

**PREFACTIBILIDAD PARA LA CREACION DE UNA EMPRESA EN SEGURIDAD  
DE LA INFORMACION PARA EL ORIENTE COLOMBIANO**

**ANA MILENA SUAREZ RODRIGUEZ  
JESUS GUALDRON FLOREZ  
OSCAR LEONARDO GIL MARIÑO**

**UNIVERSIDAD INDUSTRIAL DE SANTADER  
ESCUELA DE ESTUDIOS INDUSTRIALES Y EMPRESARIALES  
ESPECIALIZACIÓN EN EVALUACIÓN Y GERENCIA DE PROYECTOS  
BUCARAMANGA**

**2012**

**PREFACTIBILIDAD PARA LA CREACION DE UNA EMPRESA EN SEGURIDAD  
DE LA INFORMACION PARA EL ORIENTE COLOMBIANO**

**ANA MILENA SUAREZ RODRIGUEZ  
JESUS GUALDRON FLOREZ  
OSCAR LEONARDO GIL MARIÑO**

**Monografía para optar al título de especialistas en Gerencia y Evaluación de  
Proyectos**

**Docente**

**SANDRA MILENA MERCADO GONZALEZ**

**UNIVERSIDAD INDUSTRIAL DE SANTADER  
ESCUELA DE ESTUDIOS INDUSTRIALES Y EMPRESARIALES  
ESPECIALIZACIÓN EN EVALUACIÓN Y GERENCIA DE PROYECTOS  
BUCARAMANGA**

**2012**

## CONTENIDO

	Pág.
INTRODUCCION	16
1. ANTECEDENTES E HISTORIA DEL PROYECTO	18
2. ESTUDIO DE MERCADOS	21
2.1 OBJETIVOS	21
2.1.1 Objetivo Genel	21
2.1.2 Objetivos Específicos	21
2.2 MERCADO POTENCIAL Y OBJETIVO	22
2.2.1 Mercado Potencial	22
2.2.2 Mercado Objetivo	22
2.3 RECOPIACION DE INFORMACION DE DEMANDA Y COMPETENCIA	23
2.3.1 Fuentes Secundarias	23
2.3.2 Fuentes Primarias	24
2.4 ANALISIS DE LA INFORMACION RECOPIADA	29
2.4.1 Producto y/o Servicios	29
2.5 COMPETENCIA, NUESTROS SERVICIOS Y SUS SUSTITUTOS	35
2.5.1 Competidores	35
2.5.2 Nuestros servicios y sus Sustitutos	37
2.6 PRECIO	37
2.6.1 Análisis de precios de mercado	37
2.6.2 Estrategia para Fijar Precios	38
2.7 DESCRIPCION DE LA EMPRESA A CREAR	49
2.7.1 Nombre, Logo, Ubicación	49
2.7.2 Objeto Social De La Empresa	50
2.7.3 Misión y Visión de la Empresa	50
2.8 PUBLICIDAD, PROMOCION, DISTRIBUCION Y SERVICIO AL CLIENTE	51
2.8.1 Distribución	51

2.8.2 Publicidad	51
2.8.3 Promoción	51
2.8.4 Servicio al cliente	52
2.8.5 Presupuesto de costos de comercialización y ventas	53
2.9 PROCESO COMERCIALIZACION	54
2.9.1 Flujo grama de Proceso de Comercialización	54
2.10 ANALISIS DOFA	55
2.11 CONCLUSIONES ESTUDIO DE MERCADO	56
3. ESTUDIO TECNICO	58
3.1 TAMAÑO DEL PROYECTO Y LOS FACTORES INFLUYENTES	58
3.1.1 Descripción del Tamaño del Proyecto	58
3.1.2 Disponibilidad de Equipos	59
3.1.3 Tamaño del proyecto y recurso humano	60
3.1.4 Tamaño del proyecto y Proveedores	61
3.1.5 Tamaño del proyecto y la localización	62
3.1.6 Tamaño del proyecto y el financiamiento	63
3.2 CAPACIDAD DEL PROYECTO	63
3.3 LOCALIZACION	63
3.3.1 Macro Localización.	63
3.2.2 Micro Localización	63
3.4 DIAGRAMA ORGANIZACIONAL	64
3.5 ESTUDIO LEGAL	64
3.5.1 La Ley 1273 de 2009 [2].	64
3.5.2 Ley 1266 de 2008, Ley HABEAS DATA	67
4. ANALISIS FINANCIERO	70
4.1 DATOS INICIALES.	70
4.2 CALCULO DE LOS COSTOS UNITARIOS DE LOS PRODUCTOS.	70
4.3 COSTOS ADMINISTRATIVOS	71
4.3.1 Nomina.	71
4.3.2 Otros Gastos de Administración.	72

4.4 INVERSIONES.	72
4.4.1 Maquinaria y Equipo	72
4.4.2 Muebles y enseres	73
4.5 FUENTES DE FINANCIACIÓN.	74
4.6 DEFINICION DE PRECIOS DE VENTA.	74
4.7 FLUJO DE CAJA	75
4.8 ESTADO DE PÉRDIDAS Y GANANCIAS	79
4.9 BALANCE.	80
4.10 EVALUACIÓN FINANCIERA.	81
CONCLUSIONES	83
BIBLIOGRAFIA	85
ANEXOS	87

## LISTA DE FIGURAS

	<b>Pág.</b>
Figura 1. Ilustración Habilidades requeridas Vs sofisticación Ataque	17
Figura 2 Logo de Empresa	49
Figura 3. Proceso Comercialización	54
Figura 4. Plano de la planta	62
Figura 5. Organigrama	64

## LISTA DE ANEXOS

	<b>Pág.</b>
ANEXO 1. Tabulación datos del estudio de mercados	87

## RESUMEN

**TITULO:** PREFACTIBILIDAD PARA LA CREACION DE UNA EMPRESA EN SEGURIDAD DE LA INFORMACION PARA EL ORIENTE COLOMBIANO\*

**AUTORES:** ANA MILENA SUAREZ RODRIGUEZ  
JESUS GUALDRON FLOREZ  
OSCAR LEONARDO GIL MARIÑO\*\*

**PALABRAS CLAVES:** Seguridad Informática, protección de la información, Pruebas de Vulnerabilidad, seguridad perimetral, auditoría en sistemas de información.

### DESCRIPCION

Hoy en día, en todas las empresas se está desarrollando una evolución cambiante tanto en el manejo de la información como en la forma de proteger la misma, conceptos como computación en la nube entre otros conlleva a replantearse las estrategias en la aplicación de seguridad de la información ya que así como se hace más fácil el acceso a dicha información, también existen nuevas amenazas en su protección, almacenamiento y difusión que causa una exposición vulnerable para cualquier agente externo que quiera acceder sin ningún tipo de restricción.

En todas las compañías la información se convierte en uno de los activos más importantes de la misma, por lo tanto es fundamental garantizar los tres aspectos esenciales que conllevan al aseguramiento de la información como lo son la disponibilidad, accesibilidad e integridad de los datos. Para esto debemos generar estrategias efectivas y planes de acción adecuados para poder establecer elementos necesarios y de esta forma crear una cultura en seguridad de la información.

Dicha información debe ser protegida desde la creación de documentos oficiales que rijan las políticas de seguridad y cultura informática, el cumplimiento de todas las medidas aplicadas dentro de la organización y la protección tanto en el sitio de almacenamiento como en las redes de transmisión de datos y telecomunicaciones, controles de autenticación y acceso entre otros. Estos controles pueden aplicarse a todo nivel salvaguardando el activo vital en las empresas.

Una adecuada Gestión de la seguridad de la información debe ser integral, ya que no corresponde exclusivamente a los expertos en este tema establecer los protocolos de seguridad, debido a que es un proceso de todos los miembros de una organización quienes son parte fundamental en el diseño de políticas de seguridad, correctamente alineados con las necesidades del negocio.

---

\* Monografía de Grado.

\*\* Escuela de Estudios Industriales y Empresariales. Posgrado en evaluación y gerencia de proyectos.  
Director: Sandra Milena Mercado

## SUMMARY

**TITLE:** FEASIBILITY FOR THE CREATION OF A INFORMATION SECURITY COMPANY FOR THE EAST OF COLOMBIA\*

**AUTHORS:** ANA MILENA SUAREZ RODRIGUEZ  
JESUS GUALDRON FLOREZ  
OSCAR LEONARDO GIL MARIÑO \*\*

**KEY WORDS:** Computer security, data protection, Vulnerability Tests, perimeter security, information systems audit.

### DESCRIPTION

Today, all companies are developing a changing environment both in the handling of information as to how to protect it, concepts like cloud computing and others leads to rethink the strategies involved in implementing of information security, as well as makes it easier to access this information, there are new threats in their protection, storage and dissemination, exposure that causes vulnerable to any external agent who wants to access without any restriction

In most companies, the information becomes one of the most important assets; therefore it is essential to ensure the three key aspects that lead to information assurance such as availability, accessibility and integrity of data. For this, the companies must create effective strategies and appropriate action plans in order to establish necessary elements and thus create a culture in information security.

This information should be protected since the creation of official documents leading security policies and computer literacy, compliance with all the measures implemented within the organization and protection on-site warehouse as in data transmission networks and telecommunications, authentication and access controls among others. These controls can be applied at all levels while safeguarding vital assets in companies.

Proper management of information security must be comprehensive, if not solely for the experts in the field to establish security protocols, because it is a process of all members of an organization who are fundamental in the design of security policies, properly aligned with business needs.

---

\* Grade Monograph.

\*\* School of Industrial and Business Studies. Evaluation and Project management. Director: Sandra Milena Mercado

## INTRODUCCION

Los avances tecnológicos han traído inmensos beneficios a la humanidad pero también una serie de nuevos retos que exigen respuestas rápidas y oportunas. Uno de estos retos tiene que ver con uno de los activos más importantes de las personas y empresas, su información.

A lo largo de este documento hablaremos de seguridad informática y por tal razón es importante entender su concepto como: ***La seguridad informática es un proceso continuo donde se planifica, se hace, se verifica, se actúa y se realizan mejoras continuas a través de la realimentación del sistema, teniendo en cuenta sus principales componentes como son los equipos tecnológicos (hardware y software) junto con el personal de una organización, para obtener el mejor desempeño de los recursos informáticos.***

Por otra parte los incidentes informáticos hacia las infraestructuras empresariales y personales también han venido en aumento debido a la gran cantidad de herramientas disponibles en Internet y a su facilidad de uso; permitiéndoles a personas que no posea conocimientos avanzados en informática realizar algunos ataques que con suerte podrían llegar a materializarse. A continuación se muestra una gráfica que muestra como ha venido evolucionando los ataques a los sistemas de información con respecto al nivel de conocimiento que se debe tener.

Figura 1. Ilustración Habilidades requeridas Vs sofisticación Ataque



Fuente: Introducción a las técnicas de ataque e investigación forense, un enfoque pragmático – GLOBALTEKSECURITY

Debido a los incidentes materializados las empresas decidieron adquirir herramientas tipo hardware y software para tratar de mitigar el riesgo y disminuir la inseguridad de la información, dejando a un lado la adecuada administración, el debido control de procesos, la capacitación, educación y concientización de los empleados; en conclusión no crearon una cultura de seguridad informática que permita disminuir o mitigar los riesgos.

Finalmente nos resta por decir que con las legislaciones vigentes y las que están en curso, los tratados de libre comercio, la estandarización mundial; han creado una oportunidad de negocio y es por esto que los autores consideraron realizar el estudio a nivel de pre-factibilidad para la creación de una empresa que aproveche el mercado de la seguridad de la información; este estudio está siguiendo un formato que exige un concurso de emprendimiento al cual será presentado.

## 1. ANTECEDENTES E HISTORIA DEL PROYECTO

- **Hackers atacaron la página web de la Presidencia**

(...) Cinco minutos después de que el ministro de Defensa, Rodrigo Rivera, anunciara que ya habían identificado a los 'hackers' que atacaron sitios web oficiales en *Colombia*, el grupo Anonymous provocó (...)

**Fuente:** Viernes 15 de abril de 2011 | eltiempo.com | Justicia | Autor: REDACCIÓN JUSTICIA

- **Capturan a seis 'hackers' que defraudaban bancos**

(...) La Policía de Bogotá capturó ayer a seis hombres que se conectaban ilegalmente a redes informáticas de bancos en España, Argentina y *Colombia* para robar las cuentas bancarias. HERJOS (...)

**Fuente:** Viernes 8 de enero de 2010 | eltiempo.com | Bogotá | Autor: NULLVALUE

- **Piratas informáticos iban a robar \$ 17.650 millones de las gobernaciones de Cauca y Meta**

(...) lo que estaba ocurriendo y lograron frenar las transacciones. No es la primera vez que entidades oficiales son blanco de robos virtuales a través de 'hackers'. La semana pasada, el CTI capturó a 16 personas vinculadas (...)

**Fuente:** Domingo 17 de mayo de 2009 | eltiempo.com | Justicia

- **11/05 El Banco Popular revela que fueron "hackers" los que clonaron las cuentas de los ahorradores en Valledupar**

- **27/07 \$1.845 millones de la Alcaldía de Cali, por impuesto de rodamiento automotor, fueron sustraídos a través de cuentas.**

**Fuente:** <http://www.elpais.com.co/paionline/notas/Noviembre272007/robos.html>

- **27/11/07 Mediante fraude electrónico fueron sustraídos \$1.400 millones que se iban a girar a los hospitales. Los dineros son de la Gobernación del Valle.**

- **29/11/07 Ladrones informáticos le robaron 892 millones de pesos a “hospital Centro Oriente” en Bogota\_**

**Fuente:** [http://www.eltiempo.com/bogota/2007-11-30/ARTICULO-WEB-NOTA\\_INTERIOR-3838706.html](http://www.eltiempo.com/bogota/2007-11-30/ARTICULO-WEB-NOTA_INTERIOR-3838706.html)

Los anteriores titulares día a día vienen en aumento, por tal razón y observando una oportunidad de negocio en un campo reciente y por explorar en Colombia, los autores se motivaron a realizar un estudio para evaluar a nivel de prefactibilidad la creación una empresa dedicada a la disminución de la inseguridad de la información. A partir de ese momento se iniciaron reuniones de trabajo para establecer un portafolio de servicios y productos.

El tema de la seguridad Informática ha venido ganando importancia, tanto por el volumen de incidentes que se presentan y que han llegado incluso a acabar con compañías, como por legislaciones nacientes que buscan que la Protección de la Información sea una obligación. Bajo este modelo, el Oriente Colombiano adolece de empresas especializadas en este tema, y las empresas que inician el camino de asegurar su información se ven abocadas a incurrir en importantes sobrecostos por la necesidad de traer desde Bogotá o Medellín expertos que asesoren sus proyectos.

La necesidad de una empresa especializada en el tema de seguridad informática se evidencio luego de realizar una encuesta a nivel local en un estudio de oportunidad donde se preguntó que si creía necesaria la creación de una empresa especializada en seguridad informática para la región Oriente y ¿Por qué?

El 100% de los encuestados respondió que SI, y se muestran algunas de las justificaciones que dieron los encuestados:

**“El tema de seguridad informática para nuestra empresa se maneja con políticas y auditorias que lleva a cabo el grupo ubicado en Bogotá”**

...Profesional Sistemas Instituto colombiano de petroleros ICP

**“Que pueda cubrir las necesidades de una forma inmediata que la Fundación Cardio vascular demande en seguridad informática”**

.....Profesional Sistemas Fundación Cardio-Vascular

**“Porque todo lo que se requiere hay que hacerlo por Bogotá o Medellín incurriendo en altos costos”**

.....Gerente Sistemas Coopprofesores

Bajo estas necesidades se plantea el proyecto de la creación de una empresa de seguridad informática para el oriente Colombiano con base en Bucaramanga, que busca en lo económico: Preservar y proteger el activo más importante de la Empresa de hoy, la Información; a través de soluciones a la medida de las necesidades de las empresas con buen servicio técnico y soporte en la región. En el plano Regional: Aportar en la construcción de un clúster de Tecnología para Santander y en lo Social: Generar confianza en la Sociedad por la confiabilidad del manejo adecuado de su información personal o empresarial.

## 2. ESTUDIO DE MERCADOS

### 2.1 OBJETIVOS

**2.1.1 Objetivo General.** Realizar un estudio que permita determinar aspectos como precios, competencia, potencial de clientes y todas las variables de mercado a considerar para la creación de una empresa que brinde servicios de Seguridad Informática en el oriente y oriente colombiano.

### 2.1.2 Objetivos Específicos

\*\* Determinar usos y especificaciones de los servicio a ofrecer.

\*\*Analizar el mercado potencial y objetivo existente en oriente colombiano para la comercialización de productos y servicios de seguridad de la información.

\*\*Hacer un análisis de la oferta y la demanda a través del estudio de mercado.

\*\* Diseñar canales de comercialización apropiados para el tipo de producto y para el tipo de cliente propios de un servicio de Seguridad Informática.

\*\*Hacer un análisis de oferta, demanda, precios existentes en el mercado y diseñar las estrategias de fijación de los mismos.

\*\*Plantear las estrategias de publicidad y promoción necesarias para el posicionamiento adecuado de la empresa dentro del mercado local.

## **2.2 MERCADO POTENCIAL Y OBJETIVO**

**2.2.1 Mercado Potencial.** El mercado potencial son todas las empresas que cuenten con sitio virtual (ciberespacio), que cuenten con Sistemas de misión crítica en los que el manejo de información sea vital para cumplir con su objeto social. Inicialmente para el servicio directo y contar con atención personalizada, circunscribiremos el marco geográfico al Nororiente Colombiano (Santander, Norte de Santander, Cesar), pero para efectos del presente estudio y como punto de partida de nuestra empresa nos centraremos en la ciudad de Bucaramanga; también incluiremos empresas que maneje su información, la de sus clientes, proveedores, etc.. Mediante tecnologías de información. Inicialmente el nicho de mercado se establecerá en empresas que deban cumplir con regulaciones tales como la ley de habeas data, si es una entidad Financiera con SARO y si exporta con las regulaciones vigentes en dichos estados, ejemplo, la ley de Protección de datos de ESPAÑA.

**2.2.2 Mercado Objetivo.** Nuestros posibles clientes son:

- \*\*AMB (Acueducto Metropolitano de Bucaramanga) (servicios)
- \*\*ICP (Instituto Colombiano de Petróleos)
- \*\*Comprofesores (entidad financiera)
- \*\* Comultrasan (Entidad Financiera)
- \*\* Fundación Cardiovascular (salud)
- \*\*Gobernación de Santander (Gobierno)
- \*\* Sistemas Y Computadores (empresa privada)
- \*\* Policía Nacional (gobierno)
- \*\* ESSA –Electrificadora Santander (Servicios)
- \*\* CDMB (Corporación para la defensa de la meseta de Bucaramanga)
- \*\* Banco de Crédito Paris E.U (empresa Privada)

- \*\* Copetrán (transporte)
- \*\* Universidad Industrial de Santander
- \*\* Universidad Manuela Beltrán
- \*\* Universidad Santo Tomas
- \*\* Clínica Ardila Lule
- \*\* Hospital Universitario de Santander
- \*\* Alcaldías Municipales.
- \*\* Colegios
- \*\* EPS, ARS,
- \*\* Fondos de Pensión
- \*\* Telebucaramanga
- \*\* Piedecuestana de Servicios.
- \*\* Itacol
- \*\* Empresas Avícolas (distraves, incubadora Santander, incubadora andina)
- \*\* Ganados Asociados
- \*\* Berlinas del Fonce
- \*\* Telebucaramnanga.

## **2.3 RECOPIACION DE INFORMACION DE DEMANDA Y COMPETENCIA**

Se establece como metodología para recolección de información apoyarnos en datos secundarios y datos primarios.

**2.3.1 Fuentes Secundarias.** La Información que se recopiló en esta etapa del estudio se obtuvo de datos de revistas especializadas en Seguridad de la información, páginas Web como:

**Revistas:** Hackin 9.- Begins- Diaroti- Linux Magazine-Punto Seguridad.

**Páginas Web:** [www.eltiempo.com](http://www.eltiempo.com), [www.criptored](http://www.criptored), [www.Segurinfo.com](http://www.Segurinfo.com), [www.dragonjar.com](http://www.dragonjar.com).

**2.3.2 Fuentes Primarias.** Como fuente primaria de información se utiliza una encuesta aplicada en una muestra del mercado objetivo, además de las entrevistas sostenidas con los gerentes de TI de las diversas compañías visitadas.

Es de aclarar que este tipo de encuesta se considera dentro de las organizaciones como información confidencial y muchas veces no se obtiene respuesta por parte de las personas objetivo de las encuestas.

### 2.3.2.1 Modelo Encuesta Aplicada

#### ENCUESTA DE SEGURIDAD INFORMATICA

Esta encuesta busca conocer el nivel técnico y administrativo de la seguridad informática en Santander, dicha encuesta toma como referencia algunas preguntas realizadas por la Asociación Colombiana de Ingenieros de Sistemas (**ACIS**) y Computer Crime and Security Survey 2007 (**CSI**).

**Nombre Empresa (opcional):**

\_\_\_\_\_

1. Sector al que pertenece Su empresa

Sector	
Financiera	
Ingeniería	
Educación	
Servicios Publico	
Entidades Del Gobierno	
Transporte	
Manufactura	
Servicios	
Otro ( Cuál? )	

2. Número de empleados de su empresa

No. Empleados	
1-50	
51-100	
101-200	
más de 200	

3. Cargo de quien responde la encuesta

Cargo	
Presidente ó Gerente General	
Director de Área	
Profesional Dpto. Sistemas	
Oficial de Seguridad Informática	
Administrador de Sistemas	
Otro (Cual? )	

4. Presupuesto previsto para seguridad Informática

Inversión en Millones	
No hay inversión	
1-5	
5-15	
15-30	
más de 30	

5. ¿En qué tema se concentra la inversión en seguridad Informática? (Seleccione todos los aplicables)

Temas	
Protección de red	
Protección de datos Critico	
Protección de propiedad intelectual	
Proteger almacenamiento datos clientes	
Concientización\ Formación usuario final	
Comercio\ Negocios Electrónicos	
Desarrollo y afinamiento de Seguridad de las aplicaciones	
Asesores de Seguridad Informática	
Contratación de personal más calificado	
Evaluaciones de Seguridad internas y externas	
Otro (Cual? )	

6. ¿En el último año que tipos de falla de seguridad detectó? (Seleccione todos los aplicables)

<b>Incidente</b>	
Ninguno	
Mala conducta de usuarios	
Fallas de Software y Hardware	
Fraude	
Virus, Troyanos, gusanos	
Monitoreo no autorizado de trafico	
Denegación de servicio	
Pérdida integridad	
Pérdida de información	
Robo de datos	
Robo de hardware	
Penetración al Sistema	
Otro (Cual? )	

7. ¿Qué acciones toma después de un incidente de seguridad?

<b>Acciones</b>	
Procura Identificar el perpetrador	
Instala parches de Seguridad	
Adiciona ó instala software de Seguridad	
Adiciona ó instala hardware de Seguridad	
Cambia las políticas de Seguridad	
Se reporta a las autoridades locales	
Ninguno	
Otros (¿Cuál? )	

8. ¿Cuántas pruebas de seguridad Informática realizan por año, para valorar su estado?

<b>Cantidad de pruebas</b>	
Ninguna	
1	
2-4	
más de 4	

9. ¿Cuáles de los siguientes mecanismo utiliza actualmente su organización para proteger sus sistemas de información? (seleccione todos los aplicables)

Mecanismos	
Biométricos	
Antivirus	
Firewalls software	
Firewalls hardware	
Encriptación de datos	
Contraseñas	
Firmas digitales	
Sistemas Detección Intrusos (IDS)	
Sistemas de Prevención de Intrusos (IPS)	
VPN	
Proxis	
Monitoreo 7x24	
Otros ( Cual? )	

10. Cuantas y cuales empresas de seguridad informática conoce con sede en la región?

Número de Empresas	
--------------------	--

Cuáles?

1-
2-
3-
4-
5-
6-

11. El servicio de asesoría, soporte técnico preventa y postventa es?

Calificación Servicio	
Excelente	
Bueno	
Regular	
Malo	
Deficiente	

12. Considera importante la creación de una empresa de seguridad informática con sede en Santander?

SI	NO

¿Por qué?

13. ¿Qué describe mejor la política de seguridad de su organización?

**No se tiene una política de Seguridad definida	
**Está en etapa de desarrollo	
**Política formal, escrita documentada e informada a todo el personal	

14. ¿En su organización (todo el personal) reconoce la información como un activo más a proteger?

Si	
No	
No Sabe	

15. Cuáles de los siguientes servicios cree usted que su organización podría llegar a necesitar de una empresa de seguridad informática? (escoja todos los aplicables)

Servicios	
Planes de concientización	
Pruebas de hacking (Ethical Hacking)	
Análisis forense	
Diseño de modelos de seguridad	
Planes de contingencia	
Planes de continuidad del negocio	
Auditoria sistemas informáticos	
Aseguramiento de plataforma	
Análisis de riesgos	
Monitoreo dispositivos	
Soporte 7x24	
Manejo de incidentes	
Capacitación en Standares y legislatura	
Otros? (Cuál? )	

**2.3.2.2 Tabulación de los datos.** Para el análisis de la encuesta se debe tener en cuenta que de los 50 correos enviados a las empresas más representativas de Santander solo contestaron 11, pero lo relevante de las encuestas es que las personas que la diligenciaron son de los cargos directivos del área de Tecnologías de la Información (TI). Los datos tabulados se encuentran en el anexo 1 de este documento.

## 2.4 ANALISIS DE LA INFORMACION RECOPIADA

De la Información recopilada en las encuestas, se realizará el análisis de la competencia, la definición de los productos a vender y el análisis con sus posibles sustitutos. Toda esta información se extrajo **del anexo 1** de este documento donde se encuentran tabulados los datos del análisis de mercado.

**2.4.1 Producto y/o Servicios.** A continuación se describirán los servicios que brindara la empresa y sus beneficios para el cliente:

### 2.4.1.1 Pruebas de Vulnerabilidad a Sistemas Informáticos

Características físicas como empaque, cantidad, uso, si es un servicio describa lo que involucra como	Beneficios que le reporta al cliente
<p><b>USO:</b> Este tipo de pruebas se utiliza para determinar el grado de vulnerabilidades que tiene la empresa, como se encuentra actualmente su sistema de seguridad (si lo tiene). En conclusión se obtienen información referente al nivel de exposición que tiene una empresa frente a las amenazas informáticas.</p>	<p>Le permite evidenciar al cliente el grado de riesgo que tiene y le indica que correctivos puede llegar a tomar frente a las vulnerabilidades encontradas.</p>

<p><b>Cantidad:</b> Se sugiere por buenas practicas realizar este tipo de pruebas mínimo 3 veces al año.</p>	<p>Con esta práctica el usuario tendrá un sistema más confiable y menos inseguro, puesto que podrá probar sus sistemas con las amenazas más recientes que van surgiendo en el mercado.</p>
<p><b>Como:</b> Las pruebas de vulnerabilidades se ejecutan a través de la utilización de herramientas especializadas (free y licenciadas) y la experticia de la persona que la hace permitiendo tomar una radiografía del estado actual de su red.</p>	<p>El uso de buenas herramientas y contar con personas expertas, son prendas de garantía de la calidad del trabajo, que estarán reflejados para el cliente en un análisis completo y real de su estado de red.</p>

#### 2.4.1.2 Análisis Forense y recuperación de Datos

<p><b>Características físicas como empaque, cantidad, uso, si es un servicio describa lo que involucra como</b></p>	<p><b>Beneficios que le reporta al cliente</b></p>
<p><b>USO:</b> El servicio forense se usa cuando las entidades han sido vulneradas o han tenido incidentes informáticos (robos, pérdida de información, caídas de sistema, secuestro de máquinas) ya sean provocados por agentes internos o externos.</p>	<p>Un análisis forense trae beneficios para el cliente porque se puede llegar a establecer el cómo, quien (desde que maquina), cuando y donde sucedió el incidente para tratar de ubicar el perpetrador y tomar los correctivos correspondientes, por otra parte en el tema de perdida de información se beneficia puesto que puede llegar a recuperar la información perdida y así evitar perder días de trabajo, información sensible y dinero.</p>

<p><b>Cantidad:</b> El análisis forense se ejecuta a necesidad del cliente.</p>	<p>Las empresas cuando son víctimas de incidentes informáticos deben realizar una investigación para tratar de hallar el responsable y así mitigar el riesgo que significa ser objetivo de un atacante.</p>
<p><b>Como:</b> Los análisis forenses se realizan a través de la utilización de herramientas especializadas (free y licenciadas) y la experticia de la persona aportando información que contribuye con el esclarecimiento de un incidente informático.</p>	<p>El uso de buenas herramientas y contar con personas expertas, son prendas de garantía de la calidad del trabajo, que estarán reflejadas para el cliente en información útil y veraz para la investigación.</p>

#### 2.4.1.3 Administración perimetral de seguridad

<p><b>Características físicas como empaque, cantidad, uso, si es un servicio describa lo que involucra como</b></p>	<p><b>Beneficios que le reporta al cliente</b></p>
<p><b>Uso y Descripción:</b> Las empresas cliente nos posibilitan a administrar de forma remota la seguridad informática; este servicio nos permite realizar la supervisión y toma de correctivos frente a posibles ataques que se puedan tener, administración de equipos, manejo de incidentes, configuración de equipos, todos los procedimientos se realizaran con el visto bueno de la gerencia de la empresa cliente.</p>	<p>Los clientes podrán dedicarse al objeto de su negocio completamente, y no estar solucionando el día a día de la seguridad informática, además reducen costos de inversión en seguridad. Otro beneficio que trae este servicio es que se le entregara al cliente un reporte sobre el comportamiento de la red donde se podrá evidenciar si su red está siendo objetivo de ataques.</p>

<p><b>Cantidad:</b> El servicio que prestaremos será mínimo a un año debido al grado de inversión inicial que se debe hacer; este tiempo también nos va a permitir poder tener un registro que nos facilitara la tarea de auditar el sistema y realimentarlo para que sea un proceso de mejoramiento continuo.</p>	<p>La contratación a 1 año, le permitirá a nuestros clientes establecer un lazo de confianza con nosotros, además el proceso de implantación de seguridad no solo está en la instalación de equipos sino en su buena administración.</p>
<p><b>Como:</b> El servicio de administración perimetral de seguridad se prestara remotamente, accediendo a los equipos a través de un canal de Internet que nosotros proveeremos, pero si en alguna situación especial es necesaria nuestra presencia en planta hasta allí nos desplazaremos.</p> <p>Dentro de este producto se encuentran diferente tipos de administración que el cliente podar llegar a escoger de acuerdo a sus necesidades, como por ejemplo administración y soporte 7X24X365, soporte y administración durante x horas mensuales, etc.; también el cliente tiene la posibilidad de adquirir los equipos o de tomarlo en alquiler</p>	<p>Nuestros clientes se evitarían todo lo relacionado con la administración de la seguridad, manejo de incidente, soporte, monitoreo, manejo de nuevas vulnerabilidades, configuración de equipos. Capacitación de personal en el manejo de equipos. Etc.</p>

#### 2.4.1.4 Auditoría de Sistemas

<b>Características físicas como empaque, cantidad, uso, si es un servicio describa lo que involucra como</b>	<b>Beneficios que le reporta al cliente</b>
<p><b>USO:</b> La auditorías se usan para evaluar y revisar los controles y procedimientos de los sistemas informáticos, además se revisa la utilización, eficiencia y seguridad de los equipos de computo</p>	<p>Las empresas podrán en primera instancia verificar el uso que se le está dando a sus servicios informáticos, por otra parte podrán revisar y tener a mano información confiable y segura que les permita la toma de mejores decisiones.</p>
<p><b>Cantidad:</b> La auditoría la realizamos a solicitud del cliente, aunque las buenas prácticas recomiendan que de acuerdo al tamaño de la empresa se realicen cierto número de auditorías en un periodo de tiempo determinado.</p>	<p>Los clientes son libres de determinar la necesidad de una auditoria, aunque nosotros como empresa debemos concientizar a nuestros clientes que esto es necesario por el bienestar de la compañía.</p>
<p><b>Como:</b> Uno de nuestros Ingenieros se desplaza hasta la empresa e inicia sus labores de auditoria.</p>	<p>El auditor estará en contacto directo con su zona de trabajo y podrá tener más claridad sobre los eventos que allí sucedan, generando un informe con información veraz que le sirva a la empresa en la toma decisiones.</p>

### 2.4.1.5 Hardening (Aseguramiento) e instalación de plataformas no propietarias)

<b>Características físicas como empaque, cantidad, uso, si es un servicio describa lo que involucra como</b>	<b>Beneficios que le reporta al cliente</b>
<p><b>USO:</b> Este servicio lo requieren las empresas cuando compran equipos informáticos al momento de instalarlos no cuentan con un buen soporte local o sus empleados no cuentan con la experticia necesaria para realizar una buena configuración.</p>	<p>El cliente podrá tener sus equipos trabajado de una forma óptima, aprovechando las verdaderas potencialidades que traen los equipos, además una buena configuración evita una cadena de problemas e incidentes.</p>
<p><b>Cantidad:</b> Cuando el cliente lo requiera</p>	<p>Nuestros clientes encontraran en nosotros un servicio con respaldo, servicio técnico, ágil y responsable.</p>
<p><b>Como:</b> Nuestra empresa cuenta con personal capacitado y con experiencia en múltiples herramientas informáticas, que se pueden desplazar a las instalaciones de la planta para realizar la buena configuración de los equipos del cliente.</p>	<p>Nuestros clientes tendrán la seguridad que los procedimientos utilizados en la labor contratada son de alta calidad y manejando siempre las buenas practicas; todo esto no lo garantiza el trabajar con personal capacitado y experimentado en el campo.</p>

**2.4.1.6 Capacitación en Sistemas de Información y Seguridad Informática  
(grupo mínimo de 10 personas, 1 día)**

<p><b>Características físicas como empaque, cantidad, uso, si es un servicio describa lo que involucra como</b></p>	<p><b>Beneficios que le reporta al cliente</b></p>
<p><b>USO:</b> Capacitar personal en las diferentes áreas de la seguridad informática y los servicios de información.</p>	<p>Contar con personal capacitado genera un mejor desempeño laboral del empleado, además genera buen ambiente de trabajo puesto que el empleado ve que la empresa se preocupa por su superación profesional; por otra parte un empleado capacitado y concientizado es un foco de generación de cultura en el buen uso de las plataformas informáticas.</p>
<p><b>Como:</b> Se promocionara los cursos y se dictaran en salones adecuados tanto físicamente como técnicamente para cumplir con los requisitos del curso y la expectativa de los clientes.</p>	<p>La buena planificación en un curso, con la adecuada motivación de los asistentes son la combinación de una capacitación exitosa, eso encontraran nuestros clientes en nuestras capacitaciones.</p>

**2.5 COMPETENCIA, NUESTROS SERVICIOS Y SUS SUSTITUTOS**

**2.5.1 Competidores.** La necesidad de servicios especializados en el área de seguridad informática con presencia en la región, género que empresas de dicadas a la comercialización de equipos informáticos, migraran a comercializar equipos de seguridad informática.

Los equipos hacen parte de todo el proceso que significa implementar seguridad informática en las organizaciones, como lo son políticas de seguridad, manejo de

incidentes, concientización de empleados, monitoreo, administración de equipos, escaneo de vulnerabilidades, administración del riesgo, etc.

Nuestra empresa NITERIX, es una empresa que brindara el acompañamiento a las organizaciones en todos los aspectos relacionados en seguridad informática, para hacer de este un proceso integral y que realmente contribuya al crecimiento de las empresas.

A continuación citamos a las empresas halladas en nuestra investigación de la competencia.

**\*\*COINSA Ltda.**

Dirección: Calle 16 No. 31<sup>a</sup>-26, Tel./Fax.: 6456029-6456831-6328406

Ciudad: Bucaramanga – Colombia

Esta empresa en el área de seguridad informática está dedicada a la venta de equipos como lo es el Firewall FORTINET de Fortigate, la solución de ellos está alrededor de 7'000.000 el equipo, sin administración y tienen un bajo soporte técnico en la medida puesto que si la persona que conoce el equipo no está en la ciudad el cliente debe esperar.

**\*\*SIC “Seguridad Informatica Colombiana”**

Dirección: Cra. 26 No. 40-23 CC. Poblado Plaza Local 103, telf: 6900106-6464574

Girón, Colombia

Empresa dedicada a la venta de equipos como firewalls, antivirus y dispositivos biométricos como cámaras, reconocimiento de huella, cableado estructurado.

**\*\*STS “Sistemas Teleinformáticas y Servicios”**

Calle 37- 17 -46 Oficina 304, Bucaramanga

Telfax : 6337775 - Móvil 314 473 3374

Esta Empresa ofrece los siguientes Servicios:

- Servicios de Consultoría en Control y Seguridad Informática
- Servicios de Auditoria Informática
- Capacitación

**2.5.2 Nuestros servicios y sus Sustitutos.** Productos sustitutos: Nuestra empresa no tiene como objetivo la compra-venta de productos de seguridad informática, el objetivo de nuestra empresa es dar soluciones a nuestros clientes de acuerdo a las necesidades de ellos, acompañándolos en todo el proceso que esto lleve, además promovemos el concepto de administración de seguridad externa, que según lo evidenciado en el estudio de mercados no se suministra en la región.

## 2.6 PRECIO

**2.6.1 Análisis de precios de mercado.** En la tabla que se muestra a continuación se presenta los precios que se encuentran en el mercado de algunos servicios que Niterix Brindara:

Producto	Competencia	
	Nombre de la primera competencia y precio	Nombre de la segunda competencia y precio
Pruebas de Vulnerabilidad	E TEK (Bogotá) 200.000 / hora	Digiware (Bogotá) 250.000/hora
Análisis forense y recuperación de datos	Profesional (Bogotá) 300.000 /hora	UPB (Bucaramanga) 150.000/ hora
Administración de Seguridad Perimetral	-----	-----
Auditoria de Sistemas	ISL INGENIEROS DE SISTEMAS LTDA. (Bucaramanga)	-----

	85.000 /hora	
Hardeninig a plataformas no propietarias	Bitcom (Bucaramanga) 70.000 / hora	-----
Capacitación en Sistemas de información y Seguridad Informática (1 día con mínimo de 10 personas)	STS (Bucaramanga) 200.000	-----

**2.6.2 Estrategia para Fijar Precios.** Inicialmente y como estrategia de penetración nuestros precios estarán por debajo de la competencia (de otras zonas) puesto que contamos con la ventaja de hacer presencia física en la región Nororiental lo cual disminuirá a los clientes los sobrecostos por traslado de consultores desde Bogotá o Medellín, ciudades que según el estudio de las fuentes primaria se deben desplazar los consultores.

Por otra parte tendremos en cuenta aspectos como:

\*\*Necesidad del cliente

\*\*Costo de inversión y producción

\*\*Tiempo de área comercial y técnica.

\*\*Precios del mercado

\*\*Tipo de soporte.

### 2.6.2.1 Análisis de Precios Unitarios Por Producto (APU)

- Pruebas de Vulnerabilidad

Unidad de costo: Valor por hora

PRODUCTO	MATERIA PRIMA INSUMO	UNIDAD DE MEDIDA	COSTO UNITARIO DE LA UNIDAD DE MEDIDA	UNIDADES A USAR	COSTO TOTAL	COSTO UNITARIO UNIDAD PRODUCIDA
<b>PRUEBAS DE VULNERABILIDAD</b>					REVICE	\$ 27.500
	Computador	hora cómputo	5.000	1	5.000,0	
	Sistema Operativo	hora proceso	2.500	1	2.500,0	
	Software Nessus	hora proceso	2.500	1	2.500,0	
	Scanner de Puertos	hora proceso	2.500	1	2.500,0	
	Otras herramientas SW	hora proceso	2.500	1	2.500,0	
	Insumos	consumibles	2.500	1	2.500,0	
	Experto para Informes	hora hombre	10.000	1	10.000,0	

**Análisis Forense y recuperación de datos**

Unidad de costo: Valor por hora

PRODUCTO	MATERIA PRIMA INSUMO	UNIDAD DE MEDIDA	COSTO UNITARIO DE LA UNIDAD DE MEDIDA	UNIDADES A USAR	COSTO TOTAL	COSTO UNITARIO UNIDAD PRODUCIDA
<b>Análisis Forense y Recuperación de datos</b>					REVICE	\$ 23.000
					REVICE	
	Computador	hora cómputo	5.000	1	5.000,0	
	Sistema Operativo	hora proceso	2.500	1	2.500,0	
	Software FTK	hora proceso	5.000	1	5.000,0	
	Software X-Way	hora proceso	2.500	1	2.500,0	
	Otras herramientas	hora proceso	2.500	1	2.500,0	
	Insumos	consumibles	2.500	1	2.500,0	
	Ultrakit	Hora proceso	3.000	1	3.000,0	

- **Administración perimetral de seguridad Nivel GOLD. (Pequeñas y medianas empresas).**

Unidad de costo: alquiler mensual

PRODUCTO	MATERIA PRIMA INSUMO	UNIDAD DE MEDIDA	COSTO UNITARIO DE LA UNIDAD DE MEDIDA	UNIDADES A USAR	COSTO TOTAL	COSTO UNITARIO UNIDAD PRODUCIDA
<b>Administración perimetral de seguridad Nivel GOLD. (pequeñas y medianas empresa), implementación con equipos de marca propia, CICO-SIS</b>					REVICE	\$ 190.000
	Software de Monitoreo	alquiler mensual	10.000	1	10.000,0	
	Apliance CICO-SIS (Firewall, IPS, IDS Antispam, control ancho banda, logs, filtro contenido, VPN, Proxis, control trafico)	alquiler mensual	65.000	1	65.000,0	
	Computador	alquiler mensual	20.000	1	20.000,0	
	Antivirus	mensualidad	40.000	1	40.000,0	
	2 informes mensuales	mensualidad	55.000	1	55.000,0	

- **Administración perimetral de seguridad Nivel Silver. (Pequeñas y medianas empresas).**

Unidad de costo: alquiler mensual

PRODUCTO	MATERIA PRIMA INSUMO	UNIDAD DE MEDIDA	COSTO UNITARIO DE LA UNIDAD DE MEDIDA	UNIDADES A USAR	COSTO TOTAL	COSTO UNITARIO UNIDAD PRODUCIDA
<b>Administración perimetral de seguridad SILVER . (pequeñas y medianas empresa), implementación con equipos de marca propia, SICO-SIS</b>					REVICE	\$ 120.000
	Software de Monitoreo	alquiler mensual	10.000	1	10.000,0	
	Apliance CICO-SIS (Firewall, IPS, IDS Antispam, control ancho banda, logs, filtro contenido, VPN, Proxis, control trafico)	alquiler mensual	60.000	1	60.000,0	
	Computador	alquiler mensual	20.000	1	20.000,0	
	Antivirus FREE	mensualidad	-	1	0	
	1 informe mensual	mensual	30.000	1	30.000,0	

- **Administración perimetral de seguridad Nivel PLATINIUM. (Pequeñas y medianas empresas).**

Unidad de costo: alquiler mensual

PRODUCTO	MATERIA PRIMA INSUMO	UNIDAD DE MEDIDA	COSTO UNITARIO DE LA UNIDAD DE MEDIDA	UNIDADES A USAR	COSTO TOTAL	COSTO UNITARIO UNIDAD PRODUCIDA
<b>Administración perimetral de seguridad Nivel PLATINIUM. (pequeñas y medianas empresa), implementación con equipos de marca propia, SICO-SIS soporte 7x24</b>					REVICE	\$ 1.135.000
	Software de Monitoreo	alquiler mensual	10.000	1	10.000,0	
	Apliance CICO-SIS (Firewall, IPS, IDS Antispam, control ancho banda, logs, filtro contenido, VPN, Proxis, control trafico)	alquiler mensual	65.000	1	65.000,0	
	Computador	alquiler mensual	20.000	1	20.000,0	
	Antivirus	mensualidad	40.000	1	40.000,0	
	Soporte 7X24	mensualidad	1.000.000	1	1.000.000,0	

- **Administración de Seguridad Perimetral (Mediana empresa) Soporte7x24 y equipos comprado a proveedores internacionales**

Unidad de costo: alquiler mensual

PRODUCTO	MATERIA PRIMA INSUMO	UNIDAD DE MEDIDA	COSTO UNITARIO DE LA UNIDAD DE MEDIDA	UNIDADES A USAR	COSTO TOTAL	COSTO UNITARIO UNIDAD PRODUCIDA
<b>Administración de Seguridad Perimetral (Mediana empresa) Soporte7x24 y equipos comprado a proveedores internacionales</b>	IDS/IPS (HW)	alquiler mensual	50.000	1	50.000,0	1'300.000,00
	Firewall	alquiler mensual	50.000	1	50.000,0	
	Software de Monitoreo	alquiler mensual	40.000	1	40.000,0	
	Otras herramientas	alquiler mensual	40.000	1	40.000,0	
	Insumos	consumibles mes	30.000	1	30.000,0	
	Asesor Técnico Comercial	honorario mensual	20.000	1	20.000,0	
	Computador	alquiler mensual	50.000	1	50.000,0	
	informe	mensual	20.000	1	20.000,0	
	Soporte 7X24	valor mensual	1.000.000	1	1.000.000,0	

- Auditoría de Sistemas

Unidad de costo: Valor Hora

PRODUCTO	MATERIA PRIMA INSUMO	UNIDAD DE MEDIDA	COSTO UNITARIO DE LA UNIDAD DE MEDIDA	UNIDADES A USAR	COSTO TOTAL	COSTO UNITARIO UNIDAD PRODUCIDA
Auditoría de Sistemas (por horas)					REVICE	\$ 12.500
	Computador	hora cómputo	5.000	1	5.000,0	
	Sistema Operativo	hora proceso	2.500	1	2.500,0	
	Insumos	consumibles	2.500	1	2.500,0	
	Software Ofimático	hora proceso	2.500	1	2.500,0	

- **Hardening (Aseguramiento) e instalación de plataformas no propietarias**

Unidad de costo: Valor Hora

PRODUCTO	MATERIA PRIMA INSUMO	UNIDAD DE MEDIDA	COSTO UNITARIO DE LA UNIDAD DE MEDIDA	UNIDADES A USAR	COSTO TOTAL	COSTO UNITARIO UNIDAD PRODUCIDA
<b>Hardening(Aseguramiento) e instalación de plataformas no propietarias</b>					REVICE	\$ 8.000
	Equipo computo	Alquiler por hora	3.000	1	3.000,0	
	Sistema Operativo	hora proceso	2.500	1	2.500,0	
	Insumos	consumibles	2.500	1	2.500,0	
					REVICE	

- **Capacitación en Sistemas de Información y Seguridad Informática (grupo mínimo de 10 personas, 1 día)**

Unidad de costo: capacitación por persona por día

PRODUCTO	MATERIA PRIMA INSUMO	UNIDAD DE MEDIDA	COSTO UNITARIO DE LA UNIDAD DE MEDIDA	UNIDADES A USAR	COSTO TOTAL	COSTO UNITARIO UNIDAD PRODUCIDA
<b>Capacitación en Sistemas de Información y Seguridad Informática (grupo mínimo de 10 personas, 1 día )</b>					REVICE	\$ 38.000
	Material de trabajo	consumibles	8.000	1	8.000,0	
	Equipo de trabajo	alquiler por capacitación	10.000	1	10.000,0	
	Logística, salón + refrigerio	consumibles	20.000	1	20.000,0	

**2.6.2.2 Precios de venta:** Para obtener el precio de venta fueron calculados teniendo en cuenta el precio mínimo de venta, es decir el punto de equilibrio y sumando un porcentaje de ganancia, (para ver detalles del cálculo de los precios, mirar capítulo 4-Análisis Financiero)

- **Precios NITERIX**

<b>PRODUCTO</b>	<b>PRECIO AL PUBLICO</b>
PRUEBAS DE VULNERABILIDAD	57.627
Análisis Forense y Recuperación de datos	63.027
Administración perimetral de seguridad Nivel GOLD. (pequeñas y medianas empresa), implementación con equipos de marca propia, CICO-SIS	398.151
Administración perimetral de seguridad SILVER. (pequeñas y medianas empresa), implementación con equipos de marca propia, SICO-SIS	251.464
Administración perimetral de seguridad Nivel PLATINUM. (pequeñas y medianas empresa), implementación con equipos de marca propia, SICO-SIS	2.378.428
Administración de Seguridad Perimetral (Mediana empresa) Soporte7x24 y equipos comprado a proveedores internacionales	2.724.191
Auditoría de Sistemas (por horas)	36.269
Hardening (Aseguramiento) e instalación de plataformas no propietarias	24.502
Capacitación en Sistemas de Información y Seguridad Informática (grupo mínimo de 10 personas, 1 día )	79.630

- **Precios Competencia**

<b>Producto</b>	<b>Precio unitario</b>
Pruebas de Vulnerabilidad	150.000 / hora
Análisis forense y recuperación de datos	170.000 / hora
Administración de Seguridad Perimetral	Es un producto que no se ofrece en la región
Auditoria de Sistemas	80.000 / hora
Hardening a plataformas no propietarias	65.000/hora
Capacitación en Sistemas de información y Seguridad Informática	180.000 día

Del análisis de las anteriores tablas podemos observar que tenemos unos precios competitivos respecto a la competencia, además de ello que estamos en la zona de influencia por tal razón tenemos una ventaja competitiva.

## **2.7 DESCRIPCION DE LA EMPRESA A CREAR**

### **2.7.1 Nombre, Logo, Ubicación**

**NOMBRE:** NITERIX, se propone este nombre que significa “Bajo Control”.

**LOGO:**

**Figura 2 Logo de Empresa**



Fuente: Los Autores

**Ubicación:** Bucaramanga

**2.7.2 Objeto Social De La Empresa.** La empresa tendrá como objeto principal desarrollar por intermedio de sus socios y de sus dependientes o a través de la contratación con terceros actividades relacionadas con:

1.- El estudio, diseño, implementación, certificación, administración y acompañamiento de soluciones relacionadas con la seguridad informática 2.- La prestación de servicios de asesoría, capacitación e implementación de proyectos relacionados con la aplicación de Leyes, normas y mejores prácticas relacionadas con la administración de riesgos y la seguridad informática. 3.- La administración de áreas de tecnología informática y de comunicaciones. 4.- La administración de riesgos. 5.- **La prestación de servicios relacionados con la seguridad informática en la modalidad de outsourcing.** 6.- Realizar obras civiles necesarias para cumplir con el objeto social de la Empresa. 7.- La celebración de cualquier tipo de operación comercial con personas naturales o jurídicas, privadas o públicas, a nivel nacional o internacional con la capacidad de distribuir, importar y exportar bienes o servicio relacionados con el objeto social de la Empresa.

### **2.7.3 Misión y Visión de la Empresa**

- **Misión**

Somos el aliado en Seguridad Informática de nuestros clientes, brindando soluciones personalizadas a través de desarrollos tecnológicos que faciliten sus procesos de negocio haciéndolos confiables y Seguros, permitiéndoles mejorar la competitividad al producir impactos técnicos, económicos y comerciales favorables

- **Visión.**

En el año 2017 Niterix será reconocido en el Oriente Colombiano como la mejor alternativa para la Administración outsourcing de la Seguridad Informática y de soluciones en todo lo relacionado con esta área del conocimiento.

## **2.8 PUBLICIDAD, PROMOCION, DISTRIBUCION Y SERVICIO AL CLIENTE**

### **2.8.1 Distribución**

- **Atención directa:** Presencia física en las oficinas de nuestros clientes a través de un agente comercial
- **Atención virtual:** Atención y solución de inconvenientes vía Internet
- **Atención Telefónica:** Helpdesk telefónico.

### **2.8.2 Publicidad**

- Mercadeo Directo
- Participación en eventos de Tecnología
- Organización de eventos especializados para empresas
- Página web
- Medios Impresos (periódicos, catálogos)
- Referencia por parte de los clientes

### **2.8.3 Promoción**

- Concientizando sobre la importancia de la seguridad Informática
- Informando sobre fallas de seguridad que se han presentado en otras empresas

- Presentando un reporte mensual a cada cliente, si adquirió el servicio de monitoreo y administración de la seguridad outsourcing.

#### **2.8.4 Servicio al cliente**

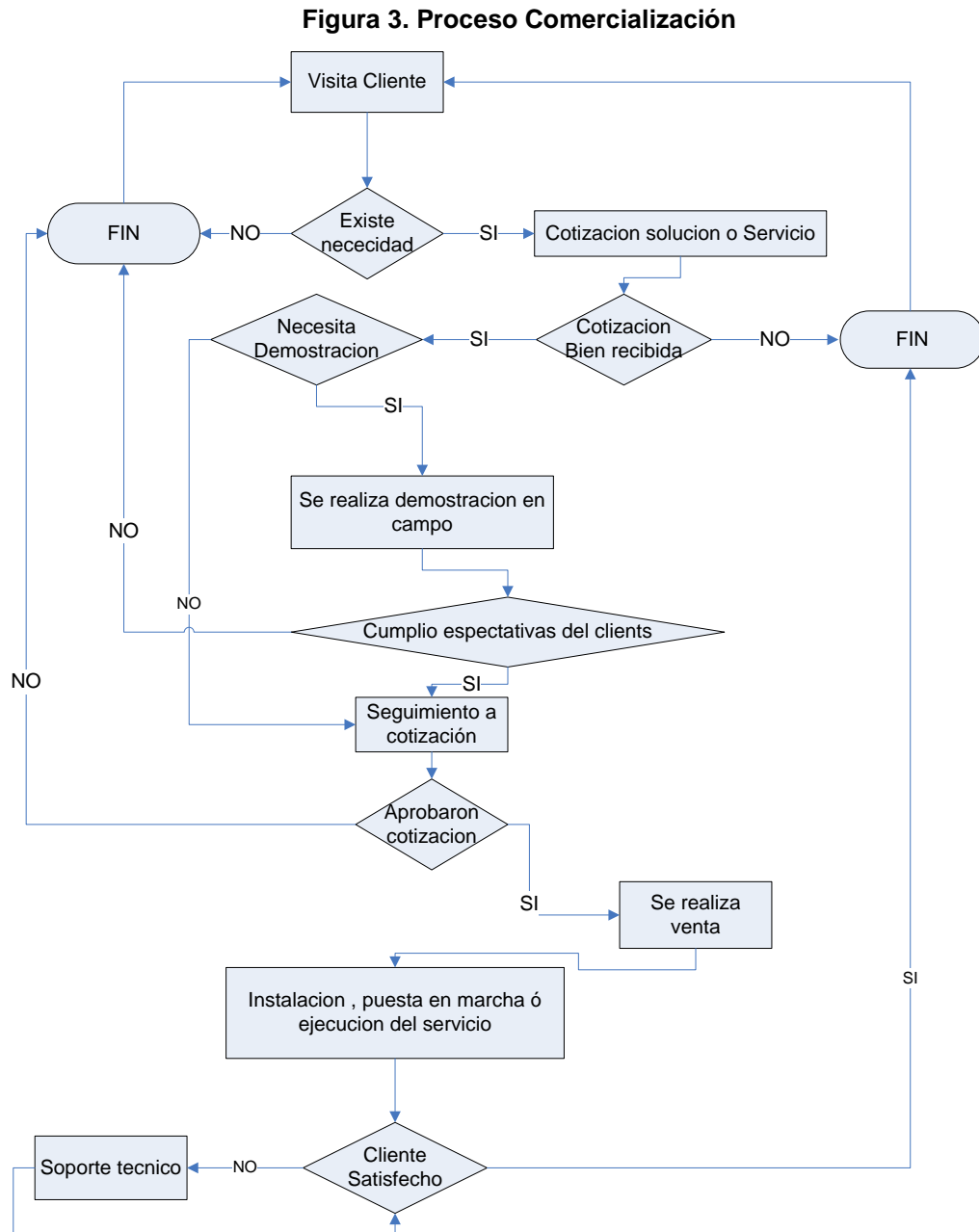
- Desarrollando jornadas de capacitación y entrenamiento al personal, como valor agregado.
- Afinando políticas de seguridad.
- Dar más de lo esperado por el cliente
- Brinda un muy buen servicio y soporte en todas las gamas de nuestros productos.
- Brindando soluciones óptimas para cada cliente, soluciones que satisfagan las necesidad del cliente sin olvidar la calidad de las mismas

## 2.8.5 Presupuesto de costos de comercialización y ventas

Concepto	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12	Total
Producto													
Precio													
Distribución	0	0	0	0	0	0	0	0	0	0	0	0	0
Publicidad y promoción, otras herramientas de comunicación	4.000.000	100.000	100.000	100.000	100.000	1.500.000	100.000	100.000	100.000	100.000	100.000	100.000	6.500.000
Servicio al cliente	200.000	200.000	200.000	200.000	200.000	200.000	200.000	200.000	200.000	200.000	200.000	200.000	2'400.000
<b>Total costos de comercialización y ventas</b>	<b>4.200.000</b>	<b>300.000</b>	<b>300.000</b>	<b>300.000</b>	<b>300.000</b>	<b>1.700.000</b>	<b>300.000</b>	<b>300.000</b>	<b>300.000</b>	<b>300.000</b>	<b>300.000</b>	<b>300.000</b>	<b>8'900.000</b>

## 2.9 PROCESO COMERCIALIZACION

### 2.9.1 Flujo grama de Proceso de Comercialización



Fuente: Los Autores

Den la anterior figura muestra de manera ilustrativa el proceso de comercialización desde la visita al cliente que es nuestro primer paso y acercamiento; hasta lograr la negociación, implementación y soporte post venta.

## 2.10 ANALISIS DOFA

FORTALEZAS (Aspectos a favor)	¿Cómo voy a mantenerlas?
Personal Calificado	Capacitación permanente
Disposición de servicio	Fomentar las habilidades para el servicio al cliente
Precio	Mantener estándares de costos competitivos
Ubicación en la región	Posicionarnos en el mercado para que la competencia no nos afecte.
Servicios nuevos para la región	Estudiar e indagar las nuevas tecnologías que nos permitan estar siempre proponiendo nuevos servicios e innovando.
<b>¡USELAS!</b>	
DEBILIDADES (Problemas presentes)	¿Cómo voy a superarlas?
Dinero para montaje de laboratorio	Destapa Futuro o crédito bancario
Falta de conciencia en las empresas sobre la necesidad de seguridad informática	Capacitación, Información y cumplimiento de legislación
Desconocimiento de nuestra empresa	Publicidad

<b>¡ELIMINELAS!</b>	
<b>OPORTUNIDADES</b> <b>(Aspectos a favor)</b>	<b>¿Cómo voy a mantenerlas?</b>
Creación de legislación sobre protección de información	Darlas a conocer y entregar soluciones acordes
Crecimiento en el nivel de difusión de los incidentes informáticos	Replicando la información a clientes y a posibles clientes
Mercado de PYMES	Generando soluciones de acuerdo a las necesidades de cada empresa, con precios competitivos y buen servicio.
<b>¡ÚSELAS!</b>	
<b>AMENAZAS</b> <b>(Problemas presentes)</b>	<b>¿Cómo voy a superarlas?</b>
Desconocimiento por parte de las empresas de la necesidad de inversión en seguridad informática	Charlas y ventas publicitarias, crear cultura de seguridad informática
Nuevas empresas que surjan para el mercado	Posicionarnos, y generar fidelización prestando un buen servicio y soporte.
<b>¡ELIMÍNELAS!</b>	

## 2.11 CONCLUSIONES ESTUDIO DE MERCADO

Al finalizar el trabajo de levantamiento de campo se puede concluir desde la óptica del mercado lo siguiente:

- Que el 90% de los gerentes de TI entrevistados y encuestados, aceptan que hoy día adolecen de servicios calificados en el área de la seguridad de la información en la región. Que la oferta de estos servicios con la que pueden contar en estos momentos resulta costosa por ser de otras ciudades y además que el servicio postventa es deficiente.
- Que la industria regional espera poder contar con soluciones de seguridad informática de acuerdo a las necesidades del cliente, contando con soporte técnico en la región, Respaldo, capacitación y servicio de asesoría técnica-comercial en la preventa y postventa, además esperan recibir acompañamiento en todo el proceso que implica la mitigación de la inseguridad de la información.
- En conclusión podemos afirmar que desde el punto de vista de mercado podemos afirmar que existe la viabilidad de seguir con el proyecto.

### 3. ESTUDIO TECNICO

#### 3.1 TAMAÑO DEL PROYECTO Y LOS FACTORES INFLUYENTES

En esta etapa del estudio se define la capacidad con la cual se debe contar para la prestación de los servicios de seguridad de la información.

**3.1.1 Descripción del Tamaño del Proyecto.** En Función de la Demanda. El tamaño del proyecto depende directamente de factores como lo son la demanda, la mano de obra calificada, los equipos especializados. Para este proyecto específico, se trata de una empresa que tendrá la capacidad de brindar servicios en el área de la seguridad de la información con los siguientes servicios específicos y con las siguientes proyecciones. Nota: tener en cuenta las unidades de cada servicio

Productos/Servicios	mar-12	mar-12	abr-12	may-12	jun-12	jul-12	ago-12	sep-12	oct-12	nov-12	dic-12	ene-13
PRUEBAS DE VULNERABILIDAD	0	15	10	10	8	8	8	11	8	15	20	11
Análisis Forense y Recuperación de datos	0	0	12	15	13	16	16	16	16	16	14	14
Administración perimetral de seguridad Nivel GOLD. (pequeñas y medianas empresa), implementación con equipos de marca propia, CICO-SIS	0	15	12	8	9	13	13	16	14	15	17	11
Administración perimetral de seguridad SILVER. (pequeñas y medianas empresa), implementación con equipos de marca propia, SICO-SIS	0	15	12	15	18	10	12	14	15	16	8	8
Administración perimetral de seguridad Nivel PLATINUM. (pequeñas y medianas empresa), implementación con equipos de marca propia, SICO-SIS	0	14	0	12	12	12	12	12	12	12	12	12
Administración de Seguridad Perimetral (Mediana empresa) Soporte 7x24 y equipos comprado a proveedores internacionales	0	14	0	12	5	12	12	12	12	12	12	12
Auditoría de Sistemas (por horas)	0	12	12	12	13	13	13	13	13	13	19	19

Hardening(Aseguramiento) e instalación de plataformas no propietarias		13	0	0	13	0	14	0	13	0	16	0
Capacitación en Sistemas de Información y Seguridad Informática (grupo mínimo de 10 personas, 1 día )	0	10	14	14	11	14	6	7	13	15	8	8

**3.1.2 Disponibilidad de Equipos.** La disponibilidad de los equipos tanto para la prestación de servicios de Niterix hacia los clientes y los equipos que el propio cliente adquiere, son los insumos fundamentales para la actividad comercial de Niterix.

### 3.1.2.1 Equipos procesos técnicos y operativos:

Maquinaria y Equipo	unidades
Tenable Nessus ( Scanner de vulnerabilidades para red ) (licencia por un año)	1
Acunetix(Scanner vulnerabilidades para web) (licencia perpetua)	1
FTK(forensic tool Kit) (herramienta para análisis forense)	1
x-way forensic (Winhex) (herramienta par análisis forense)	1
Ontrack EasyRecovery (Herramienta para recuperación de datos)	1
Ultrakit + Ultrablok USB	1
SunFire X-2100 M2 server	2
Portátil LENOVO IBM THINK PAD T61	2
UPS 200KVA (CDP)	1
Rack con componentes (Patch pannel categoría 6 (1), ventiladores (2), Organizadores (1))	1
Portátiles Dell Inspiron 1520 Notebook	2
Switch 3COM 4200G 12 puertos 10/100/1000 3CR1 7660-91	1
Computador escritorio baja gama	1
Computador escritorio gama alta	2
CPU ensamble soluciones seguridad ensambladas por CICO-SIS	1
BitDefender Corporate Security (10 usuarios)	1

### 3.1.2.2 Equipos proceso administrativo

Maquinaria y Equipo	Unidades
Escritorios (3)	3
Sillas ergonómicas (6)	6
Silletería oficina (10)	10
equipo de oficina( grapadora, saca ganchos, lapiceros, papel membretado, teléfonos)	1 GLB

**3.1.3 Tamaño del proyecto y recurso humano.** El recurso humano necesario para la puesta en marcha del proyecto corresponde al manejo técnico, como son el gerente y el equipo de ingeniería.

#### 3.1.3.1 Talento humano

CARGO	FUNCIONES
Gerente	Planifica las tareas de la empresa, se encarga de la promoción de la misma, se encarga de proveedores, pagos, buscar nuevos productos y líneas de negocio
Asesor Comercial	Se encarga de la venta de las soluciones de seguridad, visitar cliente, retroalimentar a los cliente, hacer seguimiento a cotizaciones.
Ingenieros Soporte	Implementaran las soluciones vendidas, dar soporte pos-venta, monitoreo de redes, auditoria, demostraciones técnicas de producto.
Secretaria	Contestar el teléfono, coordinar mensajeros, coordinar diligencias, registro de llamadas.

**3.1.4 Tamaño del proyecto y Proveedores.** La tecnología especial que requiere el proyecto está dada en los equipos de alta tecnología que se requieren como lo son los firewall, appliance, equipos de cómputo de alto nivel, software forensic tool kits entre otros, se ha evidenciado que podemos contar con proveedores nacionales e internacionales de alta confiabilidad como los son:

1) MPS mayorista de colombia s.a.

LISTA SEMANAL DE PRECIOS - **INTERNA NOVIEMBRE 6 A 13** DE 2007

<b>Bogotá</b>	Autopista Bogotá - Medellín (Calle 80) Kilómetro 2. PBX Ventas (1) 8 766565 – Fax Ventas (1) 8 766616
<b>C.A.T.</b>	Cra. 15 # 77 - 05 Loc. 307 y 308
<b>Medellín</b>	Cra. 43A No. 63 Sur 152 Bodega 149 (Sabaneta) - PBX (4) 3014949 - Fax (4) 2888060
<b>Cali</b>	Av. 5 A # 23DN-68 Centro Comercial La Pasarella Local 2-103 – Tel.: 6676590 / 66771 74 / 66771 79 / 6680897 / 6679098 / 661 8696
<b>Barranquilla</b>	Cra 43. # 50 - 12 Parque Central Barranquilla Local 170 – Tel: - 3518580 / 3518323 / 3518834 / 3519091 / 3519346 / 3519346 / 3519603
<b>Línea gratuita</b>	018000 911679 (Exclusiva para clientes de la Costa Atlantica, Valle, Santanderes y Eje Cafetero)

2) Dell

[www.dell/colombia.com](http://www.dell/colombia.com)

3) Acces Data

[www. Accesdata.com](http://www.Accesdata.com)

384 South 400 West Lindon UTA ,USA

4) Nessus

<http://www.nessus.org/contact/index.php>

5) Bitdefender

[www.bitdefender.com](http://www.bitdefender.com)

Aagón, País Vasco, La Rioja, Navarra y Cantabria)  
C/ Padre Marin, 24 bajo  
26004 Logroño (La Rioja) , **Tel/Fax: (+34) 941 27 48 48**

6) X-ways Win-Hex

<http://www.x-ways.net/corporate/contact.html>

X-Ways Software Technology Aktiengesellschaft

Carl-Diem-Str. 32

32257 Bünde

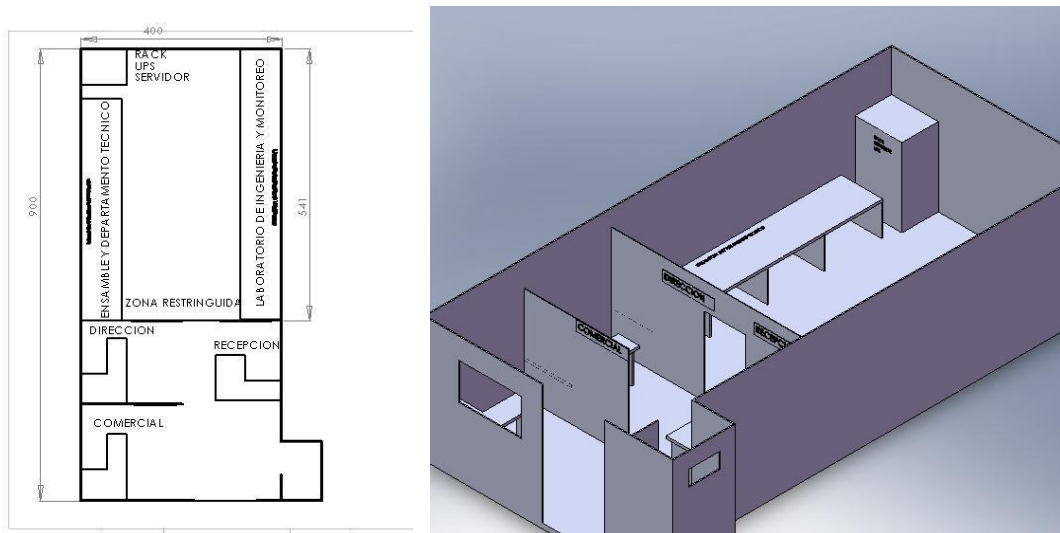
+49 221-420 486 5

+49 721-151 322 561

Germany

**3.1.5 Tamaño del proyecto y la localización.** La localización de la oficina se realizara teniendo en cuenta el POT de la ciudad de Bucaramanga, y que cuente con espacio para la siguiente distribución:

**Figura 4. Plano de la planta**



Fuente: Los Autores

**3.1.6 Tamaño del proyecto y el financiamiento.** La formulación del presente proyecto se realiza con el ánimo de presentarlo ante un concurso de emprendimiento donde el financiamiento está pensado en que nosotros como socios financiemos con recursos propios el 23% del proyecto y la fundación Bavaria financie el 77%. Cabe resaltar que el 77% de la financiación que puede aportar Bavaria está dentro del rango de capital semilla que ellos aportan.

### **3.2 CAPACIDAD DEL PROYECTO**

La capacidad de un proyecto se define por su capacidad diseñada, instalada y utilizada y estos a su vez dependen del talento humano, maquinaria y equipo y finalmente del tiempo requerido para la ejecución.

Nuestra capacidad instalada está diseñada para cubrir el primer año de funcionamiento según las proyecciones anteriormente mencionadas, sin embargo de llegar a superarse dichas proyecciones no tendríamos problemas con adaptarnos.

### **3.3 LOCALIZACION**

**3.3.1 Macro Localización.** La compañía Niterix se ubicara en la ciudad de Bucaramanga, perteneciente al departamento de Santander en el territorio colombiano.

**3.2.2 Micro Localización.** Para la micro localización se analizan aspectos como

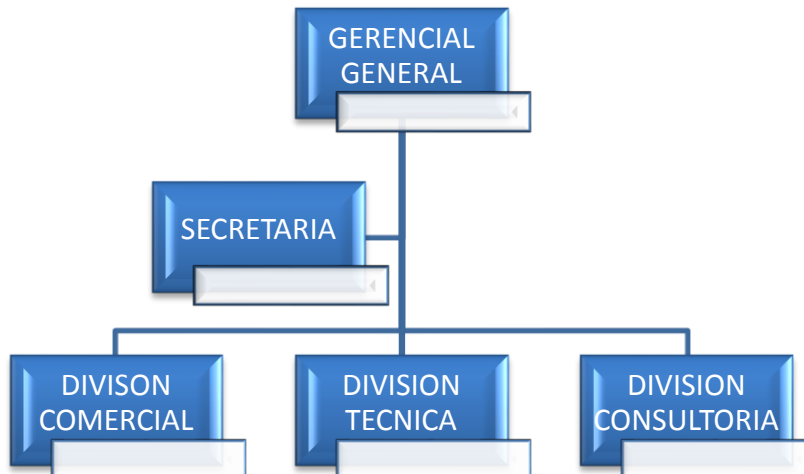
- ❖ Ubicación.
- ❖ Área.
- ❖ Vías de acceso
- ❖ Servicios públicos: agua, luz, gas, alcantarillado y teléfono.

- ❖ Distribución del sitio.
- ❖ Canon de arrendamiento.

Para tomar la decisión de la localización se realizó una comparación cualitativa y cuantitativa, utilizando un proceso de jerarquización, al final del ejercicio se obtuvo que el mejor sitio dentro de la baraja de opciones es la calle 20 32-77 San Alonzo –Bucaramanga.

### 3.4 DIAGRAMA ORGANIZACIONAL

Figura 5. Organigrama



Fuente: Los Autores

### 3.5 ESTUDIO LEGAL

**3.5.1 La Ley 1273 de 2009 [2].** Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales. No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más

usuales en todas partes del mundo. Según la Revista Cara y Sello, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos.

- *Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*

- *Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.*

- *Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.*

- *Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*

- Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

- Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

- Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239[3] manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal[4], es decir, penas de prisión de tres (3) a ocho (8) años.

- *Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.*

**3.5.2 Ley 1266 de 2008, Ley HABEAS DATA [3].** *La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.*

ARTÍCULO 3o. *DEFINICIONES.* Para los efectos de la presente ley, se entiende por:

a) Titular de la información. Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley;

b) Fuente de información. Es la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. Si la fuente entrega la información directamente a los usuarios y no, a través de un operador, aquella tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos. La fuente de la información responde por la calidad de los datos

suministrados al operador la cual, en cuanto tiene acceso y suministra información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos;

c) Operador de información. <Literal CONDICIONALMENTE exequible> Se denomina operador de información a la persona, entidad u organización que recibe de la fuente datos personales sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la presente ley. Por tanto el operador, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. Salvo que el operador sea la misma fuente de la información, este no tiene relación comercial o de servicio con el titular y por ende no es responsable por la calidad de los datos que le sean suministrados por la fuente.

d) Usuario. El usuario es la persona natural o jurídica que, en los términos y circunstancias previstos en la presente ley, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. El usuario, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. En el caso en que el usuario a su vez entregue la información directamente a un operador, aquella tendrá la doble condición de usuario y fuente, y asumirá los deberes y responsabilidades de ambos;

e) Dato personal. Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados;

f) Dato público. Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas;

g) Dato semiprivado. Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley.

h) Dato privado. Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

i) Agencia de Información Comercial. Es toda empresa legalmente constituida que tenga como actividad principal la recolección, validación y procesamiento de información comercial sobre las empresas y comerciantes específicamente solicitadas por sus clientes, entendiéndose por información comercial aquella información histórica y actual relativa a la situación financiera, patrimonial, de mercado, administrativa, operativa, sobre el cumplimiento de obligaciones y demás información relevante para analizar la situación integral de una empresa. Para los efectos de la presente ley, las agencias de información comercial son operadores de información y fuentes de información.

## 4. ANALISIS FINANCIERO

### 4.1 DATOS INICIALES.

En el siguiente cuadro se describen los datos iniciales con los cuales se realizan los cálculos para el análisis financiero del proyecto.

<b>APORTES SALARIALES</b>	
<b>Salario Mínimo Legal</b>	\$ 566.700,00
<b>Subsidio de Transporte</b>	\$ 67.800,00
<b>SEGURIDAD SOCIAL</b>	
EPS	8,50%
PENSION	11,63%
FONDO SOLIDARIDAD PEN	
ARP	1,25%
CAJA COMPENSACION	9,00%
<b>TOTAL SEGURIDAD SOCIAL</b>	<b>30,38%</b>

<b>PRESTACIONES SOCIALES</b>	
CESANTIAS	8,33%
INTERESES/CESANT	1,00%
PRIMAS	8,33%
VACACIONES	4,17%
<b>TOTAL PRESTACIONES</b>	<b>21,83%</b>
<b>GRAN TOTAL %</b>	<b>52,21%</b>

### 4.2 CALCULO DE LOS COSTOS UNITARIOS DE LOS PRODUCTOS.

Se realizó un análisis de costo unitario de cada uno de los productos donde se tienen en cuenta solo los costos directos el personal especializado que se involucra no se tiene en cuenta en estos costos ese valor se adiciona en los costos administrativos.

PRODUCTO	COSTO UNITARIO
PRUEBAS DE VULNERABILIDAD	\$ 27.500
Análisis Forense y Recuperación de datos	\$ 23.000
Administración perimetral de seguridad Nivel GOLD. (pequeñas y medianas empresa), implementación con equipos de marca propia, CICO-SIS	\$ 190.000
Administración perimetral de seguridad SILVER . (pequeñas y medianas empresa), implementación con equipos de marca propia, SICO-SIS	\$ 120.000
Administración perimetral de seguridad Nivel PLATINIUM. (pequeñas y medianas empresa), implementación con equipos de marca propia, SICO-SIS	\$ 1.135.000
Administración de Seguridad Perimetral (Mediana empresa) Soporte 7x24 y equipos comprado a proveedores internacionales	\$ 1.300.000
Auditoría de Sistemas (por horas)	\$ 12.500
Hardening (Aseguramiento) e instalación de plataformas no propietarias	\$ 8.000
Capacitación en Sistemas de Información y Seguridad Informática (grupo mínimo de 10 personas, 1 día )	\$ 38.000

### 4.3 COSTOS ADMINISTRATIVOS

#### 4.3.1 Nomina.

No	Cargo	Salario	Total Salario con prestaciones
1	Gerente	\$ 2.500.000	\$ 3.805.125
2	Asesor Técnico Comercial	\$ 1.200.000	\$ 1.826.460
3	Secretaria	\$ 566.700	\$ 930.346
4	Ingeniero Soporte Técnico 1	\$ 1.500.000	\$ 2.283.075
5	Ingeniero Soporte Técnico 2	\$ 1.500.000	\$ 2.283.075
6	Tecnólogo soporte 1	\$ 1.000.000	\$ 1.589.850
7	Tecnólogo soporte 2	\$ 1.000.000	\$ 1.589.850

#### 4.3.2 Otros Gastos de Administración.

DESCRIPCIÓN	GASTOS AL AÑO
Arriendo	7.150.000
Servicios	5.500.000
Aseo	880.000
Mantenimiento	-
Papelería y Útiles	935.000
Gastos de Viaje	-
Cuota de Préstamos Anteriores	-
Honorarios	3.300.000
Imprevistos	1.650.000
Transporte	-
Otros	550.0

#### 4.4 INVERSIONES.

**4.4.1 Maquinaria y Equipo.** En este ítem se describen las inversiones realizadas en el software y el hardware requeridos para la prestación de los servicios. El total de este ítem es de \$82.796.800.

Maquinaria y Equipo	Unidades	Valor
Tenable Nessus (Scanner de vulnerabilidades para red ) (licencia por un año)	1	2.460.000
Acunetix(Scanner vulnerabilidades para web) (licencia perpetua)	1	15.375.000
FTK(forensic tool Kit) (herramienta para análisis forense)	1	3.792.500
x-way forensic (Winhex) (herramienta para análisis forense)	1	1.435.000

Ontrack EasyRecovery (Herramienta para recuperación de datos)	1	3.075.000
Ultrakit + Ultrablok USB	1	3.280.000
SunFire X-2100 M2 server	2	16.810.000
Portatil LENOVO IBM THINK PAD Y450	2	7.884.300
UPS 200KVA (CDP)	1	3.075.000
Rack con componentes (Patch pannel categoría 6 (1), ventiladores (2), Organizadores (1))	1	1.640.000
Portátiles Toshiba Satellite	2	3.120.000
Switch 3COM 4200G 12 puertos 10/100/1000 3CR1 7660-91	1	2.050.000
Computador escritorio baja gama	1	1.300.000
Computador escritorio gama alta (2 unidades)	2	6.000.000
CPU ensamble soluciones seguridad ensambladas por CICO-SIS	1	10.000.000
BitDefender Corporate Security (10 usuarios)	1	1.500.000
<b>TOTAL MAQUINARIA Y EQUIPO</b>		<b>82.796.800</b>

**4.4.2 Muebles y enseres.** En este apartado se incluyen los activos representados en muebles y enseres destinados a la oficina, incluyendo los elementos básicos de escritorio y las adecuaciones e instalaciones.

Esta inversión suma un total de \$ 4.450.000

Muebles, Enseres y Utensilios	Unidades (glb)	Instalación
Escritorios	1	\$ 850.000
Sillas ergonómicas	1	\$ 500.000
Silletería oficina	1	\$ 500.000
equipo de oficina( grapadora, saca ganchos, lapiceros, papel membreteado, teléfonos)	1	\$ 800.000
Adecuaciones	1	\$ 1.800.000

<b>INVERSION TOTAL</b>	<b>\$ 87.246.800</b>
------------------------	----------------------

La inversión total del proyecto está representada en la compra del software y hardware, en los muebles y enseres y su adecuación e instalación para un total de OCHENTA Y SIETE MILLONES DOSCIENTOS CUARENTA Y SEIS MIL OCHOCIENTO PESOS COLOMBIANOS (\$ 87.246.800).

#### 4.5 FUENTES DE FINANCIACIÓN.

Esta inversión se pretende realizar el 23% es decir veinte millones de pesos (\$20.000.000) con recursos propios de los inversionistas y el 77% equivalente Sesenta y siete millones doscientos cuarenta y seis mil ochocientos (\$67.246.800), se pretenden obtener del premio del concurso destapa futuro de la empresa BAVARIA, al cual se presentará este proyecto.

#### 4.6 DEFINICION DE PRECIOS DE VENTA.

En este proyecto los precios de venta son de vital importancia para la definición de cada uno de los precios de venta se calcula un facto con base en los gastos y este factor se le aplica al costo de producción de cada servicio, esto para garantizar que cada precio de venta sea siempre mayor que lo que cuesta su producción.

PRODUCTO	COSTO UNITARIO	FACTOR	PRECIO MINIMO	% de Ganacia	PRECIO AL PUBLICO
PRUEBAS DE VULNERABILIDAD	27500	0,61	44.328,55	30%	57.627
Análisis Forense y Recuperación de datos	23000	0,61	37.074,78	70%	63.027
Administracion perimetral de seguridad Nivel GOLD. (pequeñas y medianas empresa), implementación con equipos de marca propia, CICO-SIS	190000	0,61	306.269,95	30%	398.151
Administracion perimetral de seguridad SILVER . (pequeñas y medianas empresa), implementación con equipos de marca propia, SICO-SIS	120000	0,61	193.433,65	30%	251.464

Administración perimetral de seguridad Nivel PLATINIUM. (pequeñas y medianas empresa), implementación con equipos de marca propia, SICO-SIS	<b>1135000</b>	0,61	1.829.559,98	30%	2.378.428
Administración de Seguridad Perimetral (Mediana empresa) Soporte 7x24 y equipos comprado a proveedores internacionales	<b>1300000</b>	0,61	2.095.531,25	30%	2.724.191
Auditoría de Sistemas (por horas)	<b>12500</b>	0,61	20.149,34	80%	36.269
Hardening (Aseguramiento) e instalación de plataformas no propietarias	<b>8000</b>	0,61	12.895,58	90%	24.502
Capacitación en Sistemas de Información y Seguridad Informática (grupo mínimo de 10 personas, 1 día)	<b>38000</b>	0,61	61.253,99	30%	79.630

#### 4.7 FLUJO DE CAJA

El flujo de caja del proyecto se elaboró en un horizonte de tiempo de un año esto debido a las exigencias propias del concurso de emprendimiento al que se está proyectando presentar.

Es importante aclarar en este punto del documento que de las entrevistas sostenidas con los gerentes de TI y de seguridad Informática, obtuvimos información que nos ayudó a determinar los servicios a ofrecer y el nivel de ventas que se puede llegar a tener de cada servicio, siendo este el sustento que nos permite conectar el estudio de mercados con los niveles de venta proyectados. Las apreciaciones de los entrevistados fueron diversas, pero nos centramos en niveles de inversión, en descripción de productos y la diferenciación que tendríamos con respecto a nuestros competidores como motivante para lograr negocios en el futuro.

El flujo de caja en el año tiene como ingresos las ventas de cada mes que fueron calculadas con la cantidad de productos o servicios prestados por el precio de

venta de cada uno para cada mes, como egresos se tiene en cuenta los costos operativos que para cada mes son calculados de la cantidad de servicios prestados en cada mes por el costo de producción de cada producto o servicio, adicionalmente los gastos de administración, los gastos de ventas (publicidad y transporte) y la nómina variable al inicio del flujo con una tendencia a estabilizarse.

% de ventas de Contado	70%
% de ventas a crédito	30%
Plazo para el pago de las ventas a crédito (días múltiplos de 30)	30

DESEMBOLSO	mar-12	mar-12	abr-12	may-12	jun-12	jul-12	ago-12	sep-12	oct-12	nov-12	dic-12	ene-13	ACUMULADO
------------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	--------	-----------

<b>Saldo Inicial</b>	<b>20.000.000</b>	-	-	77.445.625	61.225.282	53.361.529	36.277.917	16.804.059	5.672.281	29.917.603	54.710.494	79.678.080	97.745.925	-
<b>Ingresos</b>														
Ventas	-	58.516.735	32.553.216	53.085.626	58.630.772	66.349.887	72.124.027	73.311.508	73.848.577	74.497.772	74.065.126	49.325.654	<b>686.308.899</b>	
Otros Ingresos	67.246.800												-	
Crédito	-												-	
<b>Total Ingresos</b>	<b>87.246.800</b>	<b>-</b>	<b>58.516.735</b>	<b>32.553.216</b>	<b>53.085.626</b>	<b>58.630.772</b>	<b>66.349.887</b>	<b>72.124.027</b>	<b>73.311.508</b>	<b>73.848.577</b>	<b>74.497.772</b>	<b>74.065.126</b>	<b>49.325.654</b>	<b>686.308.899</b>
<b>Egresos</b>														
Operativos	-	-	39.786.500	4.953.000	33.842.000	25.193.500	34.172.500	34.220.500	35.039.000	35.028.500	35.503.000	34.951.500	33.436.000	<b>346.126.000</b>
Gastos de Administración		-	1.815.000	1.815.000	1.815.000	1.815.000	1.815.000	1.815.000	1.815.000	1.815.000	1.815.000	1.815.000	1.815.000	<b>19.965.000</b>
Gastos de Ventas		-	4.200.000	300.000	300.000	300.000	300.000	1.700.000	300.000	300.000	300.000	300.000	300.000	<b>8.600.000</b>
Nómina		-	7.364.060	9.264.873	9.264.873	14.238.660	10.588.529	11.912.186	11.912.186	11.912.186	11.912.186	18.930.780	11.912.186	<b>129.212.706</b>
Crédito CFE		-	-	-	-	-	-	-	-	-	-	-	-	-
Crédito adicional		-	-	-	-	-	-	-	-	-	-	-	-	-
Impuestos Legalizaciones y Registros													68.424.591	<b>68.424.591</b>
Maquinaria y Equipos	<b>82.796.800</b>	-	82.796.800	-	-	-	-	-	-	-	-	-	-	<b>82.796.800</b>
Muebles, Enseres y Utensilios	<b>2.650.000</b>	-	-	-	-	-	-	-	-	-	-	-	-	-
Adecuaciones	<b>1.800.000</b>	-	-	-	-	-	-	-	-	-	-	-	-	-

Otros egresos

Total Egresos	87.246.800	-	135.962.360	16.332.873	45.221.873	41.547.160	46.876.029	49.647.686	49.066.186	49.055.686	49.530.186	55.997.280	115.887.777
Disponible periodo		-	77.445.625	16.220.343	7.863.753	17.083.612	19.473.858	22.476.341	24.245.322	24.792.891	24.967.586	18.067.845	-66.562.123
Caja Acumulada	-	-	77.445.625	61.225.282	53.361.529	36.277.917	16.804.059	5.672.281	29.917.603	54.710.494	79.678.080	97.745.925	31.183.803

## 4.8 ESTADO DE PÉRDIDAS Y GANANCIAS

	mar-12	mar-12	abr-12	may-12	jun-12	jul-12	ago-12	sep-12	oct-12	nov-12	dic-12	ene-13	ANUAL
Ventas	0	83.595.336	10.678.021	71.260.313	53.218.112	71.977.791	72.186.699	73.793.569	73.872.151	74.765.895	73.764.796	70.465.220	729.577.904
Costos de Ventas	0	39.786.500	4.953.000	33.842.000	25.193.500	34.172.500	34.220.500	35.039.000	35.028.500	35.503.000	34.951.500	33.436.000	346.126.000
<b>Utilidad Bruta</b>	<b>0</b>	<b>43.808.836</b>	<b>5.725.021</b>	<b>37.418.313</b>	<b>28.024.612</b>	<b>37.805.291</b>	<b>37.966.199</b>	<b>38.754.569</b>	<b>38.843.651</b>	<b>39.262.895</b>	<b>38.813.296</b>	<b>37.029.220</b>	<b>383.451.904</b>
<i>Margen bruto</i>		52,4%	53,6%	52,5%	52,7%	52,5%	52,6%	52,5%	52,6%	52,5%	52,6%	52,5%	52,6%
Gastos de Administración	0	1.815.000	1.815.000	1.815.000	1.815.000	1.815.000	1.815.000	1.815.000	1.815.000	1.815.000	1.815.000	1.815.000	19.965.000
Nómina	0	8.845.006	11.128.081	11.128.081	12.717.931	12.717.931	14.307.781	14.307.781	14.307.781	14.307.781	14.307.781	14.307.781	142.383.713
Depreciación	1.417.030	1.417.030	1.417.030	1.417.030	1.417.030	1.417.030	1.417.030	1.417.030	1.417.030	1.417.030	1.417.030	1.417.030	17.004.360
Gastos de Ventas	0	4.200.000	300.000	300.000	300.000	300.000	1.700.000	300.000	300.000	300.000	300.000	300.000	8.600.000
<b>Utilidad Operacional</b>	<b>-1.417.030</b>	<b>27.531.800</b>	<b>-8.935.089</b>	<b>22.758.203</b>	<b>11.774.651</b>	<b>21.555.330</b>	<b>18.726.389</b>	<b>20.914.758</b>	<b>21.003.841</b>	<b>21.423.085</b>	<b>20.973.485</b>	<b>19.189.410</b>	<b>195.498.831</b>
<i>Margen Operacional</i>		32,9%	-83,7%	31,9%	22,1%	29,9%	25,9%	28,3%	28,4%	28,7%	28,4%	27,2%	26,8%
Otros Egresos	0	0	0	0	0	0	0	0	0	0	0	0	0
Otros Ingresos	0	0	0	0	0	0	0	0	0	0	0	0	0
<b>Utilidad Antes de Impuestos</b>	<b>-1.417.030</b>	<b>27.531.800</b>	<b>-8.935.089</b>	<b>22.758.203</b>	<b>11.774.651</b>	<b>21.555.330</b>	<b>18.726.389</b>	<b>20.914.758</b>	<b>21.003.841</b>	<b>21.423.085</b>	<b>20.973.485</b>	<b>19.189.410</b>	<b>195.498.831</b>
Impuestos													68.424.591
<b>Utilidad Neta</b>	<b>-1.417.030</b>	<b>27.531.800</b>	<b>-8.935.089</b>	<b>22.758.203</b>	<b>11.774.651</b>	<b>21.555.330</b>	<b>18.726.389</b>	<b>20.914.758</b>	<b>21.003.841</b>	<b>21.423.085</b>	<b>20.973.485</b>	<b>19.189.410</b>	<b>127.074.240</b>
<i>Margen Neto</i>		32,9%	-83,7%	31,9%	22,1%	29,9%	25,9%	28,3%	28,4%	28,7%	28,4%	27,2%	17,4%

#### 4.9 BALANCE

<b>ACTIVOS</b>	
Caja y Bancos	31.183.803
Cuentas por Cobrar	43.269.005
Inventarios	-
<b>Total Activos Corrientes</b>	<b>74.452.807</b>
Activos Fijos	170.043.600
Depreciación Acumulada	17.004.360
<b>Total Activo Largo Plazo</b>	<b>153.039.240</b>
<b>Total Activos</b>	<b>227.492.047</b>

<b>PASIVOS</b>	
Cuentas por Pagar	13.171.007
Obligaciones Financieras	-
Otras Obligaciones	-
<b>Total Pasivos</b>	<b>13.171.007</b>
<b>Capital Inicial</b>	<b>20.000.000</b>
<b>Donación Bavaria</b>	<b>67.246.800</b>
<b>Aporte bienes muebles</b>	<b>-</b>
<b>Utilidad del Ejercicio</b>	<b>127.074.240</b>
<b>Patrimonio</b>	<b>214.321.040</b>
<b>Pasivo + Patrimonio</b>	<b>227.492.047</b>

#### 4.10 EVALUACIÓN FINANCIERA.

Con la información que se tiene se decide realizar el cálculo de algunos indicadores financieros con el fin de evaluar la viabilidad del proyecto.

		RESULTADOS
REZONES DE LIQUIDEZ	PRUEBA ACIDA No.1	5,65
REZONES DE ENDEUDAMIENTO	ENDEUDAMIENTO TOTAL	0,06
RENTABILIDAD	RENTABILIDAD ACTIVO	0,56
	RENTABILIDAD OPERACIONAL	0,27
VALOR PRESENTE NETO	VPN	3.080.507
TASA INTERNA DE RETORNO	TIR	0,12

- La prueba ácida efectuada para la evaluación financiera de nuestro proyecto donde  $PA = (\text{Activo corriente} - \text{Inventarios}) / \text{Pasivo corriente}$  que en este caso es de 5,65, nos da un indicio que para el análisis en el horizonte de un año, el proyecto estaría en capacidad de pagar los pasivos a corto plazo sin vender todos los productos y servicios.

También nos muestra que garantiza en este espacio de tiempo un pago de la deuda a corto plazo, sin embargo debemos tener en cuenta que en la inversión inicial el 67% (67.246.800) lo aportaría el éxito del proyecto y que el análisis por lo tanto está proyectado a un año inicialmente.

- El proyecto no me genera un alto nivel de endeudamiento ya que solo registra un 0,06 ya que la mayoría de recursos son financiados y lo cual me indica que es una relación, adecuada y conservadora, mostrándonos que la estructura de financiamiento está compartida entre el desarrollo del proyecto (financiación) y los aportes (saldo inicial).

- La rentabilidad del activo que me muestra un 0,56 de capacidad de producción de utilidad me indica que hay un margen de capacidad del activo para producir utilidades, independientemente de la forma como haya sido financiado, que en este caso hace parte de un 23% de aportes y un 77% de la financiación por parte del concurso.
- La rentabilidad operacional del proyecto (0,27) está influenciada tanto como por el costo de las ventas, sino también por los gastos operacionales de administración y ventas. La rentabilidad operacional tiene gran importancia dentro del desarrollo del proyecto, ya que nos indica que el negocio es rentable, independientemente de la forma como ha sido financiado en este caso.
- Un VPN positivo de 3.080.507 nos indica que el proyecto renta por encima de la tasa de descuento y que los ingresos a valor presente son superiores a la inversión. Y por tanto el proyecto es conveniente, sin embargo debemos resaltar nuevamente que el VPN calculado para el horizonte de tiempo de un año nos muestra una rentabilidad inicial.
- Una TIR de 0,12 nos indica que que el proyecto tiene una rentabilidad asociada mayor que la tasa de descuento por lo tanto es el proyecto es viable, pues estima un rendimiento mayor al mínimo requerido.

## **CONCLUSIONES**

### **Ambiental**

Nuestra empresa contribuirá en la parte ambiental de la siguiente forma: como uno de nuestros servicios es la administración remota de seguridad, esto implicara una disminución en la compra de equipos por parte de nuestros clientes y posteriormente una reducción de basura tecnológica, puesto que las empresas compartirán ciertos servicios a través de nosotros y no tendrán que comprar cada una de ellas todos los equipos, es decir estamos hablando del mejor aprovechamiento de la tecnología el reusó.

### **Técnica**

Es un proyecto que nos exige un alto nivel técnico porque nuestra empresa generara soluciones de seguridad informática a la medida de las necesidades de nuestros clientes, teniendo como principio la operatividad, calidad, servicio y soporte. Además el tema de seguridad informática está en constante cambio y exige de parte nuestra un continuo estudio y desarrollo para poder suplir las necesidades de nuestros clientes de manera óptima y oportuna.

### **De mercado**

Actualmente existe la necesidad de una empresa que se preocupe por la seguridad informática en nuestra región de una forma personalizada con soporte y buena asesoría técnica, puesto que las empresas que actualmente tienen implementadas soluciones de seguridad evidencian la necesidad de soporte en la región; además la gran mayoría de PYMES están desprotegidas por varios factores como desconocimiento y el factor más importante es el costo de la

seguridad informática; lo que nosotros proponemos son soluciones outsourcing económicas y administradas por nosotros para que las PYMES centren su energía en el objeto de su negocio y no en estar solucionando problemas de seguridad informática, de esta segunda parte nosotros nos encargamos.

## **Financiera**

El actual avance en las telecomunicaciones, y el uso de Internet como bastión principal de estas y como uno de los medios de comunicación más utilizado a nivel mundial, nos garantiza un mercado necesitado de nuestros servicios; porque día a día todas las empresas pequeñas, medianas y grandes necesitan comunicarse y realizar sus labores comerciales con sistemas de información; es por esto que creemos que NITERIX será sostenible en el tiempo y jugara un papel importante en el desarrollo de nuestra región, sin embargo se debe hacer un análisis más profundo a nivel de factibilidad.

## **Jurídica**

La legislatura en el tema de seguridad informática avanza cada día, actualmente está aprobada por la corte constitucional la ley de regulación del derecho fundamental de habeas data consagrado en el artículo 15 de la constitución de Colombiana, también se sanciono la ley de delitos informáticos 1273 de 2009, además a puertas de firmar tratados de libre comercio con diferentes países, existen exigencias a nivel internacional sobre la seguridad de la información. Por otro lado las exigencias de la superfinanciera con SARO para la seguridad de la información.

## BIBLIOGRAFIA

[1] A. Carvajal. Fundamentos sobre la inseguridad de la información, un enfoque pragmático. Editorial xyz, Julio de 2008, Bogotá - Colombia, 548 pág.

[2] Ley 1273 de 2009

[3] Ley 1268 de 2008

[4] NIST SPECIAL PUBLICATION 800-82. GUIDE TO SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) AND INDUSTRIAL CONTROL SYSTEMS SECURITY, Septiembre de 2006.

[5] KUROSE JAMES F - ROSS KEITH . REDES DE COMPUTADORES UN ENFOQUE DESCENDENTE BASADO EN INTERNET, 2005

[6] Miranda Miranda Juan José. Gestión de Proyectos. 2000

[7]

[http://library.abb.com/GLOBAL/SCOT/scot271.nsf/VerityDisplay/40A9A9D3961939D3C125701C00498C5C/\\$File/66-70%202M535\\_SPA72dpi.pdf](http://library.abb.com/GLOBAL/SCOT/scot271.nsf/VerityDisplay/40A9A9D3961939D3C125701C00498C5C/$File/66-70%202M535_SPA72dpi.pdf). Seguridad de los sistemas de información industrial.

[8] K. STREETT. <http://www.selinc.com/techpprs/6148.pdf>. Secure scada and engineering access communications: a case study of private and public communication link security.

[9] Y. Wang y B. Chu. <http://citeseer.ist.psu.edu/wang04sscada.html>. Securing SCADA Infrastructure Communications. 2004

[10] <http://citeseer.ist.psu.edu/112165.html>. TCP/IP Manufacturing Applications.

[11] <http://csrc.nist.gov/>. National Institute Of Standars And Technology –  
Computer Security Resource Center.

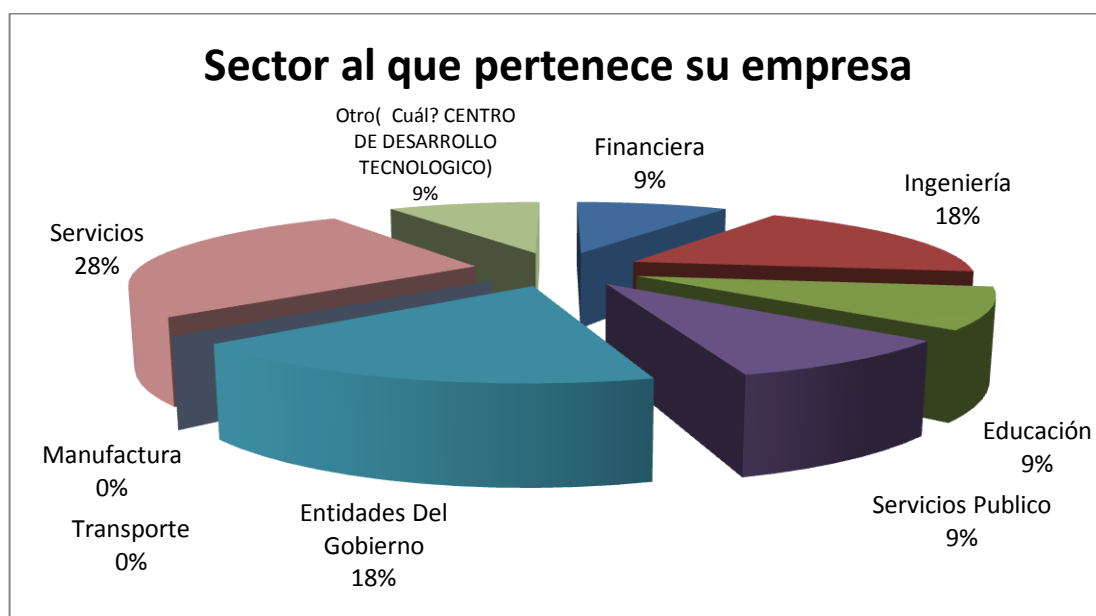
[12] <http://www.digitalbond.com>. Seguridad de la información para sistemas SCADA.

## ANEXOS

### ANEXO 1. TABULACION DATOS DEL ESTUDIO DE MERCADOS

#### 1. Sector al que pertenece su empresa

Figura 6. Pregunta1, Sector al que pertenece su empresa.



Fuente: Los Autores

#### 2. Número de empleados de su empresa

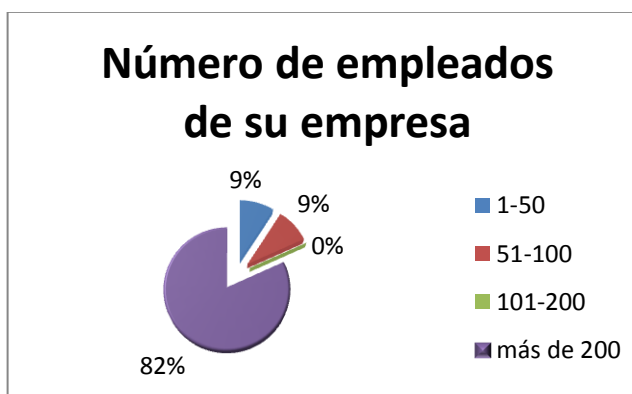
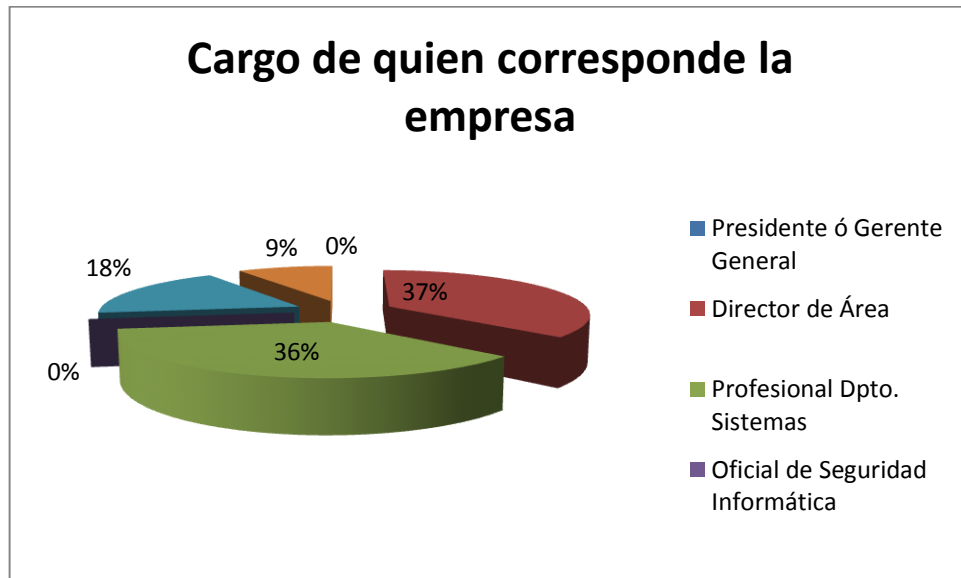


Figura 7. Pregunta 2, Números de empleados de su empresa.

Fuente: Los Autores

### 3. Cargo de quien responde la encuesta

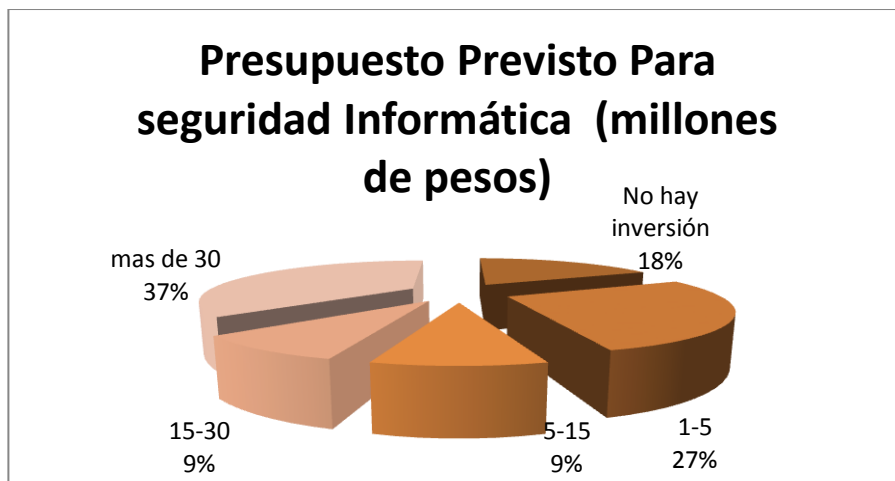
Figura 8. Pregunta 3, Cargo de Quien responde la encuesta.



Fuente: Los Autores

### 4. Presupuesto previsto para seguridad Informática

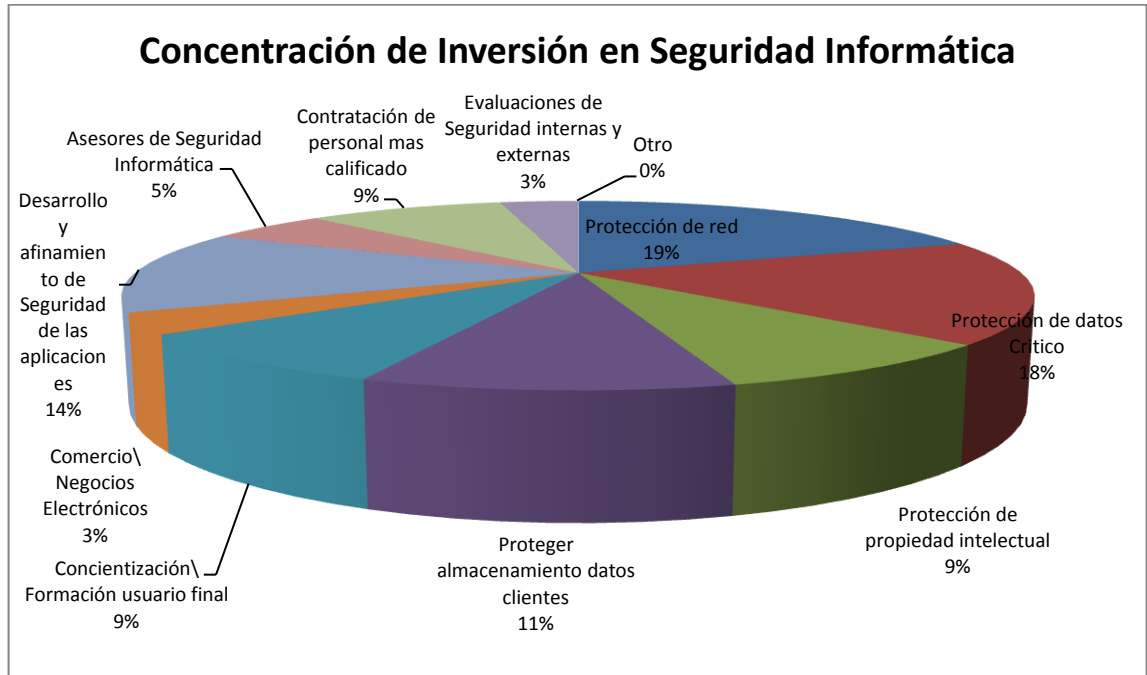
Figura 9. Pregunta 4, Presupuesto previsto para seguridad informática



Fuente: Los Autores

5. ¿En qué tema se concentra la inversión en seguridad Informática? (Seleccione todos los aplicables)

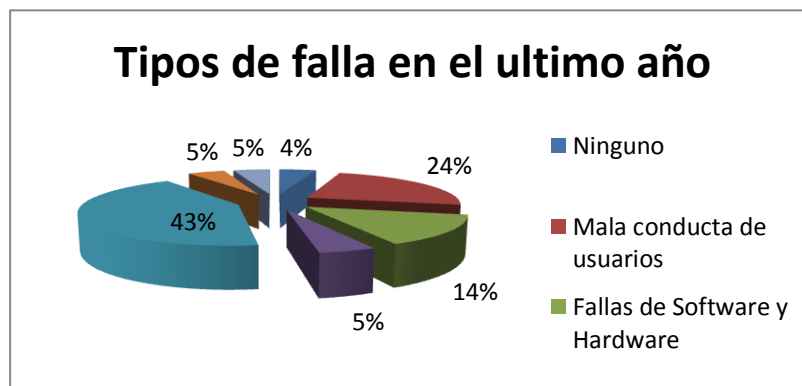
**Figura 10. Pregunta 5, Concentración de Inversión en Seguridad Informática**



Fuente: Los Autores

6. ¿En el último año que tipos de falla de seguridad detectó? (Seleccione todos los aplicables)

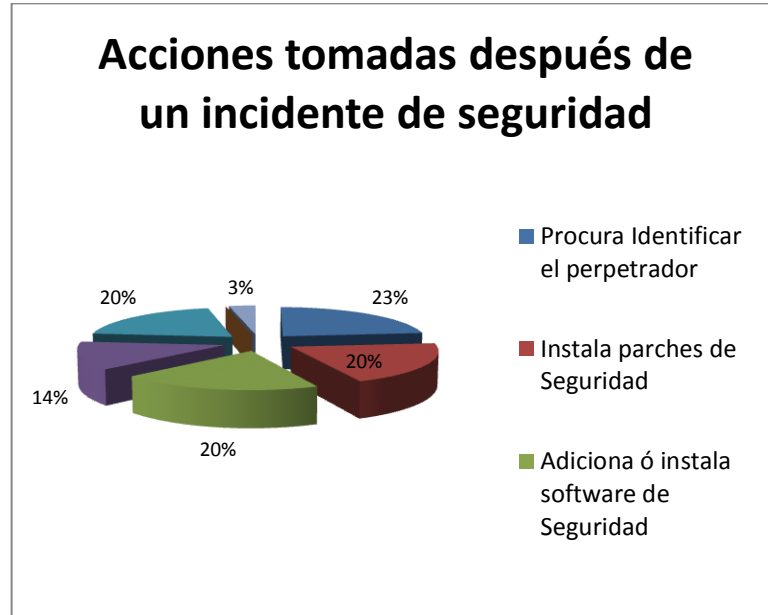
**Figura 11. Pregunta 6, Tipos de falla en el último año**



Fuente: Los Autores

7. Qué acciones toma después de un incidente de seguridad?

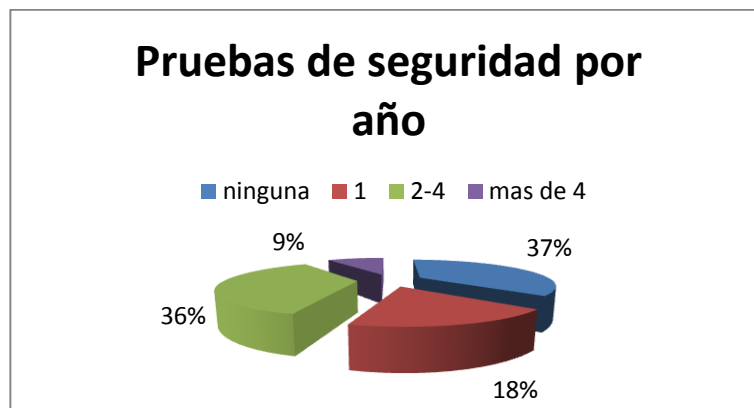
Figura 12. Pregunta 7, Acciones tomadas después de un incidente de seguridad.



Fuente: Los Autores.

8. ¿Cuántas pruebas de seguridad Informática realizan por año, para valorar su estado?

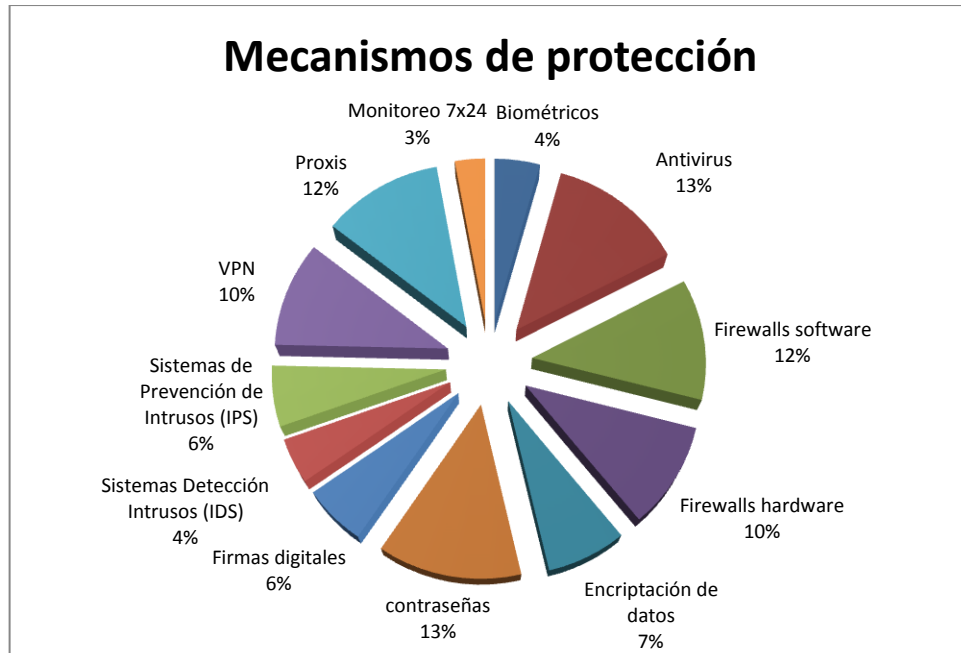
Figura 13. Pregunta 8, Pruebas de seguridad informática realizadas por año.



Fuente: Los Autores.

9. ¿Cuáles de los siguientes mecanismo utiliza actualmente su organización para proteger sus sistemas de información? (seleccione todos los aplicables)

Figura 14. Pregunta 9, Mecanismos de protección



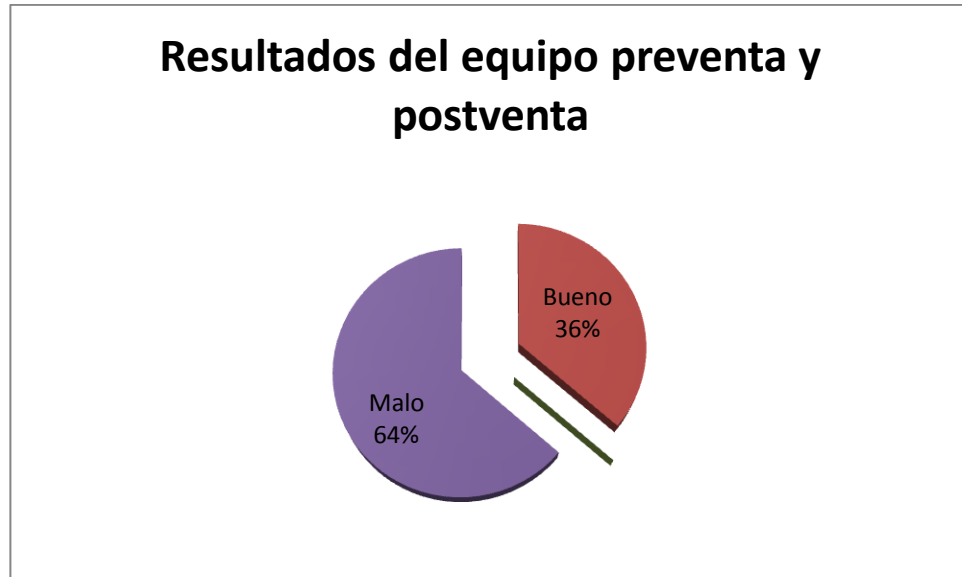
Fuente: Los Autores

10. Cuantas y cuales empresas de seguridad informática conoce con sede en la región?

- Sistemas teleinformaticos y servicios
- Sekurity Net
- Coinsa

11. El servicio de asesoría, soporte técnico preventa y postventa es?

Figura 15. Pregunta 11, Resultados del soporte preventa y postventa



Fuente: Los Autores

12. Considera importante la creación de una empresa de seguridad informática con sede en Santander?

Figura 16. Pregunta 12, Importancia de la creación de una empresa de seguridad informática en Santander



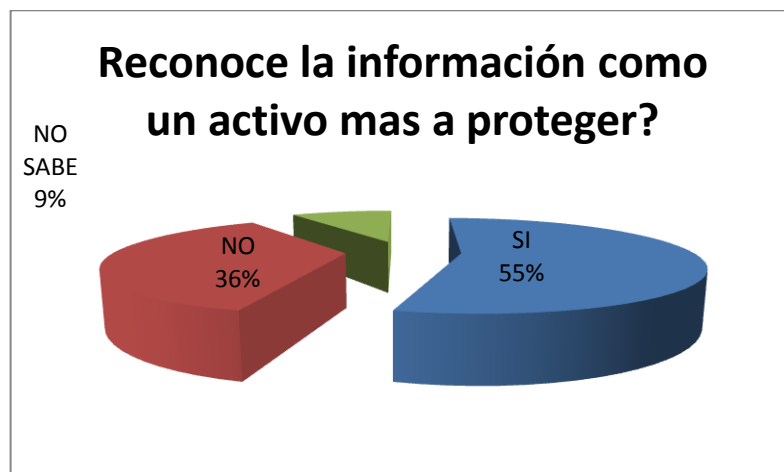
Fuente: Los Autores.

¿Por qué?

- I) Para obtener servicios especializados en el área sin tener que implementar infraestructura dentro de la empresa.
- II) No conozco ninguna.
- III) Para dar soporte en Seguridad Informática y realizar planes a nivel regional de concientización.
- IV) El tema de seguridad informática para la empresa se maneja con políticas y auditorías que lleva a cabo el grupo ubicado en Bogotá
- V) Actualmente los seminarios de actualización se llevan a cabo con una empresa de Bogotá ETECO lo cual eleva los costos mantener el personal de seguridad al día.
- VI) Por la falta de asesoría local en este tema.
- VII) Porque todo lo que se requiera hay que hacerlo por Bogotá o Medellín

13. ¿En su organización (todo el personal) reconoce la información como un activo más a proteger?

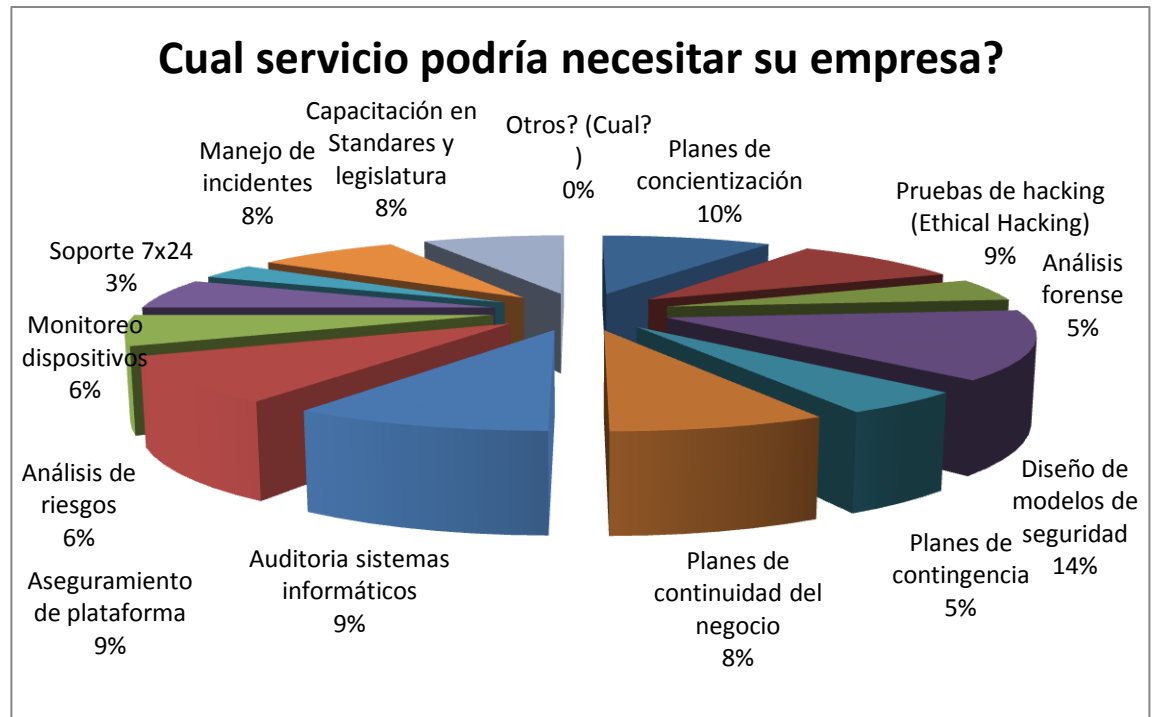
Figura 13. Pregunta 13, Reconocimiento de la información como un activo



Fuente: Los Autores

14. Cuáles de los siguientes servicios cree usted que su organización podría llegar a necesitar de una empresa de seguridad informática? (escoja todos los aplicables)

Figura 14. Pregunta 14, Servicios que necesitan las empresas.



Fuente: Los Autores