000
Gerente General	Realizar la planeación estratégica de la organización, administración de recursos humanos y gestionar el presupuesto asignado	Administrador de empresas	6 años	4 Años gerenciando empresas de TI	Prestación de servicios	Tiempo Parcial	Horas	$ 200000

Fuente: Elaboración propia

8. Aspectos organizacionales y legales

8.1. Misión:

Fortalecer los procesos de seguridad, ciberseguridad y riesgos de los clientes con el fin de hacerlas más seguras y confiables para la seguridad y protección de los datos de sus clientes y poder garantizar la continuidad de negocio de las empresas y sus clientes

8.2. Visión

Para el 2030, posicionar a Bluedice como un referente líder y ser identificados por los clientes como un socio estratégico que contribuye a fortalecer su seguridad, reducir los niveles de riesgo y facilitar el cumplimiento de normativas, a través de la oferta de servicios innovadores y competitivos de alta calidad.

8.3. Análisis DOFA

Se realiza un análisis del entorno interno y externo con el fin de tener una visión integral de la empresa de las posibles afectaciones y estrategias que se pueden identificar para el alcance de los objetivos, identificación, análisis y gestión de riesgos, al igual que permitirá comprender el entorno competitivo y permitirá que Bluedice desarrolles estrategias que permitan aprovechar las fortalezas y abordar las debilidades en comparación con la competencia.

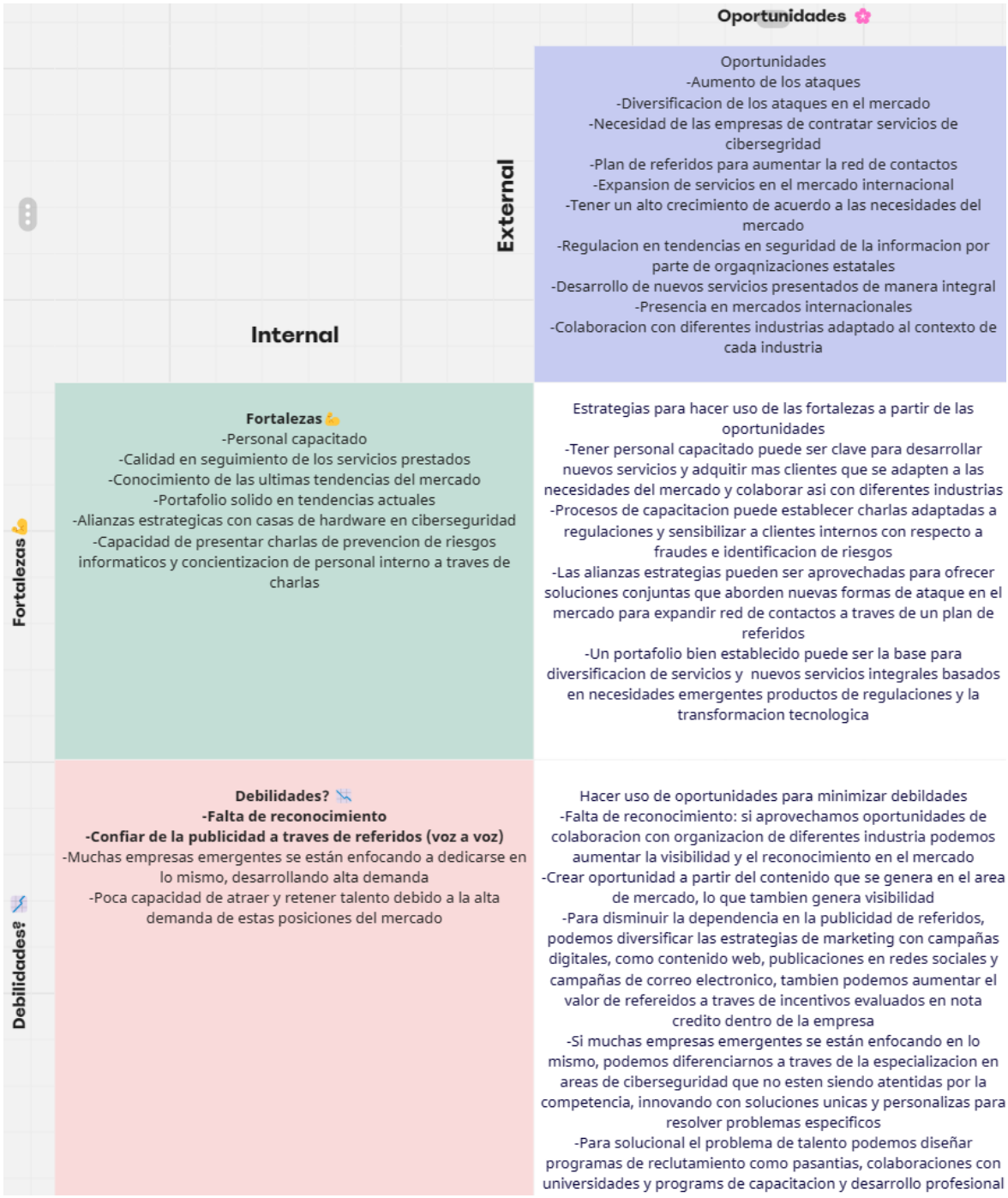
Imagen 22-Análisis Dofa

Fuente: Elaboración propia

8.4. Análisis cruzado Matriz DOFA BLUEDICE

8.4.1. Análisis cruzado oportunidades

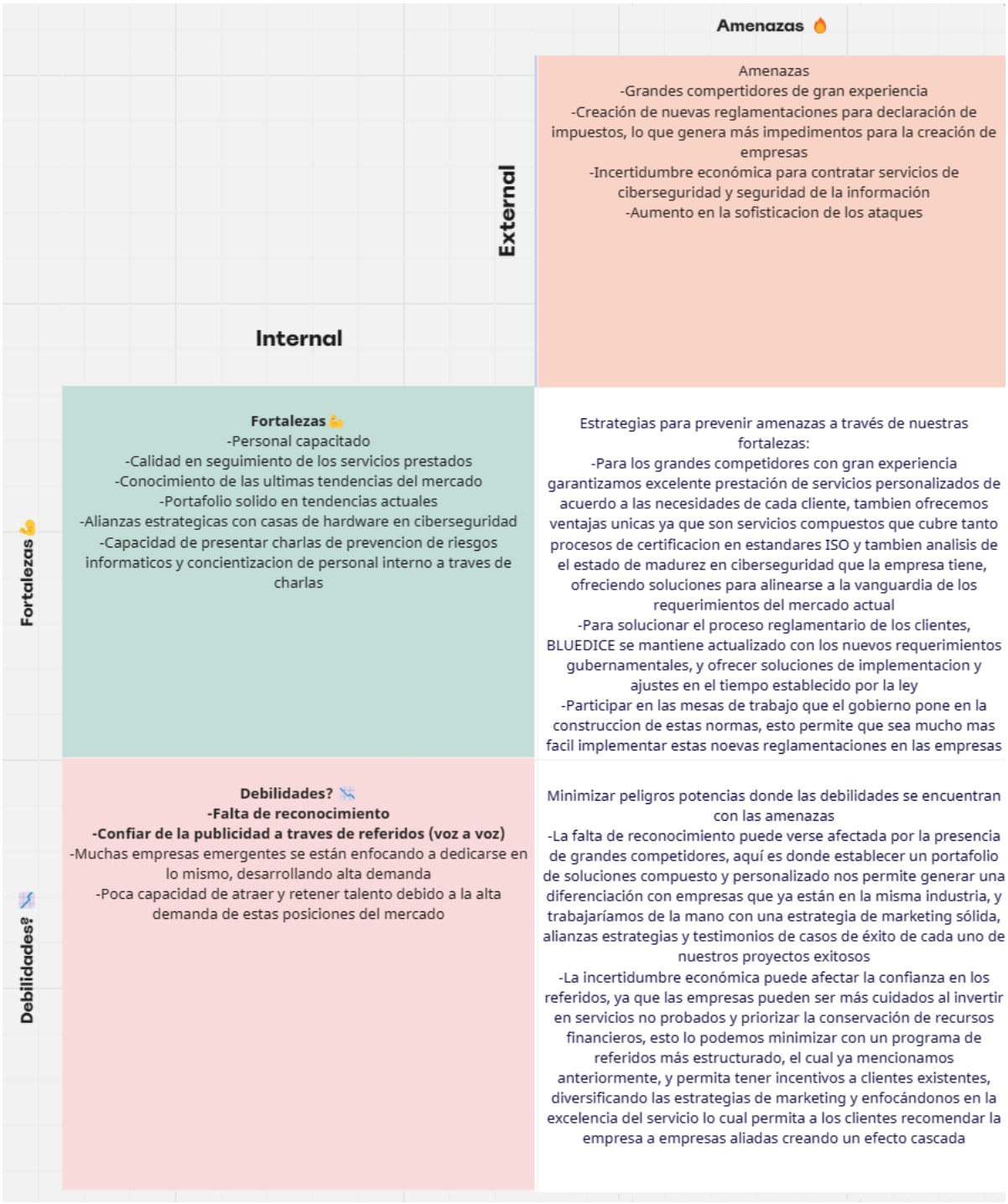
Imagen 23 - Análisis cruzado matriz DOFA



Fuente: Elaboración propia

8.4.2. Análisis Cruzado Amenazas

Imagen 24 - Análisis cruzado matriz DOFA Amenazas



Fuente: Elaboración propia

8.5. Normatividad empresarial

Existe un marco normativo que regula las micro, pequeñas y medianas empresas (MiPymes) los cuales acogería a la empresa Bluedice S.A.S debido a que esta pertenece a la presente categoría.

A continuación, se presenta la reglamentación a la cual se acoge la organización:

Tabla 22 - Normatividad aplicable

Norma	Tema
Ley 1838 de 2017	Por la cual se dictan normas de fomento a la ciencia, tecnología e innovación mediante la creación de empresas de base tecnológica (SPIN OFFS) y se dictan otras disposiciones.
Ley 1819 de 29 de diciembre 2016	Por medio de la cual se adopta una Reforma Tributaria estructural, se fortalecen los mecanismos para la lucha contra la evasión y la elusión fiscal, y se dictan otras disposiciones
Ley 1793 del 7 de julio de 2016	Por medio de la cual se dictan normas en materia de costos de los servicios financieros y se dictan otras disposiciones.
Ley 1780 del 2 de mayo de 2016	Por medio de la cual se promueve el empleo y el emprendimiento juvenil, se generan medidas para superar barreras de acceso al mercado de trabajo y se dictan otras disposiciones.
Ley 1607 de 2012	Reforma al Estatuto Tributario, o Reforma Tributaria, mediante la cual se deroga la Ley 963 de 2005 creadora del Régimen de Estabilidad Jurídica.
Ley 1429 de 29 de diciembre de 2010	Por la cual se expide la ley de formalización y generación de empleo
Ley1314 del 13 de julio de 2009	Por la cual se regulan los principios y normas de contabilidad e información financiera y de aseguramiento de información aceptados en Colombia, se señalan las autoridades competentes, el procedimiento para su expedición y se determinan las entidades responsables de vigilar su cumplimiento.
Ley 1014 de 2006	De fomento a la cultura del emprendimiento
Ley 1004 de 2005	Modifica un régimen especial para estimular la inversión y se dictan otras disposiciones

Ley 963 de 2005	Instaura una ley de estabilidad jurídica para los inversionistas en Colombia.
Ley 905 del 2 de agosto de 2004	Por medio de la cual se modifica la Ley 590 de 2000 sobre promoción del desarrollo de la micro, pequeña y mediana empresa colombiana y se dictan otras disposiciones.

Fuente: Elaboración propia

La empresa será constituida como una Sociedad por acciones Simplificada (S.A.S), teniendo en cuenta que este tipo de sociedad tiene la flexibilidad de adaptarse a cualquier empresa, así como a su actividad económica a continuación se describen los pasos para la constitución de la empresa:

Tabla 23 - Requerimientos Constitución de empresa

Requerimientos constitución legal	Documento
Consultar nombre	Rues
Suscribir Estatutos en la Cámara de comercio	Estatutos Fotocopia RL Fotocopia Accionistas Cedula del Apoderado Poder Autentico
Pre-Rut DIAN	
Matricula Mercantil	0,7% sobre el capital asignado
Abrir cuenta Bancaria	Pre RUT Certificado de Cámara y comercio Cedula de Ciudadanía Formulario 1648 DIAN
Solicitar NIT	Certificación de la cuenta Fotocopia de la cedula
Inscribir NIT en cara y comercio	
Solicitud de Facturación electrónica	Nit Formulario 1302 Certificado de Cámara y comercio
Inscribir libros oficiales de Cámara y comercio	

Fuente: Elaboración propia

Bluedice al estar constituida como una pyme deberá cumplir con las obligaciones tributarias las cuales están regidas por la siguiente regulación Ley 2155 de 2021 o reforma tributaria, la cuales se describen a continuación:

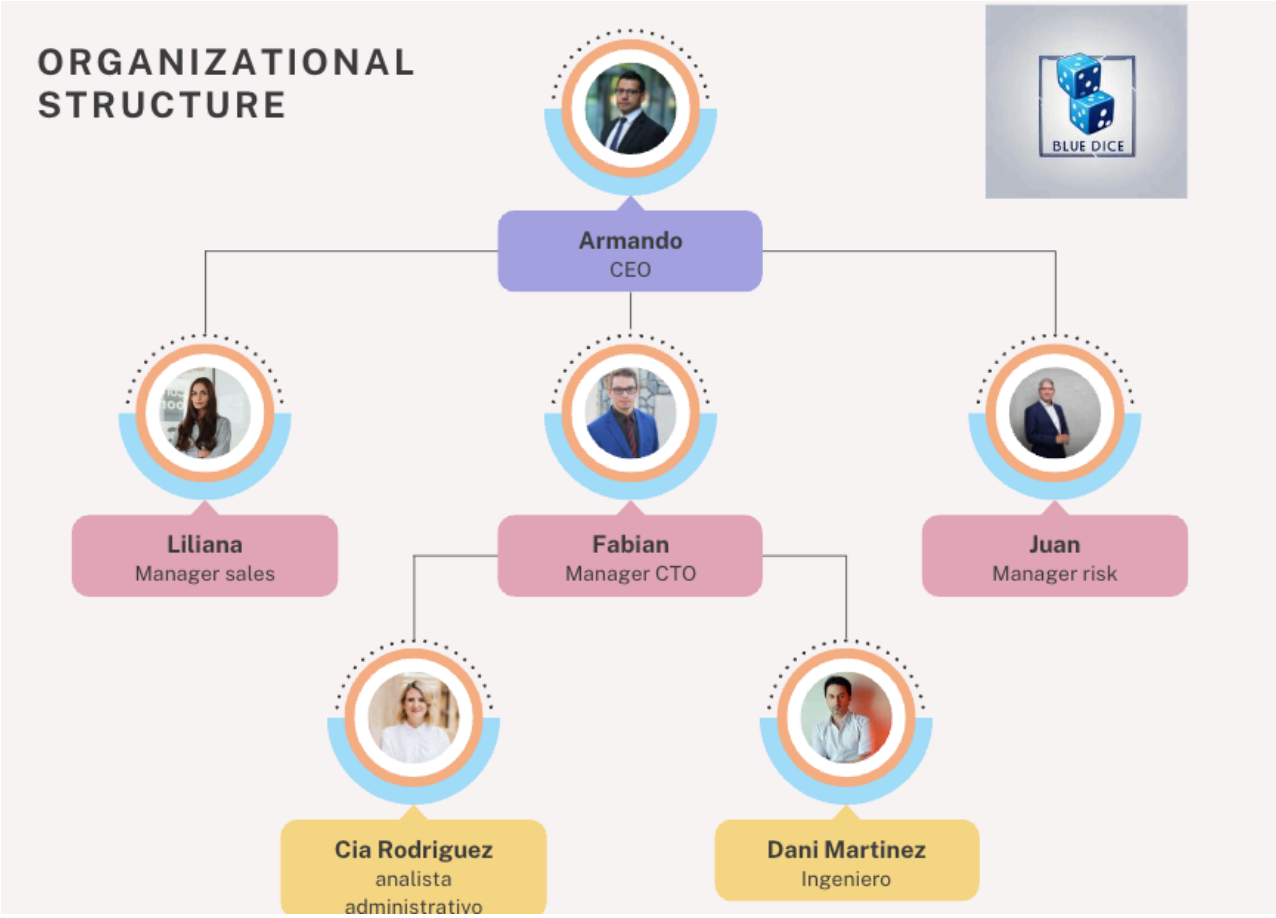
- Impuesto de Renta.
- Impuesto al Valor Agregado (IVA).
- ICA.
- Retención en la Fuente.
- Impuesto al Patrimonio
- Gravamen a los Movimientos Financieros, y aportes Parafiscales.

9. Aspectos financieros

Periodo de Arranque del proyecto

Se espera que Bluedice inicié operaciones formalmente el segundo semestre del 2024, debido a que se necesita mínimo 3 a meses para el prealistamiento de los requisitos normativos para su puesta en funcionamiento

Imagen 25 - Estructura organizacional Bluedice



Fuente: Elaboración propia

Periodo improductivo

El periodo improductivo se espera que no sea mayor a 3 meses luego de haberse constituido la empresa.

Ingresos/ventas primer año

La proyección de ingresos/Ventas el primer año dará una visión clara de la proyección de los ingresos a causa del portafolio de servicios brindados por BLUEDICE. Dentro del análisis se provee que el primer año se tendrán ingresos totales por valor de $409.500.000

Imagen 26 - Ingresos- Ventas año 1

INGRESOS/VENTAS DEL PRIMER AÑO

	NOMBRE DEL PRODUCTO O SERVICIO	CANTIDADES		PRECIO DE VENTA UNITARIO SIN IVA		INGRESOS TOTALES	
1	Implementacion de Sistemas de Gestión X proceso	25,00	$	5.500.000,00	$	137.500.000	34%
2	Bolsas de horas	280,00	$	300.000,00	$	84.000.000	21%
3	Auditoria por proceso	25,00	$	1.800.000,00	$	45.000.000	11%
4	Pruebas de Ciberseguridad alto nive	25,00	$	2.800.000,00	$	70.000.000	17%
5	Pruebas de ingenieria Social	20,00	$	1.700.000,00	$	34.000.000	8%
6	Pruebas de Ciberseguridad aplicaciones Moviles	30,00	$	1.300.000,00	$	39.000.000	10%
7		-	$	-	$	-	0%
8		-	$	-	$	-	0%
9		-	$	-	$	-	0%
10		-	$	-	$	-	0%
				TOTAL	$	409.500.000	100%

Fuente: Elaboración propia

Costos de cada producto o servicio

En la definición del alcance de los costos de los productos y/o servicios ofrecidos por BLUEDICE, se construyó el número de servicios que debemos dar y el costo monetario que este representa. Estos costos fueron estimados de acuerdo con el alcance y el esfuerzo de cada uno de ellos

Es importante resaltar que otro objetivo por el cual se construyó una tabla con precios, es definir un estándar y que no se cometa un grave error y es cobrar dependiente el tipo y/o tamaño de la empresa.

Imagen 27 - Costos por servicio

COSTOS DE CADA PRODUCTO O SERVICIO

	NOMBRE DEL PRODUCTO SERVICIO	CANTIDADES	COSTO UNITARIO DEL PDTO O SERVICIO	COSTOS TOTALES	
1	Implementacion de Sistemas de Gestión X proceso	25	$ 2.700.000,00	$ 67.500.000	36%
2	Bolsas de horas	280	$ 130.000,00	$ 36.400.000	19%
3	Auditoria por proceso	25	$ 700.000,00	$ 17.500.000	9%
4	Pruebas de Ciberseguridad alto nivel	25	$ 1.600.000,00	$ 40.000.000	21%
5	Pruebas de ingenieria Social	20	$ 800.000,00	$ 16.000.000	8%
6	Pruebas de Ciberseguridad aplicaciones Moviles	30	$ 400.000,00	$ 12.000.000	6%
7	0	0	$ -	$ -	0%
8	0	0	$ -	$ -	0%
9	0	0	$ -	$ -	0%
10	0	0	$ -	$ -	0%
			TOTAL	$ 189.400.000	100%

Fuente: Elaboración propia

Proyecciones

Dentro del análisis financiero se incluyó una proyección a 5 años (2028), cuya finalidad es poder determinar el margen operativo y viabilidad del negocio. Para BLUEDICE la simulación se ve en la siguiente tabla:

Imagen 28 - Proyecciones por año

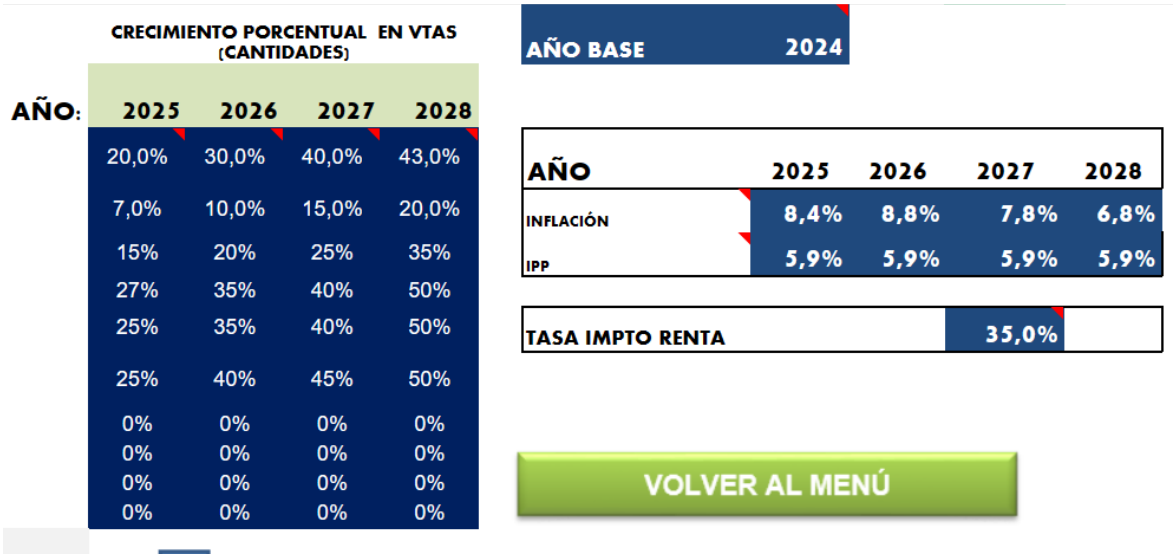
PROYECCIONES

AÑO	2024	2025	2026	2027	2028
VENTAS ANUALES	$ 409.500.000,0	$ 527.426.130,0	$ 732.191.923,6	$ 1.066.112.847,3	$ 1.617.285.994,4
COSTOS ANUALES	$ 189.400.000,0	$ 239.199.507,0	$ 323.965.356,6	$ 464.535.266,8	$ 700.650.188,0
MARGEN OPERATIVO	**$ 220.100.000,0**	**$ 288.226.623,0**	**$ 408.226.567,0**	**$ 601.577.580,5**	**$ 916.635.806,4**

Crecimiento porcentual en ventas/cantidades

Se espera que bajo una proyección conservadora a cierre del 2028 tengamos un incremento del 43%

Imagen 29 - Crecimiento en ventas



CRECIMIENTO PORCENTUAL EN VTAS (CANTIDADES)

AÑO:	2025	2026	2027	2028
	20,0%	30,0%	40,0%	43,0%
	7,0%	10,0%	15,0%	20,0%
	15%	20%	25%	35%
	27%	35%	40%	50%
	25%	35%	40%	50%
	25%	40%	45%	50%
	0%	0%	0%	0%
	0%	0%	0%	0%
	0%	0%	0%	0%
	0%	0%	0%	0%

AÑO BASE	2024

AÑO	2025	2026	2027	2028
INFLACIÓN	8,4%	8,8%	7,8%	6,8%
IPP	5,9%	5,9%	5,9%	5,9%

TASA IMPTO RENTA	35,0%

VOLVER AL MENÚ

Fuente: Elaboración propia

Se plantean las siguientes proyecciones de ventas las cuales tiene un aumento alto por año teniendo como base las siguientes premisas:

A. Las empresas que están certificadas en el sistema de Gestión de Seguridad de la información con ISO27001:2013, si conservan la certificación y alcance actual, deben ajustar la documentación, sistemas, procesos y procedimiento a la versión de la nueva normatividad, la ISO 27001:2022.
B. Para las entidades vigiladas por la Superfinanciera la normatividad exige la prestación de los servicios, que se consideren los servicios en la nube, por lo que se tienen que realizar ajustes a nivel de procesos, procedimientos, garantizando la información de cada sistema.

C. En general, se observará un crecimiento ya que cada vez hay más organizaciones que requieren tener sistemas seguros y contar con la certificación ISO 27001, para tener más oportunidades en el mercado colombiano y participar en procesos de contratación con el Estado. Adicional a ello se evidencia como el crecimiento de los ciberataques hace que cada día existan más empresas que busquen asegurar sus datos.

Inversión inicial para puesta en marcha del negocio

Para la puesta en marcha de BLUEDICE, se debe contar con una inversión inicial de $30.000.000. Dentro de este valor están contemplado (espacios físicos y de cómputo, muebles, equipos de oficina, y gastos operativos).

Imagen 30 - Inversión inicial

	INVERSIÓN INICIAL	
TERRENOS	$	-
PROPIEDAD PLANTA Y EQUIPO	$	15.000.000,00
MUEBLES Y ENSERES	$	6.000.000,00
EQUIPO DE OFICINA	$	8.000.000,00
EQUIPO DE TRANSPORTE	$	-
FRANQUICIAS	$	-
PATENTES /INV en INTANGIBLES	$	-
GASTOS DE PUESTA EN MARCHA	$	1.000.000,00
TOTAL INVERSIONES	$	30.000.000,00

Fuente: Elaboración propia

Presupuesto Marketing Mix año de inicio

Dentro la inversión, se contempló un rubro netamente enfocado al área de mercadeo, Su objetivo principal es el posicionamiento de BLUEDICE en las búsquedas en Google, redes sociales y la creación del perfil en LinkedIn.

Imagen 31 - Presupuestos Marketing Mix

PRESUPUESTO DEL MARKETING MIX año de INICIO.	$ 5.000.000,00

Fuente: Elaboración propia

Gastos Fijos:

De acuerdo con el análisis financiero se logró identificar que durante el primer año de la ejecución de BLUEDICE se prevén gastos fijos por valor de $96.900.000.

Se prevé que con esta inversión se logre dar todos los recursos necesarios para un óptimo funcionamiento tanto para la compañía como sus empleados.

Imagen 32 - Gastos fijos

GASTOS FIJOS:	VALOR AÑO 1
ARRIENDO:	$ 7.000.000,00
SERVICIOS PÚBLICOS:	$ 4.500.000,00
TELEFONÍA CELULAR:	$ 2.400.000,00
INTERNET:	$ 6.000.000,00
PAPELERÍA:	-
	$ -
SERVICIOS DE SEGURIDAD:	
SERVICIOS DE ASEO:	
Sevicios de Coworking	$ 5.000.000,00
Outsourcing	$ 12.000.000,00
Servicios Outsourcing	$ 60.000.000,00
	$ -
	$ -
	$ -
TOTAL GASTOS FIJOS	$ 96.900.000,00

Fuente: Elaboración propia

Inversión Total y necesidades de financiación

La inversión inicial necesaria para poner en marcha BLUEDICE en el año 2024 es de unos $191.525.000,00. Dentro de los conceptos están incluíos los operativos, nomina, marketing, gastos fijos.

El costo que los emprendedores deben invertir en el proyecto es de alrededor de $55.000.000 y de debe hacer una solicitud de préstamo a alguna entidad bancaria con la finalidad de financiar a BLUEDICE por un valor de $ 136.525.000

Dentro de la proyección financiera se contempló que este crédito que se adquiera con una entidad financiera sea proyectado para un pago anual con el objetivo de no incurrir en gastos adicionales por el pago de intereses o seguros dentro del mismo crédito.

Imagen 33 - Inversión total

INVERSIÓN TOTAL Y NECESIDADES DE FINANCIACIÓN

TOTAL INVERSIONES	$ 30.000.000,00			TASA DE INT ANUAL CRÉDITO 13,50%			AÑOS DE CRÉDITO 5		
CALCULO DEL CAPITAL DE TRABAJO INICIAL				**CALCULO DEL PRÉSTAMO**					
	MESES	**VALOR**			inicial	interés	amort	cuota	final
COSTOS OPERATIVOS	6,0	$ 94.700.000,00		**AÑO 0**					$136.525.000,0
NÓMINAS	3,0	$ 13.375.000,00		**2024**	$136.525.000,0	$18.430.875,0	$20.859.804,3	$ 39.290.679,3	$115.665.195,7
MARKETING MIX	12,0	$ 5.000.000,00		**2025**	$115.665.195,7	$15.614.801,4	$23.675.877,9	$ 39.290.679,3	$ 91.989.317,8
GASTOS FIJOS	6,0	$ 48.450.000,00		**2026**	$ 91.989.317,8	$12.418.557,9	$26.872.121,4	$ 39.290.679,3	$ 65.117.196,4
TOTAL		**$ 161.525.000,00**		**2027**	$ 65.117.196,4	$ 8.790.821,5	$30.499.857,8	$ 39.290.679,3	$ 34.617.338,6
				2028	$ 34.617.338,6	$ 4.673.340,7	$34.617.338,6	$ 39.290.679,3	$ -
TOTAL INVERSIÓN		**$ 191.525.000,00**							
APORTE DE LOS EMPRENDEDORES		**$ 55.000.000,00**							
PRÉSTAMO A SOLICITAR		**$ 136.525.000,00**							

VOLVER AL MENÚ

Fuente: Elaboración propia

9.1. Estados financieros Básicos proyectados

Estado de resultados:

Imagen 34 - Estado de resultados

ESTADOS FINANCIEROS BÁSICOS PROYECTADOS

Todos los datos de los Estados financieros se generan de forma automática.

ESTADO DE RESULTADOS

	2024	2025	2026	2027	2028
VENTAS	$ 409.500.000,0	$ 527.426.130,0	$ 732.191.923,6	$ 1.066.112.847,3	$ 1.617.285.994,4
COSTO VENTAS	$ 189.400.000,0	$ 239.199.507,0	$ 323.965.356,6	$ 464.535.266,8	$ 700.650.188,0
UTILIDAD BRUTA	$ 220.100.000,0	$ 288.226.623,0	$ 408.226.567,0	$ 601.577.580,5	$ 916.635.806,4
GASTOS ADTIVOS Y VTAS	$ -	$ -	$ -	$ -	$ -
GASTOS FIJOS DEL PERIODO	$ 96.900.000,0	$ 104.991.150,0	$ 114.230.371,2	$ 123.140.340,2	$ 131.513.883,3
OTROS GASTOS	$ 5.000.000,0	$ 6.000.000,0	$ 5.000.000,0	$ 5.000.000,0	$ 5.000.000,0
DEPRECIACIÓN	$ 4.500.000,0	$ 4.500.000,0	$ 4.500.000,0	$ 4.500.000,0	$ 4.500.000,0
UTILIDAD OPERATIVA	$ 113.700.000,0	$ 172.735.473,0	$ 284.496.195,8	$ 468.937.240,4	$ 775.621.923,1
GASTOS FINACIEROS	$ 16.625.250,0	$ 14.085.059,8	$ 11.201.944,0	$ 7.929.607,5	$ 4.215.505,6
UTILIDAD ANTES DE IMPTOS	$ 97.074.750,0	$ 158.650.413,2	$ 273.294.251,8	$ 461.007.632,8	$ 771.406.417,5
IMPUESTOS	$ 33.976.162,5	$ 55.527.644,6	$ 95.652.988,1	$ 161.352.671,5	$ 269.992.246,1
UTILIDAD NETA	**$ 63.098.587,5**	**$ 103.122.768,6**	**$ 177.641.263,6**	**$ 299.654.961,3**	**$ 501.414.171,4**

Fuente: Elaboración propia

Balance:

El balance permite establecer gastos de caja con base a la plantilla presentada durante la actividad permite establecer gastos de caja, flujo depreciable y no depreciable, depreciación acumulada y activo fijo para los siguientes cinco años, lo que permite establecer un estimado del Activo, pasivo y patrimonio esperado para los siguientes años, es importante resaltar que esta proyección es viable siempre y cuando en el primer año se cumplan las siguientes condiciones:

- El total activo sea iguales o superiores a $190.000.000.
- El pasivo, que representa el préstamo solicitado más los gastos iniciales sean de los $136.000.000 planteados originalmente.
- El valor del patrimonio se estima que esté alrededor de los $55.000.000.

- Estas condiciones permiten entender si la proyección esperada para la empresa tiene los resultados esperados o si se debe plantear un plan de maniobra.

Imagen 35 - Balance

BALANCE

	AÑO 0	2024	2025	2026	2027	2028
			ACTIVO			
CAJA/BANCOS	$ 161.525.000,00	$ 186.934.320,69	$ 225.142.739,38	$ 312.626.466,26	$ 469.776.056,76	$ 745.837.718,06
FIJO NO DEPRECIABLE	$ -	$ -	$ -	$ -	$ -	$ -
FIJO DEPRECIABLE	$ 30.000.000,00	$ 30.000.000,00	$ 30.000.000,00	$ 30.000.000,00	$ 30.000.000,00	$ 30.000.000,00
DEPRECIACIÓN ACUMULADA	$ -	$ 4.500.000,00	$ 9.000.000,00	$ 13.500.000,00	$ 18.000.000,00	$ 22.500.000,00
ACTIVO FIJO NETO	$ 30.000.000,00	$ 25.500.000,00	$ 21.000.000,00	$ 16.500.000,00	$ 12.000.000,00	$ 7.500.000,00
TOTAL ACTIVO	**$ 191.525.000,00**	**$ 212.434.320,69**	**$ 246.142.739,38**	**$ 329.126.466,26**	**$ 481.776.056,76**	**$ 753.337.718,06**
			PASIVO			
Impuestos X Pagar	0	$ 14.619.193,8	$ 34.703.697,6	$ 73.153.244,5	$ 137.255.551,4	$ 244.418.201,3
TOTAL PASIVO CORRIENTE	$ -	$ 14.619.193,8	$ 34.703.697,6	$ 73.153.244,5	$ 137.255.551,4	$ 244.418.201,3
Obligaciones Financieras	$ 136.525.000,00	$ 115.665.195,69	$ 91.989.317,80	$ 65.117.196,39	$ 34.617.338,60	$ -
PASIVO	**$ 136.525.000,00**	**$ 130.284.389,44**	**$ 126.693.015,35**	**$ 138.270.440,85**	**$ 171.872.889,95**	**$ 244.418.201,32**
			PATRIMONIO			
Capital Social	$ 55.000.000,00	$ 55.000.000,00	$ 55.000.000,00	$ 55.000.000,00	$ 55.000.000,00	$ 55.000.000,00
Utilidades del Ejercicio	0	$ 27.149.931,3	$ 64.449.724,0	$ 135.856.025,4	$ 254.903.166,8	$ 453.919.516,7
TOTAL PATRIMONIO	**$ 55.000.000,00**	**$ 82.149.931,25**	**$ 119.449.724,03**	**$ 190.856.025,41**	**$ 309.903.166,80**	**$ 508.919.516,74**
TOTAL PAS + PAT	**$ 191.525.000,00**	**$ 212.434.320,69**	**$ 246.142.739,38**	**$ 329.126.466,26**	**$ 481.776.056,76**	**$ 753.337.718,06**
CUADRE (ACT = PAS+PAT)	$ -	$ -	$ -	$ -	$ -	$ -

Fuente: Elaboración propia

Flujo de caja del proyecto

Bluedice para un óptimo desempeño de sus operaciones necesita un flujo de caja con las siguientes características:

- El KTNO (Capital de trabajo neto operativo) para el primer año por un valor de $161.525.000 y se espera de a lo largo de los siguientes 5 años (en el 2028) sea por un valor de $501.419.517
- Activos fijos brutos: El promedio de los activos fijos netos de BLUEDICE a lo largo de 5 años está proyectado en un valor de $30.000.000

Imagen 36 - Flujo de caja

FLUJO DE CAJA DEL PROYECTO:
CAPITAL INVERTIDO

	AÑO 0	2024	2025	2026	2027	2028
Activos Corrientes	$ 161.525.000	$ 186.934.321	$ 225.142.739	$ 312.626.466	$ 469.776.057	$ 745.837.718
Pasivos Corrientes	$ -	$ 14.619.194	$ 34.703.698	$ 73.153.244	$ 137.255.551	$ 244.418.201
KTNO	**$ 161.525.000**	**$ 172.315.127**	**$ 190.439.042**	**$ 239.473.222**	**$ 332.520.505**	**$ 501.419.517**
Activo Fijo Neto	$ 30.000.000	$ 25.500.000	$ 21.000.000	$ 16.500.000	$ 12.000.000	$ 7.500.000
Depreciación Acumulada	$ -	$ 4.500.000	$ 9.000.000	$ 13.500.000	$ 18.000.000	$ 22.500.000
Activo Fijo Bruto	**$ 30.000.000**	**$ 30.000.000**	**$ 30.000.000**	**$ 30.000.000**	**$ 30.000.000**	**$ 30.000.000**
Total Capital Operativo Neto	$ 191.525.000	$ 197.815.127	$ 211.439.042	$ 255.973.222	$ 344.520.505	$ 508.919.517

CALCULO DEL FLUJO DE CAJA LIBRE

EBIT	$ 60.200.000,0	$ 114.768.223,0	$ 221.427.827,8	$ 400.949.539,7	$ 703.011.058,8
Impuestos	$ 21.070.000,0	$ 40.168.878,1	$ 77.499.739,7	$ 140.332.338,9	$ 246.053.870,6
NOPLAT	$ 39.130.000,0	$ 74.599.345,0	$ 143.928.088,0	$ 260.617.200,8	$ 456.957.188,2
Inversión Neta	$ -6.290.126,9	$ -13.623.914,9	$ -44.534.180,0	$ -88.547.283,6	$ -164.399.011,3
Flujo de Caja Libre del periódo	**$ 32.839.873**	**$ 60.975.430**	**$ 99.393.908**	**$ 172.069.917**	**$ 292.558.177**

Fuente: Elaboración propia

Cálculo del flujo de caja libre

El Cálculo del flujo de caja libre permitirá identificar cuanto efectivo genera una empresa después de cubrir sus gastos operativos y de inversión. Para el año 1 el costo será de $32.839.873, sin embargo, basados en la proyección, se espera finalizar el año 2028 con un incremento significativo de $292.558.177 debido a que a esta fecha ya se contempla lograr y superar el punto de equilibrio generando ganancias y rentabilidad.

Imagen 37 -Calculo de flujo de caja

CALCULO DEL FLUJO DE CAJA LIBRE

EBIT	$ 60.200.000,0	$ 114.768.223,0	$ 221.427.827,8	$ 400.949.539,7	$ 703.011.058,8
Impuestos	$ 21.070.000,0	$ 40.168.878,1	$ 77.499.739,7	$ 140.332.338,9	$ 246.053.870,6
NOPLAT	$ 39.130.000,0	$ 74.599.345,0	$ 143.928.088,0	$ 260.617.200,8	$ 456.957.188,2
Inversión Neta	$ -6.290.126,9	$ -13.623.914,9	$ -44.534.180,0	$ -88.547.283,6	$ -164.399.011,3
Flujo de Caja Libre del periódo	**$ 32.839.873**	**$ 60.975.430**	**$ 99.393.908**	**$ 172.069.917**	**$ 292.558.177**

Fuente: Elaboración propia

9.2. Evaluación financiera y punto de equilibrio

Tasa de Evaluación del proyecto

Esta es la tasa mínima que se espera obtener al invertir en la empresa; si el rendimiento real supera el 30%, se considera una inversión positiva.

Imagen 38 - Punto de equilibrio

EVALUACIÓN FINANCIERA Y PUNTO DE EQULIBRIO	
TASA DE EVALUACIÓN DEL PROYECTO	30,00%

Fuente: Elaboración propia

Valor presente neto del proyecto

Se espera que el proyecto genere un margen de ganancia de $54.098.201 después de haber descontado los costos y flujos de efectivo futuros a la tasa de descuento apropiada.

La Tasa Interna de Retorno (TIR) es del 39.67%. Esta tasa representa la tasa de crecimiento anualizada que iguala el VPN a cero, el rendimiento que hace que los flujos de efectivo del proyecto sean valiosos que la inversión inicial; tanto el VPN positivo como la TIR del 39.67% sugieren que el proyecto podría ser financieramente atractivo, ya que está generando un retorno significativo sobre la inversión inicial.

Imagen 39 - TIR

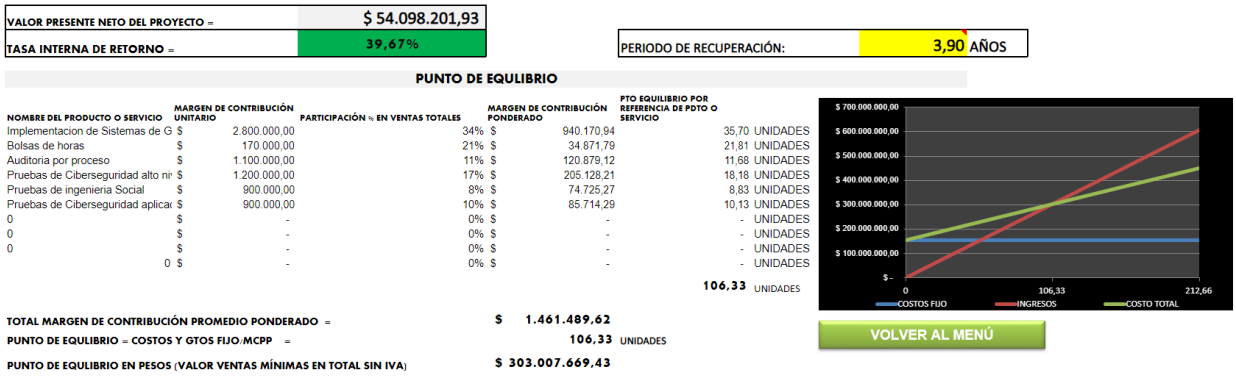
VALOR PRESENTE NETO DEL PROYECTO =	$ 54.098.201,93
TASA INTERNA DE RETORNO =	39,67%

Fuente: Elaboración propia

Punto de equilibrio

Según el modelo el punto de equilibrio proyectado está alrededor de $ 1303.007.669,43 pesos colombianos sin incluir IVA. Esto indica que Bluedice en un periodo aproximado de 3,90 años tendrá un balance en donde los gastos no serán superiores a los ingresos. Se espera que luego de este tiempo, la empresa empieza a generar ganancias, capitalice su patrimonio y pueda devolver el costo invertido por sus accionistas

Imagen 40 - Punto de equilibrio



VALOR PRESENTE NETO DEL PROYECTO =	$ 54.098.201,93
TASA INTERNA DE RETORNO =	39,67%

PERIODO DE RECUPERACIÓN: 3,90 AÑOS

PUNTO DE EQULIBRIO

NOMBRE DEL PRODUCTO O SERVICIO	MARGEN DE CONTRIBUCIÓN UNITARIO	PARTICIPACIÓN % EN VENTAS TOTALES	MARGEN DE CONTRIBUCIÓN PONDERADO	PTO EQUILIBRIO POR REFERENCIA DE PDTO O SERVICIO
Implementacion de Sistemas de G	$ 2.800.000,00	34%	$ 940.170,94	35,70 UNIDADES
Bolsas de horas	$ 170.000,00	21%	$ 34.871,79	21,81 UNIDADES
Auditoria por proceso	$ 1.100.000,00	11%	$ 120.879,12	11,68 UNIDADES
Pruebas de Ciberseguridad alto ni	$ 1.200.000,00	17%	$ 205.128,21	18,18 UNIDADES
Pruebas de ingenieria Social	$ 900.000,00	8%	$ 74.725,27	8,83 UNIDADES
Pruebas de Ciberseguridad aplicac	$ 900.000,00	10%	$ 85.714,29	10,13 UNIDADES
0	$ -	0%	$ -	- UNIDADES
0	$ -	0%	$ -	- UNIDADES
0	$ -	0%	$ -	- UNIDADES
0	$ -	0%	$ -	- UNIDADES
				106,33 UNIDADES

TOTAL MARGEN DE CONTRIBUCIÓN PROMEDIO PONDERADO =	$ 1.461.489,62	
PUNTO DE EQUILIBRIO = COSTOS Y GTOS FIJO/MCPP =	106,33	UNIDADES
PUNTO DE EQUILIBRIO EN PESOS (VALOR VENTAS MÍNIMAS EN TOTAL SIN IVA)	$ 303.007.669,43	

Fuente: Elaboración propia

10. Sostenibilidad

Bluedice entiende que la sostenibilidad no se limita a un solo aspecto, sino que abarca dimensiones económicas, sociales y ambientales. Esta estrategia integral busca no solo minimizar el impacto negativo de las operaciones, sino también crear valor compartido para todas las partes interesadas. Bluedice espera compartir las siguientes estrategias específicas en cada dimensión, junto con las acciones concretas y los mecanismos de seguimiento asociados:

Tabla 24 - Estrategias de Sostenibilidad Bluedice

Dimensión	Objetivo	Acciones	Mecanismos de Seguimiento
Social	Contribuir al bienestar social y promover una cultura de responsabilidad compartida	- Ofrecer servicios de concientización y capacitación en ciberseguridad a comunidades locales y organizaciones sin fines de lucro.	- Retroalimentación de los participantes sobre la utilidad y efectividad de las capacitaciones. - Evaluación del impacto percibido en la comunidad.
		- Participar en eventos y actividades de divulgación sobre ciberseguridad en escuelas y centros comunitarios.	- Encuestas a los asistentes para medir el nivel de conocimiento y conciencia sobre ciberseguridad. - Informes sobre la participación en eventos.

Económica	Garantizar la viabilidad económica y la sostenibilidad financiera de la empresa	- Desarrollar un modelo de negocio sostenible que considere tarifas justas y transparentes, al tiempo que integre prácticas sostenibles.	- Análisis periódico de la rentabilidad y los costos operativos. - Revisión de la percepción del cliente sobre la propuesta de valor.
		- Fomentar alianzas estratégicas con proveedores de tecnología y servicios que compartan valores de sostenibilidad.	- Evaluación del impacto de las alianzas en la rentabilidad y la sostenibilidad económica. - Feedback de los clientes sobre la calidad de los servicios.
Ambiental	Minimizar el impacto ambiental y promover prácticas sostenibles	- Promover el trabajo remoto y el uso de tecnologías digitales para reducir la huella de carbono asociada con los desplazamientos y el consumo de papel.	- Monitorización del consumo de energía y recursos digitales. - Evaluación del impacto de las prácticas sostenibles en la reducción de la huella ambiental.

		- Compensar las emisiones de carbono mediante la participación en proyectos de reforestación o energías renovables.	- Seguimiento de la participación en programas de compensación de carbono. - Informes sobre la contribución a proyectos ambientales.
Seguimiento	Evaluar el progreso y ajustar la estrategia de sostenibilidad	- Establecer indicadores clave de desempeño (KPI) para cada dimensión de sostenibilidad y revisarlos periódicamente.	- Elaboración de informes trimestrales de sostenibilidad para revisión interna y análisis de resultados. - Reuniones periódicas para revisar los KPI y ajustar la estrategia.
Gobierno Corporativo	Desarrollar una dimensión de gobierno corporativo en Bluedice, que incluya aspectos de sostenibilidad apalancados con los	Creación de Valor Compartido: Identificar oportunidades para alinear los objetivos de Bluedice con los ODS, enfocándose en áreas como la protección de	Identificación de ODS relevantes: Analizar y seleccionar los ODS que mejor se alineen con la misión y actividades de ciberseguridad de Bluedice, priorizando aquellos relacionados con la protección de infraestructuras críticas

	objetivos de desarrollo sostenible como marco de referencia, definiendo linear jerárquica y procesos misionales para generar valor compartido en Bluedice, fortaleciendo así su contribución al logro de una infraestructura digital segura y sostenible.	infraestructuras críticas (ODS 9), promoción de la paz y seguridad cibernética (ODS 16), y colaboración internacional en ciberseguridad (ODS 17).	(ODS 9), la promoción de la paz y la justicia (ODS 16) y la colaboración internacional (ODS 17). Desarrollo de alianzas estratégicas: Establecer alianzas estratégicas con otras organizaciones, instituciones gubernamentales y entidades del sector privado que compartan los mismos objetivos relacionados con los ODS, promoviendo así la colaboración y el intercambio de mejores prácticas en ciberseguridad a nivel nacional e internacional.

Fuente: Elaboración propia

11. Conclusiones

El análisis de mercado realizo permitió identificar los competidores actuales, al igual que unas oportunidades de crecimiento significativo en el sector de la prestación de servicios de Seguridad de la información, Ciberseguridad y riesgos, si bien se evidencian diversos competidores en el mercado también se evidenciaron oportunidades de crecimiento y expansión en nichos de mercado no cubiertos teniendo en cuenta la creciente demanda de servicios especializados en términos de seguridad de la información y ciberseguridad.

La realización del análisis de mercado proporcionando una base solidad para buscar estrategias efectivas que permitan que Bluedice pueda posicionarse en el mercado de manera competitiva y que pueda capitalizar las oportunidades emergentes en el mercado dinámico de la Seguridad de la información, Ciberseguridad y riesgos.

El análisis técnico y Operativo permitió identificar claramente los riesgo y oportunidades a los que se enfrentaría Bluedice para la prestación de los servicios, permitiendo crear estrategias sólidas para la creación del portafolio de servicio y la prestación del servicio.

El análisis estratégico y financiero es clave para validar tendencias del mercado, identificar oportunidades de negocio y asegurar la sostenibilidad y rentabilidad del negocio a largo plazo.

El análisis Financiero proyectado y las diferentes fuentes de ingresos iniciales de Bluedice muestra una comprensión clara y detallada de la viabilidad económica y financiera del proyecto demostrando la capacidad que tendría Bluedice para mantener un crecimiento económico sostenible, se evidencia como la empresa puede tener una gran rentabilidad en la prestación de los servicios teniendo un crecimiento del 20% por cada servicio tomando como base el crecimiento de las tecnologías emergentes y la generación de nueva normatividad que hace que las

organizaciones requieran conservar los protocolos de Seguridad de la información Ciberseguridad y Riesgo.

La evaluación y análisis de la estructura organizacional, procesos, procedimientos, equipo de talento humano y relacionamiento con los clientes de Bluedice proporciona una visión integral de su funcionamiento y su capacidad para satisfacer las necesidades del mercado identificando la importancia de una estructura organizacional eficiente y ágil que facilite la comunicación y la toma de decisiones.

Es importante tener un buen relacionamiento con los clientes con el fin de comprender mejor sus necesidades, expectativas y niveles de satisfacción, durante el análisis se pudieron identificar oportunidades para mejorar la experiencia del cliente, fortalecer las relaciones y poder fomentar la lealtad hacia Bluedice.

Se identificaron y priorizaron estrategias que permitan que Bluedice crezca de manera sostenible por medio de la implementación de prácticas empresariales éticas y responsables que generen beneficios tangibles tanto para la empresa como para la sociedad.

Referencias

La república (2023), *las empresas que han sido blanco de ciberataques en Colombia en el último año.* Recuperado de: https://www.larepublica.co/empresas/las-empresas-que-han-sido-blanco-de-ciberataques-en-colombia-en-el-ultimo-ano-3529667

Minitic (2023), *Colombia destinará $10.000 millones a la creación de un centro de ciberseguridad*. Recuperado de: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/276425:Colombia-destinara-10-000-millones-a-la-creacion-de-un-centro-de-ciberseguridad

NeDigital (2021), *Guía esencial sobre la ciberseguridad en Colombia.* Recuperado de https://www.nedigital.com/es/blog/ciberseguridad-en-colombia#:~:text=manejo%20de%20datos.-,Ley%201273%20de%202009,de%20software%20malicioso%2C%20entre%20otros

Javeriana (2023), *El ataque cibernético que sacude a Colombia*. Recuperado de: https://www.javeriana.edu.co/pesquisa/ciberataque-ifx-networks-colombia/

El tiempo (2023), *Ciberataque en Colombia: más grave y demorado de lo calculado.* Recuperado de: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberataque-en-colombia-es-mas-grave-y-demorado-de-lo-calculado-por-que-806234

Revista Enter (2023*), Conclusiones del ciberataque en Colombia: impacto y lecciones aprendidas*. Recuperado de: https://www.enter.co/empresas/seguridad/conclusiones-del-ciberataque-en-colombia-impacto-y-lecciones-aprendidas/

OAS (2019), *Ciberseguridad marzo NIST: Un abordaje integral de la ciberseguridad.* Recuperado de: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Asuntos Legales (2020), *Los delitos cometidos por medios informáticos crecieron 83% por cuenta de la pandemia.* Recuperado de: *https://www.asuntoslegales.com.co/consumidor/los-delitos-cometidos-por-medios-informaticos-crecieron-83-por-cuenta-de-la-pandemia-3099101*

Minitic, (2016), *Guía de gestión de riesgos: Seguridad y privacidad de la información.* Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

CCIT, (2023), *Estudio Anual de Ciberseguridad 2022-2023*. Recuperado de: https://www.ccit.org.co/estudios/estudio-anual-de-ciberseguridad-2022-2023/

Presidencia de la república, (2023), En 10,48% cierre de inflación anual a octubre de 2023, reveló el DANE. Recuperado de: https://petro.presidencia.gov.co/prensa/Paginas/En-1048--cierre-de-inflacion-anual-a-octubre-de-2023--revel--el-DANE-231108.aspx

Portafolio, (2023), A quiénes pertenece IFX, empresa del ciberataque que afecta al país https://www.portafolio.co/negocios/empresas/ifx-networks-quienes-son-los-duenos-de-la-empresa-que-recibio-ciberataque-tue-afecta-a-colombia-589134

Ciberseguridad y sostenibilidad: ¿Cómo se relacionan?

Recuperado de: El éxito de las empresas en expansión: estrategias de ciberseguridad | Rockwell Automation

Ministerio de la salud (2022), Colombia es pionero en transformación digital del sector salud https://www.minsalud.gov.co/Paginas/Colombia-es-pionero-en-transformacio-digital-del-sector-salud.aspx

Norma ISO 27001:2022 Information security, cybersecurity and privacy protection https://www.iso.org/es/contents/data/standard/08/28/82875.htmlINorma ISO 27001:2022 https://www.iso.org/es/contents/data/standard/08/28/82875.html

Rama judicial (2018) Administración / Gestión de riesgos – Lineamientos Guía. https://www.ramajudicial.gov.co/documents/5454330/14491339/Norma.ISO.31000.2018.Espanol.pdf/cb482b2c-afd9-4699-b409-0732a5261486

NIST Drafts Major Update to Its Widely Used Cybersecurity Framework (2023), https://www.nist.gov/news-events/news/2023/08/nist-drafts-major-update-its-widely-used-cybersecurity-framework

A. Anexos

Anexo 1 Encuestas y Entrevistas.zip.