DEPARTAMENTO DE CIENCIAS ECONÓMICAS, ADMINISTRATIVAS Y DEL COMERCIO

CARRERA DE INGENIERÍA EN FINANZAS Y AUDITORÍA

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN FINANZAS - CONTADOR PÚBLICO – AUDITOR

TEMA "ANÁLISIS DEL COSTO-BENEFICIO EN LAS EMPRESAS DEL SECTOR INDUSTRIAL REGULADAS POR LA SUPERINTENDENCIA DE COMPAÑÍAS QUE UTILIZAN HERRAMIENTAS DE SEGURIDAD Y PROTECCIÓN DE DATOS EN LA PROVINCIA DE COTOPAXI, DURANTE EL PERÍODO 2012-2016"

AUTORAS: FERNANDA GISSELA GÁLVEZ ESCOBAR,

JOSELINE MARIELA SÁNCHEZ CAJAMARCA

DIRECTOR: ECO. FRANCISCO CAICEDO A.

LATACUNGA

2018

DEPARTAMENTO DE CIENCIAS ECONÓMICAS ADMINISTRATIVAS Y DEL COMERCIO

CARRERA DE INGENIERÍA EN FINANZAS Y AUDITORÍA

CERTIFICACIÓN

Certifico que el trabajo de titulación**, "ANÁLISIS DEL COSTO-BENEFICIO EN LAS EMPRESAS DEL SECTOR INDUSTRIAL REGULADAS POR LA SUPERINTENDENCIA DE COMPAÑÍAS QUE UTILIZAN HERRAMIENTAS DE SEGURIDAD Y PROTECCIÓN DE DATOS EN LA PROVINCIA DE COTOPAXI DURANTE EL PERIODO 2012-2016"** realizado por las Señoritas **FERNANDA GISSELA GÁLVEZ ESCOBAR Y JOSELINE MARIELA SÁNCHEZ CAJAMARCA,** ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la **Universidad de Fuerzas Armadas ESPE,** por lo tanto me permito acreditarlo y autorizar a las señoritas **FERNANDA GISSELA GÁLVEZ ESCOBAR Y JOSELINE MARIELA SÁNCHEZ CAJAMARCA** para que lo sustente públicamente.

Latacunga, Marzo de 2018

Eco. Francisco Caicedo A.
DIRECTOR

DEPARTAMENTO DE CIENCIAS ECONÓMICAS ADMINISTRATIVAS Y DEL COMERCIO

CARRERA DE INGENIERÍA EN FINANZAS Y AUDITORÍA

AUTORÍA DE RESPONSABILIDAD

Nosotras, **FERNANDA GISSELA GÁLVEZ ESCOBAR**, con cédula de identidad N° 050402096-7 y **JOSELINE MARIELA SÁNCHEZ CAJAMARCA** con cédula de identidad N° 050358286-8, declaramos que este trabajo de titulación **"ANÁLISIS DEL COSTO-BENEFICIO EN LAS EMPRESAS DEL SECTOR INDUSTRIAL REGULADAS POR LA SUPERINTENDENCIA DE COMPAÑÍAS QUE UTILIZAN HERRAMIENTAS DE SEGURIDAD Y PROTECCIÓN DE DATOS EN LA PROVINCIA DE COTOPAXI, DURANTE EL PERIODO 2012-2016"**, ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaramos que este trabajo es de nuestra autoría, en virtud de ello nos declaramos responsables del contenido, veracidad y alcance de la investigación mencionada.

Latacunga, Marzo del 2018

FERNANDA GISSELA
GÁLVEZ ESCOBAR
C.C.: 0504020967

JOSELINE MARIELA
SÁNCHEZ CAJAMARCA
C.C.: 0503582868

DEPARTAMENTO DE CIENCIAS ECONÓMICAS ADMINISTRATIVAS Y DEL COMERCIO

CARRERA DE INGENIERÍA EN FINANZAS Y AUDITORÍA

AUTORIZACIÓN

Nosotras, **FERNANDA GISSELA GÁLVEZ ESCOBAR Y JOSELINE MARIELA SÁNCHEZ CAJAMARCA** autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en el repositorio institucional el trabajo de titulación **"ANÁLISIS DEL COSTO-BENEFICIO EN LAS EMPRESAS DEL SECTOR INDUSTRIAL REGULADAS POR LA SUPERINTENDENCIA DE COMPAÑÍAS QUE UTILIZAN HERRAMIENTAS DE SEGURIDAD Y PROTECCIÓN DE DATOS EN LA PROVINCIA DE COTOPAXI DURANTE EL PERIODO 2012-2016"** cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Latacunga, Marzo del 2018

FERNANDA GISSELA GÁLVEZ ESCOBAR
C.C. 050402096-7

JOSELINE MARIELA SÁNCHEZ CAJAMARCA
C.C. 0503582868

DEDICATORIA

A Padre Dios por darme a una gran mujer que es mi ejemplo de vida mi Madre Lourdes Escobar, mediante ella me enseñas a salir adelante a pesar de los adversidades de la vida, ella quien siempre me brinda su apoyo incondicional, su tiempo en enseñanzas, sus valores, el respeto a los demás, y sobre todo al amor y pasión en lo que uno se propone en la vida, a mi hermano Franklin Gálvez por su gran amistad, su apoyo en las buenas y en las malas, a mi Padre Hernán Gálvez que desde el reino de los cielos me das tu bendición, valor, fuerza para seguir adelante y cumplir con una de mis metas, a mi familia, mis primas y mis amigos, quienes todos ellos fueron un pilar fundamental en mi trayectoria universitaria.

Fernanda Gálvez

DEDICATORIA

A mi Familia

Nelly Cajamarca por ser la mejor madre, amiga, consejera quien ha estado presente en cada momento de mi vida apoyándome y no dejándome decaer por ser esa mujer luchadora llena de espíritu y Edguin Sánchez, mi padre sobreprotector por la confianza brindada, el apoyo incondicional ejemplo de honradez, perseverancia y lucha constante. Mis hermanas y hermanos: Ruth, Melanie, Edwin, Matias y Martin por sus ocurrencias, risas y momentos compartidos, a mis Abuelitos por sus palabras de apoyo que me han brindado día a día.

Mariela Sánchez

AGRADECIMIENTO

A padre Dios, Mamá, Papá, Hermano, Familia, Amigos, por su apoyo moral, cariño incondicional, que de una u otra manera siempre estuvieron al pendiente en mí, a mi compañera de Tesis Mary por su esfuerzo, trabajo, dedicación al realizar el proyecto de Titulación junto a mí, a la Universidad de las Fuerzas Armadas ESPE Extensión Latacunga, una institución prestigiosa y de calidad misma que me recibió con las puertas abiertas y me educo con grandes docentes e información adecuada, para lograr ser una gran profesional con conocimientos excelentes y un gran ser humano con valores y principios éticos.

Fernanda Gálvez

AGRADECIMIENTO

Por la fortaleza que me has dado Dios y me as cubierto con tu manto de protección, bendición y en los momentos más difíciles me has dado sabiduría.

A mi madre por acompañarme en esas noches de desvelo, brindarme su amor y protección, a mi padre que desde pequeña me inculco valores con los que me he formado y gracias a ellos ahora me he convertido en la persona que soy y me han ayudado a cumplir esta meta, a mis herman@s, abuelitos y demás familia que han contribuido para el logro de mi formación personal y profesional mil gracias.

A ti Fer Giss por ser esa amiga y compañera de tesis por la constancia, dedicación y el tiempo compartido juntas, mis amig@s por esos triunfos y derrotas compartidas en el transcurso de nuestra vida universitaria.

Mariela Sánchez

AGRADECIMIENTO

Agradecemos Infinitamente

Agradecemos al Eco. Francisco Caicedo por ser nuestra guía en la elaboración de nuestro trabajo de Titulación, por su tiempo y conocimientos, además de sus palabras de aliento y por ser parte de nuestra formación universitaria, Al Ing. Luis Lema por permitirnos formar parte de su Equipo de trabajo en su macro proyecto de investigación, y al Ing. Cristian Gallardo por su colaboración y ser partícipe en la elaboración de la presente investigación.

A todos y cada uno de nuestros docentes que nos impartieron sus conocimientos que han sido pilares fundamentales para nuestra formación Universitaria, al Ing. Julio Tapia por su apoyo y colaboración como guía en nuestra carrera y a la vez a la Universidad de las Fuerzas Armadas ESPE-L quien nos recibió y ahora entrega a dos mujeres con grandes conocimientos y valores capaces de afrontar situaciones de manera ética y con un espíritu solidario.

Fernanda y Mariela

ÍNDICE DE CONTENIDOS

CAPÍTULO II

2. MARCO REFERENCIAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente trabajo de investigación permitirá conocer un enfoque global sobre la inversión que realizan las empresas del sector industrial reguladas por la Superintendencia de Compañías, Valores y Seguros en software, equipos de cómputo, activos intangible a través del diagnóstico de los estados de situación financiera, además permite observar las tendencias mediante información histórica de cada una de las cuentas mencionadas, a continuación se presenta un análisis de los costos y beneficios que obtendrán estas industrias al implementar las herramientas de seguridad y protección de datos y cuán importante es su utilización. Para dar cumplimiento al propósito se desarrollaron cada uno de los capítulos los cuales contienen las generalidades de las Empresas del Sector Industrial reguladas por la Superintendencia de Compañías, Valores y Seguros, así como sus antecedentes, el área de influencia de la misma, también se detalla la problemática de investigación con su respectiva justificación e importancia, además contienen los objetivos y determinación de las variables de estudio. Posterior se presenta una visión general de la seguridad de la información, los conceptos principales necesarios para analizar y comprender la teoría, a través de las normas ISO 27001, 27002, Ley ecuatoriana de protección de datos, entre otros y mediante técnicas de investigación se realizó un estudio de campo el cual permitió conocer los controles de seguridad para resguardar la información que aplican cada una de las industrias, como propuesta de investigación se obtiene el catálogo de inversión en el cual constan las herramientas que las empresas del sector industrial podrán implementar a través de un proceso de mejora continua y por último se culmina con la elaboración de las conclusiones y recomendaciones como resultado de la investigación.

PALABRAS CLAVE:

- **SEGURIDAD DE INFORMACIÓN**
- **NORMA ISO 27002**
- **ANÁLISIS COSTO**
- **COTOPAXI-EMPRESAS INDUSTRIALES**

ABSTRACT

This research work will allow us to know a global approach on the investment carried out by the companies of the industrial sector regulated by the Superintendency of Companies, Securities and Insurance in software, computer equipment, intangible assets through the diagnosis of the states of financial situation, also allows to observe the tendencies by means of historical information of each one of the mentioned accounts, then presents an analysis of the costs and benefits that these industries will obtain to Implement the security and data protection tools and how important their use is. To fulfill the purpose, each of the chapters were developed which contain the generalities of the companies of the Industrial Sector regulated by the Superintendency of Companies, Securities and Insurance, as well as their antecedents, the area of Influence of the same, also details the problems of research with their respective justification and importance, also contain the objectives and determination of the variables of study. Later presents an overview of the information security, the main concepts necessary to analyze and understand the theory, through the Norms ISO 27001, 27002, Ecuadorian Law of data protection, among others and by means of techniques of research was conducted a field study which allowed to know the security controls to protect the information that apply each of the industries, as a research proposal is obtained the catalogue of investment in which the tools consist That the companies of the industrial sector will be able to implement through a process of continuous improvement and finally it is culminated with the elaboration of the conclusions and recommendations as a result of the investigation.

KEY WORDS

- **INFORMATION SECURITY**
- **STANDARD ISO 27002**
- **COST ANALYSIS**
- **COTOPAXI-INDUSTRIAL ENTERPRISES**

CAPÍTULO I

1. GENERALIDADES DE LA INVESTIGACIÓN

1.1. Tema de la Investigación

“Análisis del costo beneficio en las Empresas del Sector Industrial reguladas por la Superintendencia de Compañías que utilizan herramientas de Seguridad y Protección de datos en la provincia de Cotopaxi durante el período 2012-2016”

1.2. Área de influencia

1.2.1. Área de Intervención

Empresas de la Provincia de Cotopaxi.

1.2.2. Área de Influencia Directa

Empresas del Sector Industrial reguladas por la Superintendencia de Compañías, Valores y seguros en la Provincia de Cotopaxi.

1.2.3. Área de Influencia Indirecta

Las empresas de todos los sectores de la Provincia de Cotopaxi.

1.3. Antecedentes

Según Acosta (2015) en su investigación realizada para la obtención de su título menciona lo siguiente:

> Los sistemas de información conforman una parte fundamental de cada empresa, junto a los recursos de hardware y software, los datos que son almacenados y procesados en estos, necesitan estar protegidos de ataques, códigos maliciosos, vulnerabilidad en la web e incidentes como el robo de la información, los cuales han despertado en los últimos años la necesidad de preservar la información, siendo la seguridad un mecanismo que permite el óptimo funcionamiento de cada sistema evitando que haya fallas en los mismos como la pérdida de la información. (p.13)

Para el presente tema investigativo se analiza información proveniente de trabajo de campo, tesis, artículos científicos, base bibliográfica que aportarán

con conocimientos relacionados a la temática de estudio, los cuales se dan a conocer a continuación:

Hurtado Vanessa y Arias Patricio (2012), en su investigación establecen como tema de tesis el:

> Análisis costo/beneficio de la aplicación del estándar ISO/IEC 27001:2005 en una Empresa Industrial en la provincia de Pichincha, presentando como conclusiones que: La utilidad de la información y su valor en las organizaciones la convierten en un elemento que requiere ser asegurado y protegido de ataques, modificaciones indebidas, minimizando la afectación a su disponibilidad, integridad y confiabilidad. (p.117)
>
> El alineamiento entre el estándar ISO/IEC 27001:2005 y el costo beneficio para una empresa industrial, se fundamenta en cuatro fases integradas con la Evaluación de Riesgos que propone la Guía de Administración de Riesgos de Seguridad de Microsoft:
>
> - Visión general de la seguridad de la información en la empresa.
> - Recopilación de información sobre activos de información.
> - Evaluación de riesgo cualitativa y cuantitativa.
> - Análisis costo beneficio. (p. 121)

La información que manejan todas las empresas es de suma importancia y al ser revelada sin permiso puede ocasionar pérdidas además de truncar las actividades de un negocio por ello es necesario implementar medidas de seguridad contra ataques informáticos ya que actualmente toda la información se encuentra digitalizada y puede sufrir vulnerabilidades.

Según Pilco (2014) en su artículo científico sobre el tema:

> Estudio, análisis y comparación de tres herramientas para el salvaguardo de información establece similitudes de beneficios que tienen las herramientas, las cuales son:
>
> - Administrar respaldos de servidores a través de un agente que se configura e instala en cada servidor a respaldar.
> - Soportan el manejo de encriptación de datos desde la consola central y aplica a cada servidor.
> - Visualización de reportes acerca del estado de los medios de almacenamiento sean disco o cintas, estado de los respaldos,

clientes asociados a la herramienta y espacio utilizado total e individual.
- Facilidad de escalamiento acorde a necesidades del negocio y requerimientos que se presenten en el transcurso del tiempo.

En el mercado existen muchas herramientas que ayudan a proteger la información de las grandes industrias, las cual brindan un sin número de beneficios acorde las necesidades y al ser implementadas son de mucha ayuda porque disminuyen riesgos de pérdidas de datos de suma importancia.

Según Zapata (2014) en su trabajo presentado sobre Implementación del Modelo de Gestión de la seguridad de la Información aplicando ISO 27000 en la Empresa Coka Tours, Ambato-Ecuador menciona que:

> Las ventajas con la implementación de este Modelo de Seguridad de la Información es la mitigación de fuga de información que puede ocurrir, propiciando ahorro de costos y un impacto económico muy positivo para la empresa.
> No se tiene que invertir grandes cantidades de dinero en equipos (hardware) o software para la implementación disminuyendo considerablemente sus gastos, al definir el modelo la empresa mejoraría los procesos que actualmente lleva y no se requiere de contratar más empleados. Este ahorro de salario se mantendría como parte del continuo gasto que la empresa realiza por lo que los ahorros se entienden a un mayor plazo en el tiempo. (p. 107)

Se considera necesario la implementación de normas en la empresas ya que estas permiten que se realicen actividades basadas en un marco general de protección, en este caso la implementación del modelo de gestión de seguridad aplicando la ISO 27000 permitirá mitigar la fuga de información, para ello es necesario analizar cuál será la inversión y si la implementación traerá beneficios para la organización.

Según Robles (2015) en su trabajo de titulación sobre el: “Desarrollo de un modelo de seguridad para la prevención de pérdida de datos DLP, en empresas PYMES”.

> Presenta resultados tras el análisis costo-beneficio realizado, al mostrar la solución al cliente y mostrar que el beneficio económico de prevenir la pérdida de información en el lapso de un año y tres meses es positiva ya que en la disminución de los pagos generados por la fuga de información gracias a la implementación

> del sistema de prevención de pérdida de datos, la empresa tiene la ventaja de hacer inversiones en lo que está actualmente requiriendo sin la necesidad de que haya un problema de costo al momento de aumentar o disminuir los usuarios en la empresa. (p.113)

Claramente se observa que la implementación de herramientas de seguridad y protección de datos trae consigo un beneficio positivo para las organizaciones debido a que el costo de inversión se puede equilibrar con la disminución del personal, además que se previene la pérdida de información al ser propensas a ser atacadas por virus, espionajes industriales, accesos no autorizados, robos de información, evitando así poner en riesgo la confidencialidad que cada empresa posee.

1.4. Planteamiento del problema

1.4.1. Planteamiento del problema macro

Con la rápida evolución tecnológica, en estos tiempos las grandes ciudades muestran cómo va la intromisión de otras personas no autorizadas a los sistemas que utilizan las empresas con fin de acceder a la información reservada, tanto del personal, de la empresa y así también financiera. Por lo que es necesario que las industrias adopten herramientas de seguridad y protección de sus datos.

De la misma forma se visualiza en algunas partes del mundo el espionaje de datos en las industrias, según se muestran algunos casos Portaltic Europa Press (2017) :

- En China un caso reciente de espionaje en la industria tecnológica en el cual seis diseñadores de la marca Huawei vendieron información confidencial a LeEco, ambas compañías compiten con sus productos a precios muy bajos en el mercado estadounidense. La acusación de Huawei a LeEco se debe a dos patentes secretas: la primera el diseño de una antena y un reloj inteligente para niños, pero la empresa LeEco niega que haya existido dicho espionaje.
- Otro de los casos más conocidos y con más repercusión en medios fue el del espionaje en la Fórmula 1 del año 2007, cuando un ingeniero de Ferrari filtró documentos a la escudería británica McLaren.

Estos son los casos más sonados en el mundo, donde se ve que la información de datos requiere mayores niveles de seguridad. Además se dice que el espionaje ya no es solo económico sino también es político y militar, la misma que es sancionada, y al no contar con cifras exactas no se pueden realizar las denuncias respectivas de los delincuentes cibernéticos.

Según Excelsior (2011) otros de los casos conocidos en el mundo sobre el espionaje en las empresas industriales es en el cual:

> Se filtra la información es en las empresas automovilísticas como, el fabricante de automóviles francés Renault que dio inicio a una investigación judicial por espionaje industrial al presentar una demanda en la que alega corrupción, robo y encubrimiento. La empresa había suspendido a tres ejecutivos bajo sospecha, los cuales filtraron información importante sobre la tecnología de su automóvil eléctrico, en donde Francia ha calificado este caso como guerra económica.

1.4.2. Planteamiento del problema meso

La vulnerabilidad de los sistemas informáticos en América Latina se ha posicionado como la principal preocupación para varias industrias ya que se generan virus y códigos maliciosos con el fin de sustraer información relevante de las industrias afectando a las mismas. Mediante la utilización de correos electrónicos con archivos adjuntos o enlaces malintencionados con el que proceden a vulnerar los sistemas informáticos de las industrias para acceder a la información por parte de los cibercriminales.

> La firma Accenture establece que más de tres cuartas partes de las empresas creen que sus principales estrategias tienen la capacidad de evitar que existan interrupciones en sus servicios, así como la de proteger la información de sus compañías y su reputación, pero esto no es suficiente la falta de tecnología de análisis cibernético para monitorear ciberataques ha generado que una gran parte de las empresas en sectores como el de petróleo y gas no tengan una verdadera noción de cuándo o cómo podrían afectarles los ataques digitales. En Brasil, México o Argentina los niveles de seguridad industrial parecen estar despertando. Hernández (2017)

1.4.3. Planteamiento del problema micro

Según la Escuela Superior de Enseñanzas técnicas (ESET) (2016) en una encuesta realizada a varias industrias de países Latinoamericanos, (¿Qué incidentes de seguridad padecieron las empresas durante 2015?) al analizar los resultados, Ecuador con 51.9% se encuentra en el tercer lugar entre los más afectados con códigos maliciosos en el Malware; y con el Phishing, tiene una posición similar con un porcentaje de 24% ocasionando engaños y ataques a los sistemas de las industrias.

El proyecto se investigará en la provincia en la Cotopaxi al existir varias industrias, donde se puede dar a conocer las herramientas y seguridad de protección de datos siendo de gran apoyo los resultados obtenidos para evitar el robo de la información con lo que evitará los plagiadas, eliminación de datos, daños a la ruptura industrial, ataques financieros y personales.

Cabe mencionar, según fuente el Telégrafo (2016) que en las provincias de:

> “Guayas se encontraron 18 casos de delitos informáticos; Pichincha, 145; Manabí, 24; El Oro, 22; en el resto de provincias se registró una cantidad menor. La mayoría de denuncias (368) corresponde al delito de apropiación fraudulenta por medios electrónicos”.

Además una investigación realizada en el Ecuador por la Interpol, Policía Nacional, el centro de respuesta a Incidentes Informáticos de Ecuador (Ecucert), y con ayuda de los organismos de América Latina, establecen que el 85% de los ataques a los sistemas informáticos, es por negligencia de las personas que dejan abiertas las cuentas de los sistemas empresariales, de redes sociales, correos electrónicos lo cual genera vulnerabilidad a la información permitiendo que distintos usuarios no autorizados accedan a fuentes exclusivas de conocimiento personal. Fiscales mencionan que en Ecuador existen información cruzada sobre los conflictos de los casos de los delitos informáticos, por ello se ven en la necesidad de pedir asistencia penal internacional para recabar la información respectiva.

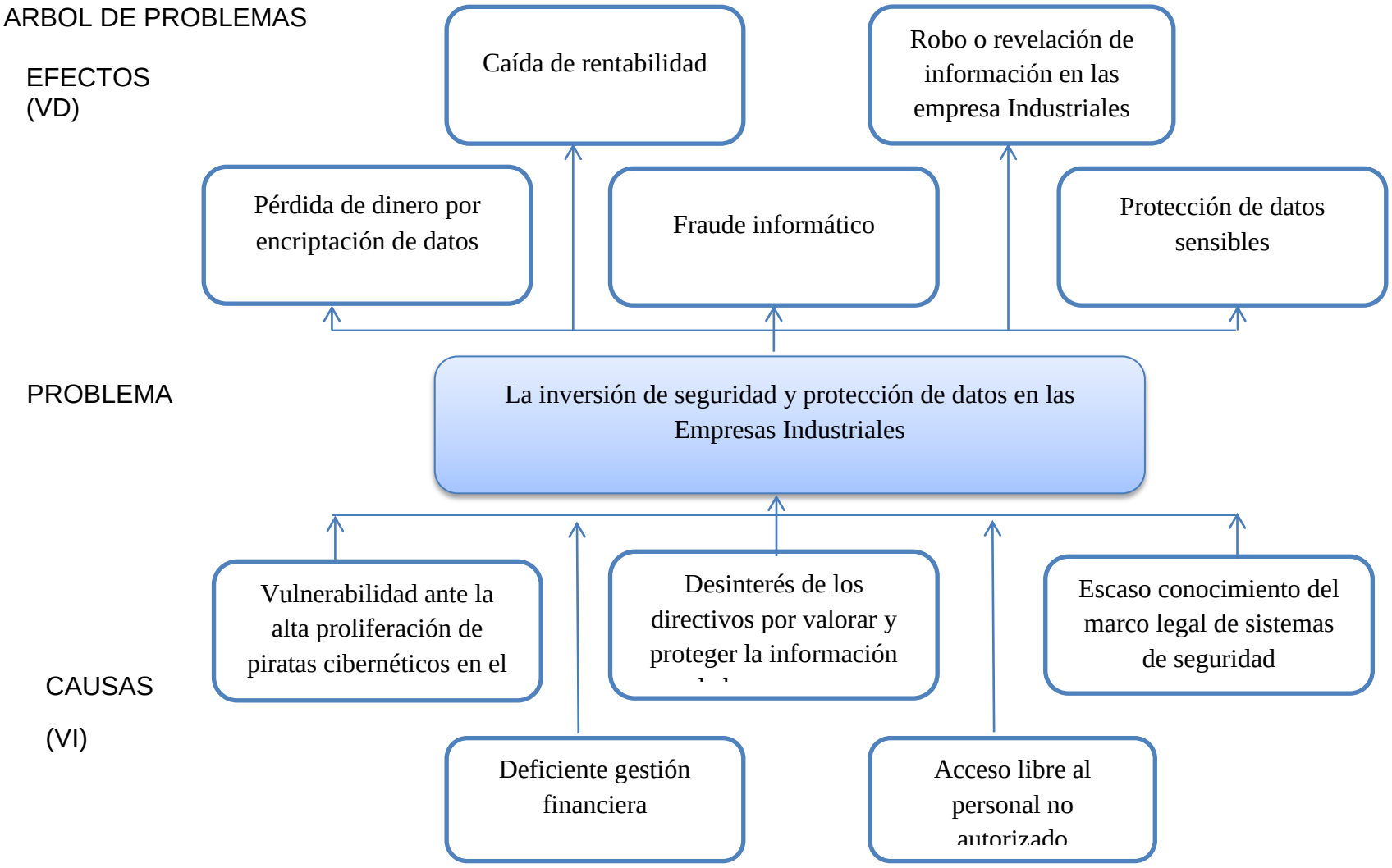

Figura 1. Árbol de problemas

1.5. Análisis crítico

El problema a ser investigado en las Empresas Industriales reguladas por la Superintendencia de Compañías, Valores y Seguros en la Provincia de Cotopaxi es: Inversión de Seguridad y protección de datos, del cual se ha podido realizar un minucioso análisis de la situación que atraviesan las empresas del sector Industrial.

Siendo una de ellas la vulnerabilidad ante la alta proliferación de piratas cibernéticos en el Ecuador, debido que es una de las causas que genera nuestra problemática empresarial lo que podría ocasionar una pérdida de dinero.

Sumado el desinterés de los directivos por valorar y proteger la información de las empresas, puede provocar en cualquier momento un fraude informático.

El escaso conocimiento del marco legal de sistemas de seguridad, atrae la inadecuada gestión de seguridad y protección de datos por lo tanto existe acceso libre de información al personal no autorizado en una organización industrial.

1.6. Formulación del Problema

¿Deficiente inversión en herramientas de seguridad y protección de información conlleva a pérdidas económicas?

1.7. Justificación e importancia

En el mundo globalizado en el cual las empresas se desenvuelven y contando con sistemas informáticos vulnerables en cualquier momento las organizaciones pueden perder información porque existen un sin número de herramientas que permiten a usuarios externos lograr tener acceso y llegar hasta la información que una empresa tiene protegida, esto sucede cuando los controles no están bien definidos, no los aplican de manera correcta y

ocasionan un peligro para la integridad, confidencialidad y disponibilidad en cada una de las empresas.

Es por ello que se ha visto la necesidad de investigar y analizar cuáles son las Herramientas de seguridad y protección de datos que necesitan las empresas del Sector Industrial reguladas por la Superintendencia de Compañías en la Provincia de Cotopaxi para minimizar el riesgo de robo de información, ataques de red o uso inadecuado de los datos.

Para lo cual se determinarán los costos en los cuales deberán incurrir las empresas para fortalecer la cultura de Seguridad Informática lo que permitirá optimizar la asignación de recursos, proteger la información, realizar copias de seguridad, garantizar la seguridad de los datos en tránsito y cifrado en los servidores.

Y al ser nuestra provincia un sector industrial estratégico necesariamente los Gerentes, junta administrativa y demás involucrados de la administración de las empresas deberán optar por invertir en implementaciones de sistemas de seguridad y protección de datos, así no se pondrá en riesgo el buen funcionamiento de las actividades productivas evitando pérdidas económicas que podrían afectar el desarrollo laboral de los empleados.

1.8. Objetivos Generales y específicos

1.8.1. Objetivo General

- Analizar el costo-beneficio de las Herramientas de Seguridad y Protección de Datos en las empresas del Sector Industrial reguladas por la Superintendencia de Compañías en la Provincia de Cotopaxi en el periodo 2012 - 2016.

1.8.2. Objetivos Específicos

- Determinar las empresas del sector industrial reguladas por la Superintendencia de Compañías que trabajan bajo el enfoque de buenas

prácticas tales como ISO, 27001, 27002, o la Ley Ecuatoriana y la perspectiva gerencial hacia la inversión en herramientas de seguridad y protección de Datos.

- Realizar un levantamiento de información sobre el costo de las Herramientas de Seguridad y Protección de Datos que podrían utilizar las empresas del sector industrial reguladas por la Superintendencia de Compañías.
- Determinar el beneficio marginal de la inversión que genera a las empresas del sector industrial reguladas por la Superintendencia de Compañías en la provincia de Cotopaxi al utilizar herramientas de seguridad y protección de datos.
- Construir un catálogo de inversiones en Herramientas de Seguridad y Protección de Datos para las empresas del Sector Industrial reguladas por la Superintendencia de Compañías.

CAPÍTULO II

2. MARCO REFERENCIAL

2.1. Marco Teórico

2.1.1. Seguridad de la Información

Resguardar la información existente en las empresas industriales para garantizar la integridad, confidencialidad, y disponibilidad de los datos registrados en el almacenamiento de la información donde se protegerá los recursos que poseen las entidades como son el software y programas de aplicación que tengan las mismas. Además la seguridad de información debe estar controlada porque en ella se encuentra las bases de los datos de cada uno de los usuarios que estén debidamente registrados en las plataformas, los estados financieros, antecedentes de la elaboración de productos, sistemas para la fabricación de bienes, incluso la información privilegiada.

INEN (2009) refiere que la información es un activo muy importante en el entorno de un negocio que esta interconectado, como resultado de la interconexión creciente la información se presenta a un sin número de amenazas y vulnerabilidades, es por ello que necesita la protección adecuada debido a que es necesario para que las organizaciones puedan desarrollar normalmente sus actividades.

2.1.2. Elementos de la seguridad de la Información

Identificación de todos los activos

Al conocer los activos en las empresas industriales lo principal es proteger de los daños, del uso inadecuado que pueden tener además de que el mismo sea sustraído por personas no autorizadas así evitar los daños y pérdidas económicas en las empresas. Al tener un conocimiento e identificados todos los activos que posee las empresas industriales se puede tomar la decisión de

protegerlos ya que el mismo contiene información de la empresa, de los empleados, además nuevos proyectos a desarrollarse.

Areito (2008) menciona lo que constituye en identificar los activos de una entidad:

> Son aquellos elementos relacionados con el entorno, como por ejemplo: el personal, los edificios, las instalaciones, los equipos, o los suministros, los relacionados con los sistemas de las TIC, como los equipos de hardware, el software, los componentes de comunicación de la entidad, los activos intangibles, como la imagen de la organización, credibilidad, licencias de software, entre otros. (p. 21)

Identificación de amenazas a los activos

Las amenazas están presentes en todo lugar y las empresas deberán identificar los puntos más importantes, como en la información de datos con el uso de las TIC´s, las cuales tendrán mayor resguardo para evitar el mal de uso de las mismas y que los ciberdelincuentes no puedan acceder a ellas.

> Una amenaza puede causar un incidente no deseado, la cual puede provocar daños o pérdidas de todo tipo en la organización. Estas pérdidas pueden proceder de un ataque directo sobre el sistema de información, las TIC, o los procedimientos manuales. (p.22)

Identificación de vulnerabilidades

Según Areito (2008) la vulnerabilidad con los activos tanto tangibles como intangibles de información se ven afectados en niveles físicos, personales, Software.

Identificación de riesgo

De acuerdo con Areito (2008) la identificación de los riesgos trata de reconocer los peligros que puede tener la empresa tanto en la vulnerabilidad de los activos donde conste la información informática “Es aquel en el que una amenaza concreta o un grupo de amenazas, pueden explorar una

vulnerabilidad o grupo de vulnerabilidades determinado, exponiendo los activos a daños o pérdidas” (p.24).

Aplicación de salvaguardas

Para las empresas es muy importante implementar herramientas que puedan resguardar la información y datos restringidos, a más de ello la protección de los equipos, lo que permitirá reducir la vulnerabilidad, limitar el impacto de un incidente no deseado y facilitar la recuperación de información Areito (2008).

2.1.3. Importancia de la Seguridad de la Información

La seguridad de la información es de suma importancia para los negocios del sector público como del privado ya que protege la infraestructura crítica en las distintas organizaciones permitiendo un mayor desempeño en los procesos que se realizan cada una de las entidades, además se lleva un control de las actividades, un seguimiento del cumplimiento del resguardo de la información, cumplimiento de políticas de seguridad de la información.

> Según INEN (2009), La información, los procesos, sistemas y redes que la soportan son activos importantes para un negocio. La definición, el logro, el mantenimiento y la mejora de la seguridad de la información pueden ser esenciales para mantener su competitividad, el flujo de caja, la rentabilidad, el cumplimiento legal y la imagen comercial. (p.7)

2.1.4. Evaluación de los riesgos de la seguridad

Los riesgos de seguridad deben ser evaluados, por lo cual el INEN (2009) señala:

> Que los requisitos de la seguridad se identifican mediante una evaluación de los riesgos de la seguridad, para ello los gastos en los controles se deben equilibrar frente a la probabilidad de daño para el negocio que resulta de las fallas en la seguridad, estimando los costos en los cuales incurrió la empresa por pérdidas.,

Es necesario que se efectúen evaluaciones para el control de las actividades que realizan los negocios, lo que permitirá que las organizaciones logren

minimizar riesgos a través de una adecuada gestión que servirá para proteger información tecnológica.

2.1.5. Sistema de Gestión de la Seguridad de la Información

La norma ISO 27000 (2005) establece que la información es un conjunto de datos organizados que posean un valor a cargo de las entidades, independientemente de cómo se guarde o transmita ya sea impresa en papel o almacenada electrónicamente ya sea información creada por la propia organización o de fuentes externas, por ello la seguridad de la información radica en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento dentro de una organización, constituyendo la base sobre la que se cimienta la seguridad de la información: Confidencialidad, Integridad, Disponibilidad.

2.1.6. Para que sirve un SGSI

Según ISO 27000 (2005) El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a las empresas a establecer políticas y procedimientos relacionados con los objetivos del negocio, para mantener un nivel de exposición menor al nivel de riesgo que las empresas deciden asumir, a través de este sistema las empresas conocen los riesgos a los cuales está sometida su información y los asumen, minimizan y controlan mediante una sistemática, documentada y conocida por todo lo que se revisa y mejora constantemente.

2.1.7. Las Tareas que tiene la Gerencia en un SGSI

La dirección cumple un rol importante para una implantación exitosa de un Sistema de Gestión de Seguridad de la Información en las organizaciones, debido a que esta afecta fundamentalmente a la gestión del negocio y requiere por tanto que Gerentes de las empresas tomen decisiones y acciones.

Algunas de las tareas fundamentales del SGSI que ISO (2005) asigna a la dirección se detallan en los siguientes puntos:

- Establecer una política de seguridad de la información.
- Asegurarse de que se establecen objetivos y planes del SGSI.
- Establecer roles y responsabilidades de seguridad de la información.
- Comunicar a la organización tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.

La dirección deberá garantizar que los procedimientos de seguridad de la información apoyan los requerimientos de negocio además implementar, revisar, operar, mantener y mejorar el SGSI para ello se deberá identificar y tratar todos los requerimientos legales y normativos.

2.1.8. Requisitos de Seguridad

INEN (2009) establece que es esencial que las organizaciones identifiquen los requisitos de seguridad con los cuales cuentan, a continuación se presentan tres fuentes principales de requisitos de la seguridad:

- Una fuente se deriva de una evaluación de los riesgos para la organización, teniendo en cuenta estrategias y los objetivos globales del negocio a través de una evaluación de riesgos, se identifican las amenazas para los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se estima el impacto potencial.
- Otra fuente son los requisitos legales, estatutarios, reglamentarios y contractuales que debe cumplir la organización, sus socios comerciales, los contratistas y los proveedores de servicios, así como su entorno socio-cultural.
- Una fuente adicional es el conjunto particular de principios, objetivos y requisitos del negocio para el procesamiento de la información que la organización ha desarrollado para apoyar todas las operaciones.(p. 7)

2.1.9. Criterios de vulnerabilidad

Ibídem, los siguientes criterios de vulnerabilidad se aplican a todas las redes identificadas y elementos de red en el ámbito de la valoración:

- Alta Vulnerabilidad: es probable su explotación, la detección es difícil y son costosos la corrección de los fallos.
- Vulnerabilidad media: Es posible que ocurra la explotación y detección y la corrección puede ser costosa.
- Baja Vulnerabilidad: Es posible su explotación y detección y los costes de corrección son mínimos.
- Vulnerabilidad mínima: la explotación no es probable, la detección es probable y los costes de corrección son mínimos.(p. 80)

2.1.10. Identificación de vulnerabilidades

Según Areitio (2008) en su libro sobre la seguridad de la información, redes e informática establece que:

> Una vulnerabilidad puede entenderse también como la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo y provocan debilidades en los sistemas que pueden explotarse dando lugar a consecuencias no deseadas. Las vulnerabilidades asociadas a los activos, incluyen las debilidades en el nivel físico sobre la organización, los procedimientos, el personal, la gestión, la administración, los equipos, el software o la información. (p.23)

Puedo mencionar que los activos de las empresas en este caso la información puede ser vulnerable cuando no se encuentra protegida, debilitando los negocios e interrumpiendo las actividades cotidianas, además al tener un sistema vulnerable las organizaciones son propensas a tener pérdidas económicas significativas.

2.1.11. Delito Informático

Según González y Quintana (2004) La definición de Jijena Leiva, menciona que el delito informático es: “Toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma”(p.582).

2.1.12. Estándar ISO 27001- Sistema de Gestión de la Seguridad de la Información.

Según Gesconsultor (2017) “La Información es un activo fundamental para el desarrollo, operativa, control y gestión de un Negocio y se ha convertido en una prioridad en los entornos globalizados actuales donde las transacciones de negocio y servicio utilizan tecnologías”.

La implementación de las Normas a más de aportar a la organización con certificaciones reconocidas implanta fundamentalmente una cultura y práctica de seguridad de la información aportando valores al negocio como: Mejora de la competitividad, la imagen corporativa, cumplimiento legal y reglamentario, optimización de recursos e inversión en tecnología, por lo tanto la reducción de costes protegiendo de esta manera y dando continuidad al negocio.

Esta norma es una solución de mejora continua que permite evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización, además de establecer controles y estrategias más adecuadas para minimizar los peligros. La norma ayuda a proteger la información asegurando la confidencialidad cuando esta es accesible sólo para las personas autorizadas a tener acceso, garantiza la disponibilidad en el cual los usuarios autorizados tengan acceso a la información y los activos relacionados cuando lo necesiten, la norma sigue el enfoque hacia la seguridad de la información (ISOTools, 2016).

2.1.13. Estándar ISO 27002:2013 - Controles de Seguridad

Tabla 1

Controles de Seguridad

DOMINIOS	OBJETIVOS
POLÍTICAS	“Dirigir y dar soporte a la gestión de la seguridad de la información en concordancia

CONTINÚA

	con los requerimientos del negocio, las leyes y las regulaciones".
ORGANIZACIÓN	"Establecer la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades en una empresa".
RECURSOS HUMANOS	"Asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios".
ACTIVOS	"Identificar los activos en la empresa y definir las responsabilidades para una protección adecuada".
ACCESOS	"Controlar los accesos a la información y las instalaciones utilizadas para su procesamiento".
CIFRADO	"Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información".
FÍSICA Y AMBIENTAL	"Evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información". Evitar la pérdida, los daños, el robo o el compromiso de activos y la interrupción a las operaciones de la organización.

CONTINÚA

OPERATIVAS	"Evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información".
TELECOMUNICACIONES	"Asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte".
ADQ., DES. Y MANTTO	Asegurar la inclusión de controles de seguridad y validación de datos en la compra y el desarrollo de los sistemas de información.
SUMINISTRADORES	"Implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea con los acuerdos de entrega de servicios de terceros".
INCIDENTES	Los acontecimientos de seguridad de la información y las debilidades asociados a los sistemas de información deben ser comunicados para aplicar acciones correctivas en un tiempo oportuno.
CONTINUIDAD NEGOCIO	"Preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad".
CUMPLIMIENTO	Es cumplir con "disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la organización y/o a los empleados que incurran en responsabilidad civil o penal como resultado de incumplimientos".

Fuente: (ISO 27002, 2013)

2.1.14. Ley de protección a la Intimidad y Protección de Datos

Según Asamblea Nacional (2016) Tiene por objeto proteger y garantizar el derecho de todas las personas a la intimidad y privacidad en el tratamiento de datos personales que se encuentren en bases o bancos de datos, ficheros, archivos, en forma física o digital, en instancias públicas o privadas.

> El titular de los datos personales tendrá el derecho de conocer, actualizar y rectificar sus datos personales frente a los responsables o encargados del tratamiento, acceder en forma gratuita a sus datos personales que han sido objeto de tratamiento en instancias públicas y privadas. (p.8)

2.1.15. Empresa

> Según García y Casanueva (2014) “Entidad que mediante la organización de elementos humanos, materiales, técnicos y financieros proporciona bienes o servicios a cambio de un precio que le permite la reposición de los recursos empleados y la consecución de unos objetivos determinados” (p. 3).

Esta definición muestra que una empresa abarca la administración del personal, los insumos a ser adquiridos, la parte financiera los cuales permitirán el desarrollo de una producción adecuada que será destina a la venta para que através de ingresos esta pueda continuar con sus actividades.

Según Estallo y Fuente (2007) Desde el punto de vista instrumental se considera a:

> La empresa desde una perspectiva integral que la estudia como unidad donde se mezclan no solo fenómenos económicos, sino otros subsistemas económicos sociales mas amplios. Con esta interpretación se quiere destacar el hecho de que la empresa es un sistema social, o sea, un fenómeno de la sociedad (p. 29).
> Como organización: se define la empresa como un conjunto de medios humanos y materiales que se disponen para conseguir una finalidad a través de un esquema determinado de relaciones y dependencias entre los diferentes elementos que la componen(p. 30).

Estos autores definen a la empresa como el conjunto de actividades que se realizan en la cual están inmersas muchas personas como son clientes,

proveedores y los empleados o colaboradores que la integran dando énfasis a los seres humanos y materiales para la creación de una empresa.

2.1.16. Clasificación De Las Empresas

Según INEC (2014) el Manual de Usuario de la Clasificación Industrial Internacional Uniforme (CIIU) en el cual las unidades de producción dentro de un sector de la economía se encuentran de la siguiente manera:

Tamaño de la Empresa: Se establece según el volumen de ventas (v) anual y el número de colaboradores o empleados (P) .

- Grande: V$5’000.001 en adelante. P: 200 en adelante
- Mediana”B”: V $2’000.001 a $5’000.000. P: 100 a 199
- Mediana “A”V $1’000.001 a $ 2’000.000. P: 50 a 99
- Pequeña: V$100.001 a 1’000.000. P: 10 a 49
- Microempresa: V < a $100.000. P: 1 a 9

Rama de Actividad

- CIIU: Constituye una estructura de clasificación coherente y consistente de todas las actividades económicas que realizan cada una de las empresas y fue emitida por la Organización de Naciones Unidas (ONU), desarrollada a través del conjunto de conceptos, principios y normas de clasificación.
- CIIU Sección: A. Agricultura B. Minas y canteras C. Manufacturas D. Suministro energías E. Distribución de Agua F. Construcción G. Comercio H. Transporte I. Alojamiento J. Información K. Financieras L. inmobiliaria M. Científico Técnico N. Administrativos O. Administración pública P. Enseñanza Q. Salud humana R. Arte S. otros servicios

Sector Económico: Se refiere a la agrupación de las actividades económicas mediante secciones, permitiendo simplificar la estructura sectorial de una economía.

- Agricultura, ganadería, silvicultura y pesca.
- Explotación de minas y canteras.
- Industrias manufactureras.
- Comercio
- Construcción
- Servicios

> Tipo de Unidad Legal: Lo constituyen personas naturales o jurídicas y este tipo de unidad legal con las particularidades jurídicas de cada organización puede derivarse en otra formas que el Directorio de Empresas denomina forma institucional la cual es una sub-clasificación de la unidad legal de las empresas e instituciones de acuerdo a sus características jurídicas.

2.1.17. La información como recurso estratégico

> Según Heredero y López (2011) El reconocimiento de la información como recurso estratégico, así como la aceptación de las tecnologías de la información y de las comunicaciones como recurso vital para la empresa, hacen imprescindible que la misma sea analizada y transformada de forma adecuada a través de los sistemas de información. Dicho proceso es crucial para el logro y sostenimiento de cualquier estrategia competitiva. (p. 22)

Distintos autores mencionan que la información como recurso estratégico puede ser considerada en dos dimensiones, la primera de explotación la cúal se asocia a disponer de información sobre el entorno antes que los competidores, la segunda dimensión disponer de nuevas armas competitivas a partir del desarrollo y aprovechamiento de la información interna y su transformación en el conocimiento de la organización.

2.1.18. Toma de decisiones Gerenciales

Según Sallenave (2012) la toma de decisiones es de suma importancia para una organización por ello la define como:

> La selección de un curso de acción entre varias opciones, también como la selección racional de un curso de acción.
> Aunque se ha señalado que una de las principales funciones del gerente o administrador es la toma de decisiones, la importancia de esta función trasciende de la empresa: los funcionarios del gobierno que no necesariamente tiene una mentalidad gerencial o se han preparado para administrar, las toman continuamente.
> Se requiere de tres condiciones para tomar decisiones:
>
> - Insatisfacción con la situación actual (resolver un problema)
> - Motivación para desear cambiar la situación (aprovechar una oportunidad)

- Capacidad de cambiar la situación, es decir vencer las amenazas.(p. 28)

Claramente se observa que un gerente para tomar decisiones primero debe identificar un problema o acción, procede a su reconocimiento a continuación se analiza posibles alternativas y sus consecuencias, deberá seleccionar la solución e implementarla, para ello es necesario una retroalimentación.

2.1.19. Inversión

Según Pareja (2014) existen decisiones que las organizaciones deben tomar en este caso las inversiones la cual se define:

> Como el compromiso actual de recursos con el objetivo de obtener más tarde algunos beneficios. El análisis de inversiones es el proceso de examen de alternativas y de decisión sobre qué alternativa es preferida. A diferencia de otros problemas de elección similares, el análisis de inversiones se da dentro del marco de los mercados financieros, que simplifican la toma de decisiones a través del principio de comparación.(p. 1)

En la actualidad los negocios cada vez se actualizan de manera tecnológica por lo cual es de suma importancia que las empresas inviertan en sistemas de seguridad para proteger la información que generan, para ello deberán analizar cual será el beneficio que la inversión presentará a más de observar cuales son sus posibles ofertantes.

2.1.20. Beneficios de la aplicación del estándar ISO/IEC 27001

Según Molina y Cruz (2012), Los beneficios más relevantes de certificarse y cumplir con la ISO/IEC 27001 están:

- Mejora y formaliza a la gestión de la seguridad de la información en una empresa en base de procesos que forman un ciclo de vida metódico y controlado en lugar de la compra sistemática de productos y tecnologías, involucrando y comprometiendo a la alta gerencia como propietaria de esta responsabilidad.
- Partiendo de la evaluación de riesgos que imparte la norma hasta la implementación de controles, se facilita la continuidad de las operaciones de negocio tras incidentes de gravedad que atentan a la información de la empresa (errores, sabotajes o desastres).

- Establece objetivos de seguridad y calidad medibles para la evaluación de su éxito y ofrece un criterio de mejora continua de los mismos.
- Proporciona un enfoque en las responsabilidades y aumento de la motivación y satisfacción del personal.
- Ofrece confianza para socios comerciales, accionistas y clientes al demostrar el compromiso de la empresa con la seguridad de la información frente a terceros (la certificación demuestra el principio de la debida diligencia), mejorando su imagen, credibilidad y diferenciación en el mercado.(p. 36)

Al estar una empresa certificada por una normativa muestra credibilidad y confianza a la vez que otorga beneficios porque los procesos se van mejorando y presentan resultados aceptables para los accionistas y demás colaboradores en las organizaciones.

2.1.21. Costo de implementación del estándar ISO/IEC 27001

> Según el experto en la norma ISO/IEC 27001, Dejan Kosutic, el costo de implementación de la ISO/IEC 27001 es una de las primeras preguntas que se hacen los potenciales clientes, sin embargo no es posible proporcionar una cifra exacta ya que ante todo el costo total de la implementación depende del tamaño de la empresa o de las áreas que se encuentren dentro del alcance de la norma. (p.42)

La tecnología que utilizan varias empresas se encuentran con un sistema legal donde el mismos controla y guarda la confidencialidad y protección de la información propia de las empresas, entre ellas esta las empresas del sector industrial, la cual debe tener un costo adicional para tener controlada su información en la cual los siguientes costos son:

- Costo de publicaciones y de capacitación
- Costo de asistencia externa
- Costo de tecnología
- Costo del tiempo de los empleados

2.1.22. Retorno de la Inversión de la seguridad informática

Según Andrés Velásquez (2017), menciona lo siguiente:

> Retorno de inversión en seguridad, llamado “ROSI” por sus siglas en inglés: Return of Security Investment. Donde se define el ROSI como

> “el gasto directo que una compañía realiza para poder implementar una seguridad deseable contra el costo de una falla de seguridad”.

2.2. Base conceptual

2.2.1. WannaCry

Según BBC Mundo (2017) WannaCry parece haber sido creado para explotar un fallo detectado por la Agencia Nacional de Seguridad de EE.UU. (NSA, por sus siglas en inglés).

> Cuando se filtraron detalles del error, muchos investigadores de seguridad predijeron que esto llevaría a la creación de gusanos de ransomware automáticos.
> Es un virus informático que bloquea datos y demanda un pago de hasta US$600 en bitcoins antes de restaurar los archivos cifrados.
> A diferencia de muchos otros programas maliciosos, WannaCry tiene la capacidad de moverse por una red por sí mismo. La mayoría de los otros gusanos necesitan la actividad humana para expandirse: intentan engañar a la víctima potencial para que abra un documento adjunto que alberga el código de ataque.
> Por contraste, una vez que WannaCry está dentro de una organización, rastreará las máquinas vulnerables y las infectará también. Su impacto fue tan público porque grandes cantidades de máquinas en cada organización atacada quedaron en situación de vulnerabilidad.

Una forma de ataque a la información reservada de la empresa es por este medio de gusanos como lo suelen llamar, ya que realiza una intromisión en los datos con la intención maliciosa de los ciberdelincuentes y ser de su interés la información.

2.2.2. Ransomware

Este sistema que amenaza con la eliminación de la información de los datos informáticos de las empresas, es preocupante ya que no solo los elimina sino también restringe al ingresar a los sistemas, donde los Hackers realizan esta fechoría con el fin de pedir una recompensa para la recuperación de la información.

> También conocido como rogueware o scareware restringe el acceso a su sistema y exige el pago de un rescate para eliminar la restricción,

> es creado por estafadores con un gran conocimiento en programación informática. Puede entrar en la PC mediante un adjunto de correo electrónico o a través del navegador si se visita páginas web infectadas con este tipo de malware, o acceder por una red. (Avast)

2.2.3. Delitos tecnológicos más comunes.

Pishing

Los delitos informáticos como es Pishing donde se comete un fraude al roba información discreta de las empresas, ocultándose con mensaje y páginas de empresas inexistentes para realizar la respectiva intromisión en los datos informáticos.

> Guerrero (2012), El método más común consiste en la recepción de mensajes de correo falsos, de diversas entidades bancarias, de las que, usted puede o no ser cliente, donde se le solicita por distintos motivos que facilite sus datos, así como que introduzca su código PIN. Para ello, suplantan de manera impecable la identidad de las entidades bancarias reales y sus correos oficiales, logrando de este modo confundir/engañar a la víctima y que está facilite los datos solicitados (p. 23).

Pharming

Este sabotaje informático causa daños en los sistemas y herramientas de información de las empresas, así mismo como el resto de programas es difícil la respectiva denuncia por lo que lo detectan a tiempo y se desconoce con el paradero de los ciberdelincientes.

> Guerrero (2012) Esta es una variante del Phising, cuyos objetivos es el robo de identidad y la obtención de los datos bancarios del afectado, Básicamente consiste en la manipulación del servicio de servidores de nombres (DNS), de tal manera, que cuando el afectado teclea en la barra de direcciones de su navegador la dirección web de su entidad bancaria, el sistema le digiere a otra exactamente igual, pero completamente falsa.

Esto se consigue de dos maneras:

- Introduciendo software malicioso en el ordenador del usuario, que modifica el archivo hots, este archivo es el responsable de guardar la correspondencia entre los nombres de dominio

- Atacando a las máquinas en internet cuya función es la de servidores de dominio, de este modo una gran cantidad de usuarios se vería afectado (p. 31).

2.3. Marco Legal

2.3.1. Constitución de la República del Ecuador 2008

Según Asamblea Nacional (2008) la ley se menciona algunos punto importantes en las secciones quinta y sexta

> Acción de hábeas data Art. 92.- Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico.
> Acción por incumplimiento Art. 93.- La acción por incumplimiento tendrá por objeto garantizar la aplicación de las normas que integran el sistema jurídico, así como el cumplimiento de sentencias o informes de organismos internacionales de derechos humanos, cuando la norma o decisión cuyo cumplimiento se persigue contenga una obligación de hacer o no hacer clara, expresa y exigible. La acción se interpondrá ante la Corte Constitucional. (p.40)

2.3.2. Ley orgánica de transparencia y acceso a la información pública

Según El Congreso Nacional en la Ley (2004) garantiza el derecho a acceder a las fuentes de información, donde se menciona los mecanismos para ejercer la participación democrática respecto del manejo público y la rendición de cuentas; información confidencial está excluida del principio de publicidad, que debe ser declarado como tal.

> Art. 6.- Información Confidencial.- Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República. El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes. (p.4)

2.3.3. Ley de Sistema Nacional de Registro de Datos Públicos

De acuerdo la ley de Sistema Nacional de Registro de Datos Públicos (2013) tiene la finalidad de proteger los derechos constituidos, y da a conocer algunos puntos las cuales regula:

- Los mensajes de datos
- La firma electrónica
- Los servicios de certificación
- La contratación electrónica y telemática
- La presentación de servicios eléctricos
- La protección a los usuarios y datos de los sistemas

Art. 9.- De las certificaciones.- “La certificación registral, constituye documento público y se expedirá a petición de la interesada o interesado, por disposición administrativa u orden judicial”. (p. 2)

2.3.4. Proyecto de Ley de Protección a la Intimidad y Protección de Datos

Nuevo proyecto de ley

A través de las Superintendencia de Telecomunicaciones prepara la nueva ley donde su objetivo es proteger y garantizar el derecho de todas las personas a la intimidad y privacidad de la misma donde se encuentren en los datos personales estén en bases o bancos de datos, ficheros, archivos, y sea de forma física y digital en instancia pública o privada.

Plan Nacional Del Buen Vivir

El presente proyecto está alineado al objetivo 11 del Plan del buen vivir en el cual establece el Consejo Nacional de Planificación (2013), asegurar la soberanía y eficiencia de los sectores estratégicos para la transformación industrial y tecnológica:

> El Ecuador tiene la oportunidad histórica para ejercer soberanamente la gestión económica, industrial y científica, de sus sectores estratégicos. Esto permitirá generar riqueza y elevar en forma general el nivel de vida de nuestra población, convertir la gestión de los sectores estratégicos en la punta de lanza de la transformación tecnológica e industrial del país, constituye un elemento central de ruptura con el pasado. (p. 387)

2.4. Sistema de Variables

2.4.1. Definición Nominal

Variable Dependiente (VD): Incremento del beneficio dentro de las organizaciones del sector industrial reguladas por la Superintendencia de Compañías en Seguridad y Protección de datos.

Variable Independiente(VI): Inversión en la aplicación de Herramientas de Seguridad de Información en las organizaciones del sector industrial reguladas por la Superintendencia de Compañías.

2.4.2. Cuadro de Operacionalización de Variables

Tabla 2

Cuadro de operacionalización de Variables

OBJETIVOS ESPECÍFICOS	VARIABLE	DIMENSIÓN	INDICADORES	INSTRUMENTOS
Determinar las empresas del sector industrial reguladas por la Superintendencia de Compañías, que trabajan bajo el enfoque de buenas prácticas tales como ISO 27001, 27002, o la Ley Ecuatoriana y la perspectiva gerencial hacia la inversión en herramientas de seguridad y protección de Datos.	Incremento del beneficio dentro de las organizaciones del sector industrial reguladas por la Superintendencia Compañías en Seguridad y Protección de datos	Normativas ISO	ISO27001 ISO27002- Controles de Seguridad Valor absoluto – Valor relativo	Políticas Seguridad Aspectos Organizativos SI Seguridad Ligada a los recursos humanos Gestión Activos Control de Accesos Cifrado Seguridad física Seguridad en la Operativa Seguridad en las Telecomunicaciones Adquisición, desarrollo y Mantenimiento de los sistemas de información Seguridad de la información en las relaciones con suministradores Gestión de Incidentes Aspectos de la SI en la Gestión de la Continuidad de Negocio Cumplimiento Análisis Horizontal

CONTINÚA

Realizar un levantamiento de información sobre el costo de las Herramientas de Seguridad y Protección de Datos que podrían utilizar las empresas del sector industrial reguladas por la Superintendencia de Compañías.	Inversión en la aplicación de Herramientas de Seguridad de Información en las organizaciones del sector industrial reguladas por la Superintendencia de Compañías.	Costo de las Herramientas de Seguridad y Protección de Datos.	Precios Variedad de Herramientas	Oferta de las Herramientas para la Seguridad de la Información, protección de datos Encuesta
Determinar el beneficio marginal de la inversión que genera a las empresas del sector industrial reguladas por la Superintendencia de Compañías en la provincia de Cotopaxi al utilizar herramientas de seguridad y protección de datos.		Beneficio Marginal	Tiempo Costos Beneficios ROSI	Encuesta
Construir un Catálogo de inversiones en Herramientas de Seguridad y Protección de Datos para las empresas del Sector Industrial reguladas por la Superintendencia de Compañías.		Inversión	Herramientas Beneficios Costos de las herramientas	Catálogo de Inversión

2.4.3. Hipótesis

(H1)= La inversión en herramientas de seguridad y protección de datos genera un beneficio a las organizaciones del sector industrial reguladas por la Superintendencia de Compañías.

(H0)= La inversión en herramientas de seguridad y protección de datos no genera un beneficio a las organizaciones del sector industrial reguladas por la Superintendencia de Compañías.

CAPÍTULO III

3. METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Modalidad de la investigación

Según Arango como se citó en (Chávez, 2015), establece que la investigación:

> Es un procedimiento científico desarrollado por el hombre para la construcción de nuevos conocimientos, con el fin de poner esté al servicio de la sociedad, debe ir encausado a la búsqueda de resolver problemas y de explicar y/o fundamentar ciertos fenómenos. (p.17)

La investigación permite descubrir hechos analizados de un problema de estudio mediante la búsqueda sistematizada de conocimientos y recolección de datos, revisando información de distintas fuentes que ayudarán a comprobar una hipótesis que ha sido planteada, permitiendo así que el investigador pueda establecer soluciones, de acuerdo con su alcance se clasifica en:

3.1.1. Investigación pura o teórica

(Kerlinger, 2017) “Se interesa en el descubrimiento de las leyes que rigen el comportamiento de ciertos fenómenos o eventos; intenta encontrar los principios generales que gobiernan los diversos fenómenos en los que el investigador se encuentra interesado” (p.16). Además esta investigación se desarrolla sin el propósito de una aplicación inmediata, aportar elementos teóricos al conocimiento científico, sin la intención de su demostración directa e inmediata.

3.1.2. Investigación aplicada

(Chávez, 2015) Cita al autor Arango Quintero quien establece que la investigación “se determina aplicada porque busca el uso de los conocimientos que se obtienen. En la investigación aplicada o empírica, lo que le concierne al investigador, primordialmente, son los resultados obtenidos” (p.17). Esto

permitirá encontrar soluciones que darán respuesta a interrogantes de una problemática.

3.1.3. Investigación teórico-práctico

Según Arango Quintero como se citó en (Chávez, 2015) esta investigación "consiste en buscar la causa y efecto de ciertos fenómenos, para poder así determinar un conjunto determinado de principios y generalidades del fenómeno" (p.17). Esta investigación radica en que busca en todo momento establecer una estrecha relación entre los conceptos teóricos que sustentan el conocimiento.

La modalidad de investigación que se usará en el desarrollo del tema a tratar es la aplicada debido a que esta permitirá poner en práctica la información consultada en distintas fuentes, ideando la mejor forma de aplicarlo en el sector a ser estudiado lo cual generará el desarrollo de los objetivos propuestos.

3.2. Alcances de la investigación

3.2.1. Investigación exploratoria

Es aquella que antecede a todas las investigaciones por ello Hernández, Fernández y Baptista (2014) establecen que:

> Se realiza cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes. Es decir, cuando la revisión de la literatura reveló que tan sólo hay guías no investigadas e ideas vagamente relacionadas con el problema de estudio, o bien, si deseamos indagar sobre temas y áreas desde nuevas perspectivas. (p.91)

Esta investigación se emplea cuando existen pocas indagaciones y fuentes relacionadas al caso de estudio o a su vez este es novedoso, por ello como su nombre lo dice lo primero que un investigador debe hacer es explorar para que de esta manera pueda obtener información completa y certera.

3.2.2. Investigación descriptiva

Hernández et al. (2014) Menciona que “Únicamente pretenden medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refieren (…)” (p.92). Es decir el investigador describirá las características, sucesos, datos, resultados y deberá tener la capacidad de identificar las variables sobre las cuales se recolectara la información.

3.2.3. Investigación Correlacional

La investigación Correlacional según Hernández et al. (2014) Establece que:

> Este tipo de estudios tiene como finalidad conocer la relación o grado de asociación que exista entre dos o más conceptos, categorías o variables en una muestra o contexto en particular. En ocasiones sólo se analiza la relación entre dos variables, pero con frecuencia se ubican en el estudio vínculos entre tres, cuatro o más variables. (p.93)

El estudio está direccionado a determinar la relación que puede existir entre las variables de investigación, una vez evaluado el grado de vinculación entre estas se podrá conocer su comportamiento en distintos escenarios prediciendo un valor aproximado para los casos de estudio.

3.2.4. Investigación Explicativa

Según Hernández et al. (2014) “Como su nombre lo indica, su interés se centra en explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta o por qué se relacionan dos o más variables” (p.95). La investigación detalla las causas, razones del porqué suceden los distintos eventos permitiendo generar un entendimiento para el investigador.

La presente investigación se caracteriza básicamente por ser exploratoria y, descriptiva. Exploratoria porqué existen pocas indagaciones en investigaciones previas relacionadas al análisis del Costo-Beneficio en las empresas del sector Industrial que utilizan herramientas de seguridad de información y protección de datos. Se aplicará la investigación descriptiva porqué se determinará las

empresas del sector industrial reguladas por la Superintendencia de Compañías de acuerdo a su tamaño, tecnología, utilidad y a través de la aplicación de técnicas de recolección de información se podrá visualizar los montos de inversión que realizan las empresas para las herramientas de seguridad de información y protección de datos a más de ello los controles que aplican de la ISO 27002:2013.

3.3. Metodología de la investigación

En la presente investigación se utilizará los siguientes métodos:

Método Inductivo

De acuerdo Hurtado y Toro (2017), el método es el que va de la mano con el razonamiento donde es lo contrario del deductivo ya que es el que de lo particular a los general, donde el resultado de una investigación en algo en específico va ayudar a dar una respuesta universal a otras investigaciones.(p.63)

Deductivo Método

Según Hurtado y Toro (2017), este método va de lo general a lo particular ya que se parte de algunas cosas y llega a lo específico de la investigación deseada, además de ello llegar a una conclusión verdadera la cual permita tomar decisiones de acuerdo a la información que arroje dicho proyecto.(p.62)

Método Analítico

Hurtado y Toro (2017), Menciona el estudio de todos los componentes de una cosa permitiendo conocer cada una de las partes de la investigación y desarrollar cada una de ellas así logrando sintetizar la información y darla a conocer al máximo de su progreso ya que son necesarios para su conclusión. (p.65)

El trabajo de tesis tubo aspectos teorizados y alcances prácticos por cuanto se describirá los beneficios que adquieren las empresas del sector industrial reguladas por la Superintendencia de Compañías al implementar las

herramientas de seguridad y protección de datos y se utilizará el método Descriptivo el cual permite describir antecedentes y efectos, también analizar las fortalezas empresariales que adquieren las Industrias en la correcta inversión en tecnología, se utilizará el método Deductivo para deducir la información de la muestra en la población; el método Analítico nos permite estudiar cada variable, indicador y resultados obtenidos.

3.4. Enfoque de la Investigación

Para la investigación se utilizará el siguiente enfoque según Hernández, Fernández y Baptista (2014) el cual nos ayudará para su respectivo desarrollo:

> El método de investigación mixto el cual representa un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada y lograr un mayor entendimiento del fenómeno bajo estudio.(p. 546)

Es decir enfoque mixto donde los datos cualitativos están emparentados con los datos cuantitativos, al estar emparentados permite tener una visión más completa y utilizar las fortalezas de ambos tipos de indagación combinándolas y tratando de minimizar sus debilidades potenciales para la investigación respectiva.

3.5. Población

"La población se define como la totalidad del fenómeno a estudiar donde las unidades de población poseen una característica común la cual se estudia y da origen a los datos de la investigación". (Tamayo, 1997, pág. 28)

Para nuestro estudio tomamos como población a las empresas del sector industrial según la Clasificación Industrial Internacional Uniforme (CIIU), los que se encuentran reguladas por la Superintendencia de Compañías, en las cuales podemos encontrar 41 empresas en la Provincia de Cotopaxi.

3.5.1. Empresas Industriales de Cotopaxi CIUU 4.0 Código C: Industrias Manufactureras

Tabla 3

Empresas de Cotopaxi CIUU 4.0 C: Industrias Manufactureras

N°	EMPRESAS
1	CARNIDEM CIA. LTDA.
2	MONARCA CIA.LTDA.
3	HILOS Y TEXTILES INDUSTRIALES COTOPAXI HITEXINCO CÍA. LTDA.
4	INDUSTRIA DE LICORES ECUATORIANOS LICOREC S.A.
5	FABRICACION, COMERCIALIZACION DE POSTES DE HORMIGÓN ARMADO O&M DISPOSTES CIA.LTDA. (C2017)
6	DLIP INDUSTRIAL DLIPINDUSTRIAL S.A.
7	ANDES KINKUNA S.A.
9	MOLINOS POULTIER SA
10	INDUACERO INDUSTRIA DE ACERO DEL ECUADOR CIA. LTDA.
11	CONSTRUCCIONES ULLOA CIA. LTDA.
12	BRIGHTENG SOCIEDAD ANÓNIMA (un Año)
13	EDITORIAL LA GACETA S.A.
14	ABINTRA S.A. (un Año)
15	CALZACUBA CIA. LTDA.
16	PROINPIEL S. A.
17	CORPORACION ECUATORIANA DE ALUMINIO SA CEDAL
18	FUENTES SAN FELIPE S.A. SANLIC
19	INDUSTRIA PLASTICA ITALO ECUATORIANA INDUPIE S.A.
20	COMPAÑÍA ALIMENTICIA AGUA SANTA ALIAGUASANTA CIA. LTDA.
21	ABELLITO S.A.
22	CONSTRUCCIONES FERROPAXI S.A.
23	PROCESADORA DE NEUMÁTICOS COTOPAXI PRONEUMACOSA S.A.
24	LA FINCA CIA. LTDA.
25	ECUATORIANA DE AUTOPARTES SA
26	PROCESADORA DE ALIMENTOS LAPICANTINA S.A.
27	NOVACERO S.A
28	PASTEURIZADORA EL RANCHITO CIA. LTDA
29	PRODICEREAL S.A.
30	AGLOMERADOS COTOPAXI SOCIEDAD ANÓNIMA
31	ECOEQUATORE S.A.
32	PRODUCTORA Y COMERCIALIZADORA DE LOS HELADOS DE SALCEDO CORPICECREAM S.A.
33	ALIMENTOS SALUDABLES ECUADOR ECUALIMFOOD S.A.

CONTINÚA

34	PULPA MOLDEADA S.A. PULPAMOL
35	MOLINOS OROBLANCO CIA. LTDA.
36	COMPAÑIA PROCESADORA DE ALIMENTOS BALANCEADOS BENITES PROBALBEN CIA. LTDA.
37	PARMALAT DEL ECUADOR S.A
38	PRODUCTOS FAMILIA SANCELA DEL ECUADOR
39	SIMEN SOLUCIONES INDUSTRIALES MECANICO, ELECTRICO Y NEUMATICO CIA. LTDA.
40	MAQUINARIA Y MATERIALES DE CONSTRUCCIÓN MATLENCOPS CIA. LTDA.
41	COMPAÑÍA DE SERVICIOS NEOCONTROL CSNEOCONTROL CIA. LTDA.

Fuente: (Superintendencia de Compañias Valores y Seguros del Ecuador, 2017)

3.6. Muestra

La muestra es un subgrupo o subconjunto de la población del cual se recolectan los datos, lo que permitirá que los resultados encontrados logren generalizarse a la población, esta debe ser estadísticamente representativa Hernández et al. (2014).

Según Tamayo (1997), la muestra “es la que puede determinar la problemática ya que es capaz de generar los datos con los cuales se identifican las fallas dentro del proceso. Afirma que la muestra es el grupo de individuos que se toma de la población, para estudiar un fenómeno estadístico” (p. 29)

Claramente los dos autores establecen que la muestra es tomada de la población para posterior realizar el estudio de esta, permitiendo conseguir resultados que serán factibles para la investigación.

3.6.1. Método de muestreo no probabilístico

Esta muestra tiene condiciones que nos permite seleccionar con mecanismos informales el total de representación de la población, también es conocida con el nombre de muestras dirigidas o intencionales Scharager (2016).

- **Muestreo Intencional por cuotas**

  Según Otzen y Manterola (2016) “es aquella que permite seleccionar casos característicos de una población limitando la muestra solo a estos casos, se utilizan en escenarios en las que la población es muy variable y consiguientemente la muestra es muy pequeña”. (p.230)

Para la presente investigación se aplicará una muestra intencional por cuotas debido a que esta permitirá obtener un número determinado de empresas por cada categoría, siendo nuestras condiciones de estudio: Las empresas que se encuentren activas, clasificándolas según su tamaño y que en el Estado de Situación Financiera se encuentren montos considerables en la Cuenta Equipo de Cómputo, también se encuentren valores positivos dentro de sus ingresos por ventas en el año 2016. Por lo tanto las empresas que cumplen que estas características son las siguientes:

Tabla 4

Empresas del Sector Industrial de Cotopaxi parte de la Muestra

EMPRESAS DEL SECTOR INDUSTRIAL				
REGULADAS DE LAS POR LA SUPERINTENDENIA DE COMPAÑÍAS, VALORES Y SEGUROS				
N°	**NOMBRE DE LA EMPRESA**	**TAMAÑO**	**AÑO 2016**	
			EQUIPO DE CÓMPUTO	**INGRESOS POR VENTAS**
1	NOVACERO S.A	GRANDE	$ 101.810,20	$ 201.736.885,00
2	AGLOMERADOS COTOPAXI SOCIEDAD ANONIMA	GRANDE	$ 847.522,57	$ 44.420.457,45
3	CORPORACION ECUATORIANA DE ALUMINIO SA CEDAL	GRANDE	$ 638.071,29	$ 58.756.867,51
4	MOLINOS POULTIER SA	GRANDE	$ 184.294,05	$ 20.600.747,68
5	PASTEURIZADORA EL RANCHITO CIA. LTDA	GRANDE	$ 77.487,31	$ 16.870.182,20
6	PRODICEREAL S.A.	GRANDE	$ 13.721,58	$ 12.675.345,46
7	PARMALAT	GRANDE	$ 114.719,36	$ 27.743.707,57
8	FAMILIA SANCELA	GRANDE	$ 2.064.542,26	$ 155.812.434,00
9	PROVEFRUT	GRANDE	$ 217.106,00	$ 57.148.555,00
10	INDUSTRIA DE LICORES ECUATORIANOS LICOREC S.A.	MEDIANA	$ 97.709,50	$ 2.696.298,98

CONTINÚA

11	DLIP INDUSTRIAL DLIPINDUSTRIAL S.A.	MEDIANA	$ 15.501,48	$ 1.090.752,06
12	INDUACERO INDUSTRIA DE ACERO DEL ECUADOR CIA. LTDA.	MEDIANA	$ 16.159,67	$ 2.574.062,67
13	FUENTES SAN FELIPE S.A. SANLIC	MEDIANA	$ 68.555,72	$ 1.667.149,80
14	CONSTRUCCIONES ULLOA CIA. LTDA.	MEDIANA	$ 2.065,00	$ 1.351.798,28
15	CARNIDEM CIA. LTDA.	MEDIANA	$ 16.758,01	$ 2.575.274,12
16	LA FINCA CIA. LTDA.	MEDIANA	$ 1.759,18	$ 3.425.998,26
17	PRODUCTORA Y COMERCIALIZADORA DE LOS HELADOS DE SALCEDO CORPICECREAM S.A.	PEQUEÑA	$ 12.731,43	$ 787.827,81
18	CALZACUBA CIA. LTDA.	PEQUEÑA	$7.260,74	$ 366.741,26
19	EDITORIAL LA GACETA S.A.	PEQUEÑA	$ 25.440,85	$ 392.948,27
20	MOLINOS OROBLANCO CIA. LTDA.	PEQUEÑA	$ 1.187,36	$ 767.696,42
21	PROCESADORA DE NEUMÁTICOS COTOPAXI PRONEUMACOSA S.A.	PEQUEÑA	$ 0,00	$ 389.805,65
22	ANDES KINKUNA S.A.	MICROEMPRESA	$ 6.329,57	$ 80. 020,52

Fuente: (Superintendencia de Compañias Valores y Seguros del Ecuador, 2017)

3.7. Técnicas e instrumentos de recolección de datos

3.7.1. Técnicas de Información

Existen diferentes técnicas que ayudan a la recolección de información, para el proyecto de investigación se aplicará la técnica de encuesta:

Según Hernández (2013), La técnica de encuesta abarca una investigación para dar respuesta a problemas por ello se recomienda su utilización ya que permite obtener y elaborar datos de modo rápido y eficaz, definiéndose como: “Un instrumento de la investigación de mercados que consiste en obtener información de las personas encuestadas mediante el uso de cuestionarios diseñados en forma previa para la obtención de información específica”. (p. 3)

En la presente investigación se estableció un modelo de encuesta. (Anexo 1 Encuesta)

3.7.2. Instrumentos de la Investigación

En este trabajo de tesis se establecerá fuentes y técnicas con las cuales recopilaremos información que ayudarán al analizar datos.

Libros, artículos, Leyes, Reglamentos, Normas, Antecedentes; que ayuden a la investigación de las herramientas de seguridad y protección de datos en las Empresas del Sector Industrial reguladas por la Superintendencia de Compañías.

Recolección de Datos

Las técnicas utilizadas son de tipo documental y de campo debido a que se recolectó información visitando cada empresa, encuestando en distintas áreas al personal de las cuales se logró obtener información que atraviesan las industrias referente a las herramientas de seguridad y protección de datos.

3.7.3. Validez y confiabilidad del instrumento de recolección.

Con la validez y revisión de los docentes: Ingeniera Nilda Abellán e Ingeniero Cristian Gallardo pertenecientes a la Universidad de las Fuerzas Armadas ESPE-L se logró validar la encuesta para posterior efectuar el trabajo de campo, dando cada uno su respectiva justificación y aclaraciones del instrumento. (Anexo 2 Validación)

3.7.4. Técnicas de Análisis de datos

En la presente investigación se obtuvo los resultados a través de las Herramientas Microsoft Excel y el Software SPSS, los cuales arrojaron información estadística, detallada mediante las tablas de frecuencia, y gráficos, conllevando a un análisis para el cumplimiento de los objetivos y la comprobación de hipótesis.

CAPÍTULO IV

4. RESULTADOS DE LA INVESTIGACIÓN

4.1. Diagnóstico Global de las Industrias

Para realizar el análisis financiero se consideró la información de los estados de situación financiera publicados en la Superintendencia de Compañías por las empresas del Sector Industrial.

Empresa la Finca Cía. Ltda.

Ubicada en el Sector Salache de la Parroquia Eloy Alfaro en la ciudad de Latacunga, dedicada a la elaboración de productos lácteos.

Con el propósito de conocer cuáles fueron los principales cambios en la estructura económica de la empresa y observar cómo han ido variando las cuentas del Activo, Pasivo y Patrimonio a continuación se detallan los análisis:

Tabla 5

Valores Relativos Activo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO	21,92%	3,19%	-12,68%	-0,80%

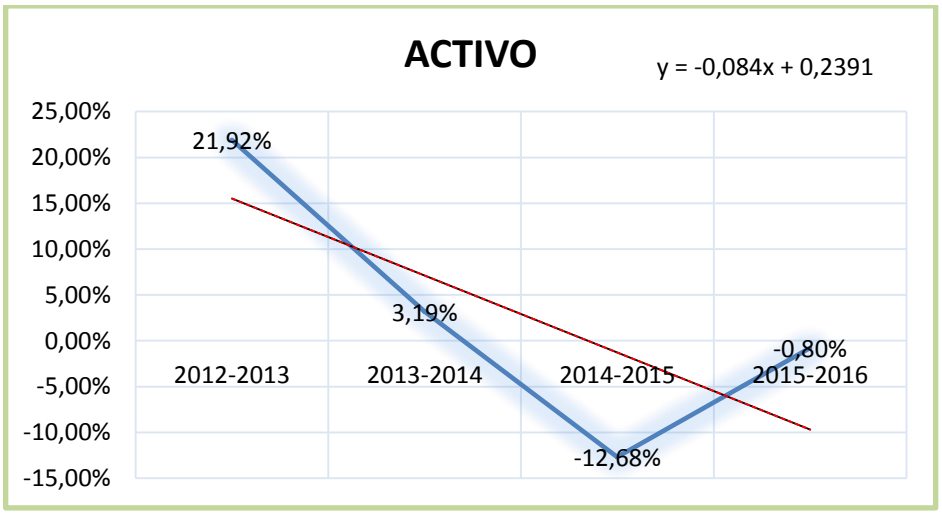

Figura 2. Valores Relativos Activo

Tabla 6

Valores Relativos Activo No Corriente

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO NO CORRIENTE	12,69%	7,56%	0,00%	-8,28%

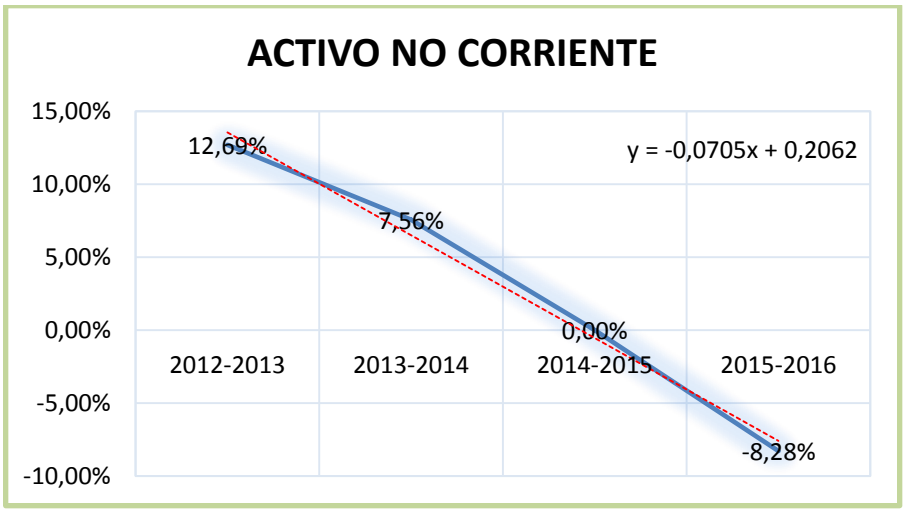

Figura 3. Valores Relativos Activo No Corriente

Tabla 7

Valores Relativos Equipo de Cómputo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
EQUIPO DE CÓMPUTO	0,00%	0,00%	0,00%	0,00%

Figura 4. Valores Relativos Equipo de Cómputo

Tabla 8

Valores Relativos Pasivo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PASIVO	23,70%	3,42%	-15,13%	-2,60%

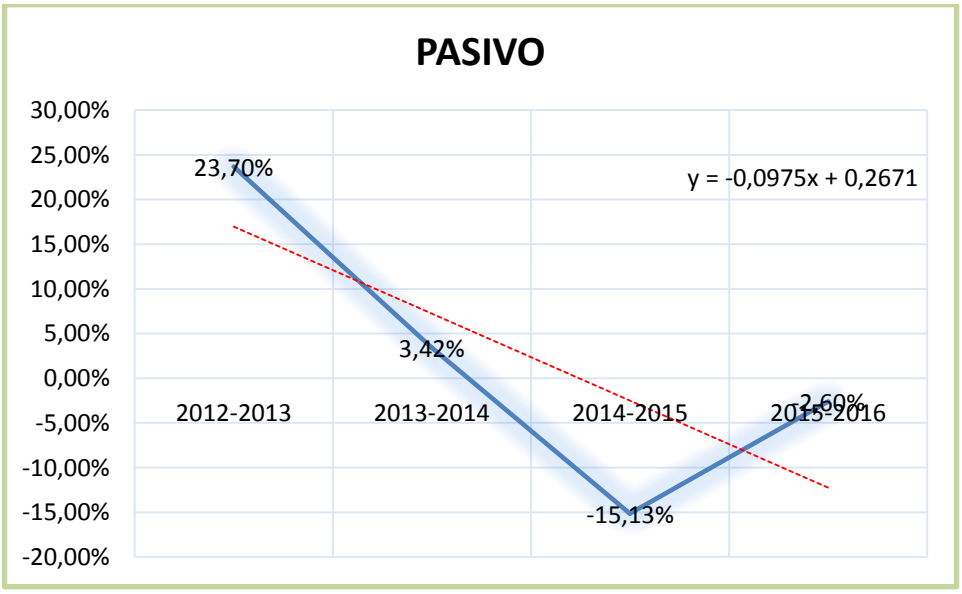

Figura 5. Valores Relativos Pasivo

Tabla 9

Valores Relativos Patrimonio

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PATRIMONIO	8,68%	1,24%	8,42%	11,35%

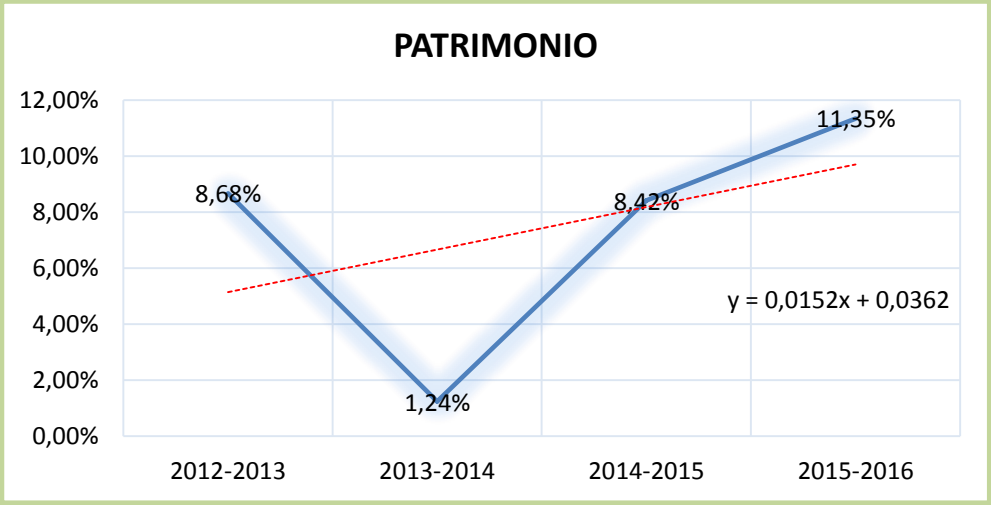

Figura 6. Valores Relativos Patrimonio

Pronósticos

Como primer método para el cálculo de los pronósticos de las diferentes cuentas se realizó aplicando la fórmula en Excel: PRONÓSTICO(x; conocido; conocido) la cual predice un valor futuro en una tendencia lineal con los valores históricos de cada una de las cuentas principales del estado de situación financiera.

Tabla 10

Pronóstico de Cuentas

CUENTA	2016-2017	2017-2018	2018-2019	2019-2020
Activo	5,60%	0,51%	0,508%	0,51%
Activo No Corriente	10,21%	2,52%	2,46%	2,40%
Pasivo	6,01%	-0,32%	-0,32%	-0,33%
Patrimonio	3,18%	5,57%	5,27%	5,01%
Equipo de Cómputo y Software	0,00%	0,00%	0,00%	0,00%

Comprobación:

Para comprobar los valores obtenidos por con la fórmula de Excel se aplicó el método de regresión lineal y como resultado arrojaron los mismos valores, aplicando el siguiente modelo general:

$$\boldsymbol{Activo = Bo + B1\ (Pasivo) + B1(Patrimonio) + E1}$$

Tabla 11

Regresión

Estadísticas de la regresión	
Coeficiente de correlación múltiple	1
Coeficiente de determinación R^2	1
R^2 ajustado	1
Error típico	2,5724E-12
Observaciones	5

Tabla 12

Variables

	Coeficientes	Error típico	Estadístico t	Probabilidad
Intercepción ; B0	0	1,8426E-11	0	1
Variable X 1; B1	1	1,5714E-17	6,3637E+16	2,4693E-34
Variable X 2; B2	1	1,1221E-16	8,9116E+15	1,2592E-32

Pronóstico Pasivo

Tabla 13

Regresión Pasivo

Estadísticas de la regresión	
Coeficiente de correlación múltiple	0,04764879
Coeficiente de determinación R^2	0,00227041
R^2 ajustado	-0,33030612
Error típico	95595,0174
Observaciones	5

Tabla 14

Coeficientes cálculo del Pasivo

	Coeficientes	Error típico	Estadístico t	Probabilidad
Intercepción	787659,792	100260,9	7,85610135	0,00429616
Variable X 1	-2497,706	30229,7988	-0,08262397	0,93935464

Fórmula: Intercepción + (Variable X1 * # del año anterior)

Tabla 15

Pronósticos del Pasivo

PRONÓSTICO 2017	**772673,556**
PRONÓSTICO 2018	770175,85
PRONÓSTICO 2019	767678,144
PRONÓSTICO 2020	765180,438

Pronóstico Patrimonio

Tabla 16

Regresión - Patrimonio

Estadísticas de la regresión	
Coeficiente de correlación múltiple	0,9667077
Coeficiente de determinación R^2	0,93452378
R^2 ajustado	0,91269838
Error típico	3429,39317
Observaciones	5

Tabla 17

Coeficientes cálculo del Patrimonio

	Coeficientes	Error típico	Estadístico t	Probabilidad
Intercepción	84895,149	3596,7779	23,6031113	0,00016663
Variable X 1	7096,289	1084,46934	6,54355889	0,00725552

Tabla 18

Pronósticos Patrimonio

PRONÓSTICO 2017	**127472,883**
PRONÓSTICO 2018	134569,172
PRONÓSTICO 2019	141665,461
PRONÓSTICO 2020	148761,75

Reemplazo de datos en la formula general:

$$\boldsymbol{Activo = Bo + B1\ (Pasivo) + B1(Patrimonio) + E1}$$

Tabla 19

Pronósticos- Activo

2017	**900146,439**
2018	904745,022
2019	909343,605
2020	913942,188

Tabla 20

Valores Históricos de las Cuentas

CUENTA	2016-2017		2017-2018	
	V. ABSOLUTO	V.RELATIVO	V. ABSOLUTO	V.RELATIVO
ACTIVO	47715,079	5,60%	4598,583	0,51%
PASIVO	43791,376	6,01%	-2497,706	-0,32%
PATRIMONIO	3923,703	3,18%	7096,289	5,57%
ACTIVO NO C.	45.845,43	10,21%	12.473,38	2,52%

Tabla 21

Pronósticos de las Cuentas

CUENTA	2018-2019		2019-2020	
	V. ABSOLUTO	V.RELATIVO	V. ABSOLUTO	V.RELATIVO
ACTIVO	4598,583	0,51%	4598,583	0,51%
PASIVO	-2497,706	-0,32%	-2497,706	-0,33%
PATRIMONIO	7096,289	5,27%	7096,289	5,01%
ACTIVO NO C.	12.473,38	2,46%	12.473,38	2,40%

Interpretación

De acuerdo a los valores reflejados en los estados de situación financiera observamos que en el año 2015 la empresa presenta en activos $ 859.304,93 disminuyendo en 12.68% y para el último año 2016 versus 2015 cuenta con un valor en activos de $852.431,36 representando una disminución de 0.80%, además se estima que después de cuatro años la cuenta se incrementará en 0,51%. La cuenta Propiedad, Planta y Equipo para el año 2016 en referencia al año 2015 la cuenta ha disminuido en 8,28% por una cantidad de $40.570,45. La cuenta de Pasivo presenta una disminución de 2,60% con una cantidad de $19.469,61 y si se mantiene el panorama económico y políticas gubernamentales actuales en los próximos cuatro años las obligaciones disminuirán en 0,33%. EL patrimonio finalizó el año 2016 con un incremento de 11,35% por una cantidad de $12.596,04 y se estima un incremento en los próximos cuatro años del 5,01%.

En el año 2016 la cuenta principal dentro de Propiedad Planta y Equipo es Maquinaria y Equipo con el 68,15% del total del Activo por un valor de $ 580.971,65, dentro del Activo Corriente tenemos Efectivo y Equivalentes al Efectivo con el 17,22% del total del activo por un valor de $146.783,33. Las cuentas y documentos por pagar alcanzaron un valor de $227.371,83 que representa el 31,19% del total de Pasivo. La cuenta principal de resultados acumulados es Ganancias Acumuladas por un valor de $114.699,02 que representa el 92,84% del total del Patrimonio.

Análisis y Diagnóstico

En la cuenta activo se observa una tendencia decreciente, dentro de está en los años 2015 y 2016 una de las cuentas con mayor representatividad es inventarios con una disminución de 39,97% y 69,17% respectivamente esto ocurrió debido que la producción de leche estuvo afectada por la caída de ceniza generada por el volcán Cotopaxi. Se puede observar que desde el año 2012 al 2016 la empresa se ha mantenido con un monto de $ 1759,18 en la

cuenta equipo de cómputo, y para el año 2016 la empresa no cuenta con activos intangibles, llegando a la conclusión que está empresa no invierte en herramientas de seguridad y protección de datos. Se observa que el patrimonio de la empresa en los últimos años presenta una tendencia creciente y un incremento poco representativo para poder generar mayores utilidades para sus accionistas la administración deberá implementar nuevas estrategias.

Novacero S.A.

Su domicilio principal está situado en el KM 15 Panamericana Norte de Lasso-Cotopaxi, la planta de Lasso es la encargada de la fundición de acero y Laminación.

Tabla 22

Valores Relativos Equipo de Computación y Software

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
EQUIPO DE COMPUTACIÓN Y SOFTWARE	32,85%	13,58%	11,77%	9,99%

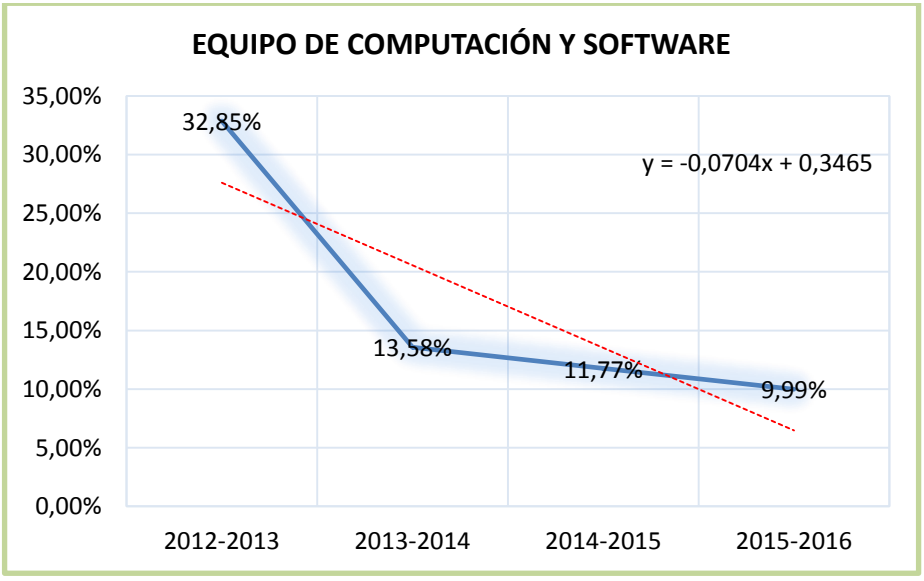

Figura 7. Valores Relativos Equipo de Computación y Software

Tabla 23 N.

Valores Relativos Activo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO	13,01%	7,18%	-7,33%	2,79%

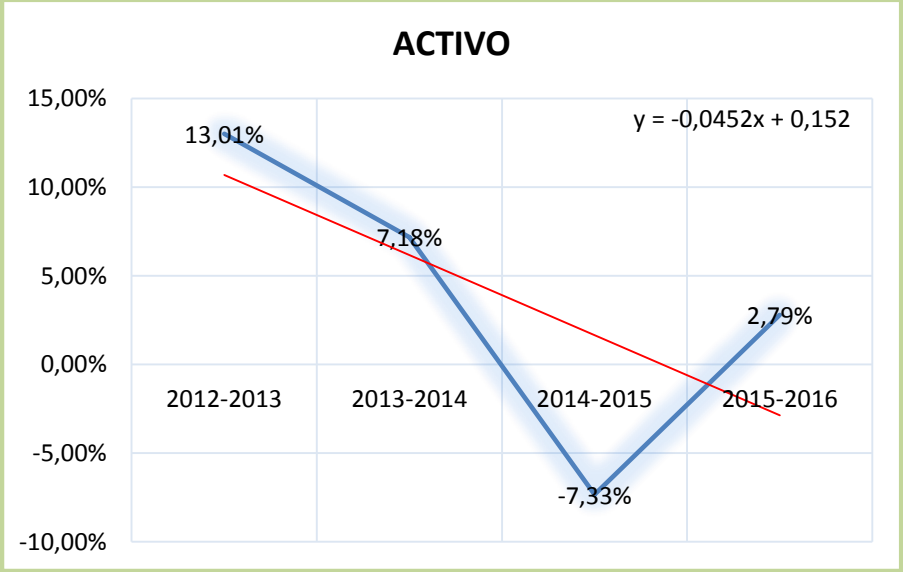

Figura 8. Valores Relativos Activo

Tabla 24

N. Valores Relativos Activo No C.

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO NO CORRIENTE	13,83%	10,71%	19,25%	3,57%

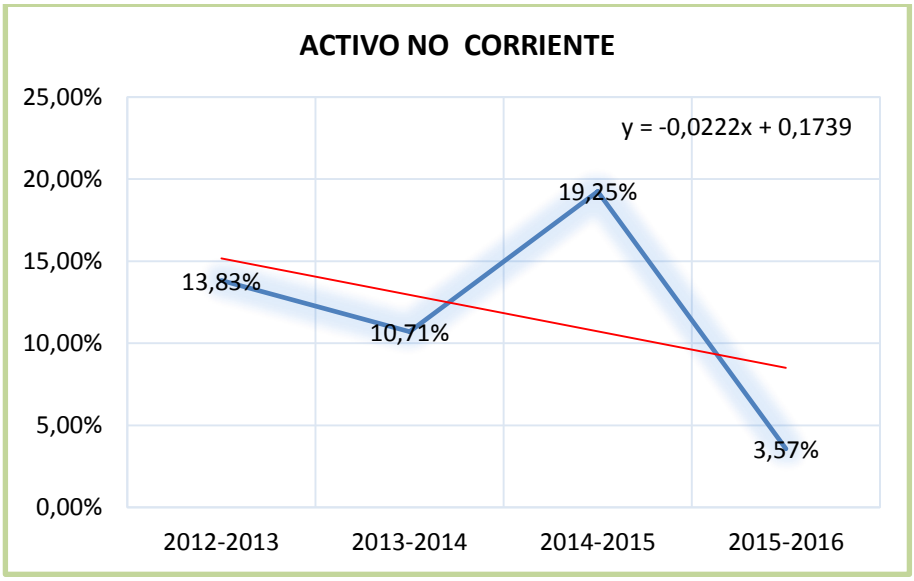

Figura 9. N. Valores Relativos Activo No C.

Tabla 25

N. Valores Relativos Pasivo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PASIVO	17,61%	11,02%	-14,83%	-0,59%

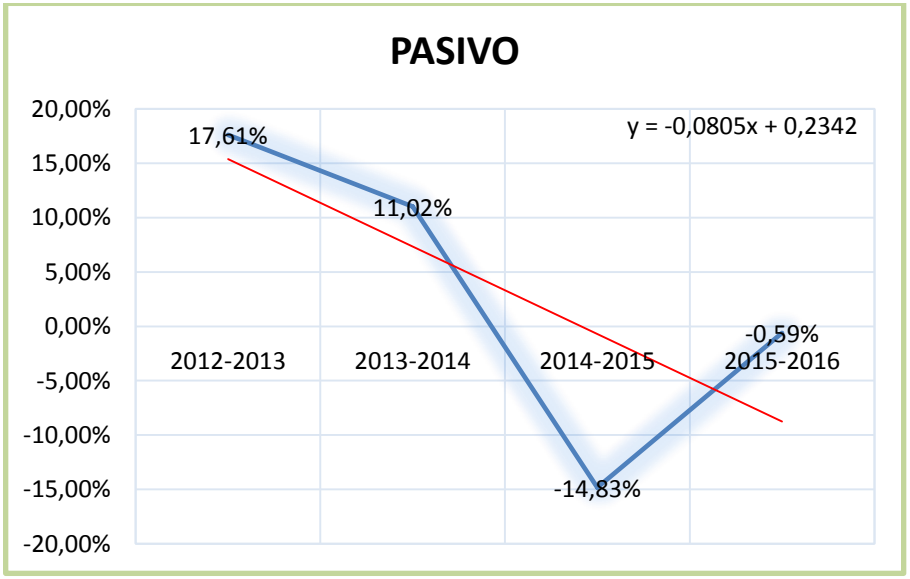

Figura 10. N. Valores Relativos Pasivo

Tabla 26

N. Valores Relativos Patrimonio

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PATRIMONIO	5,45%	0,15%	7,87%	8,21%

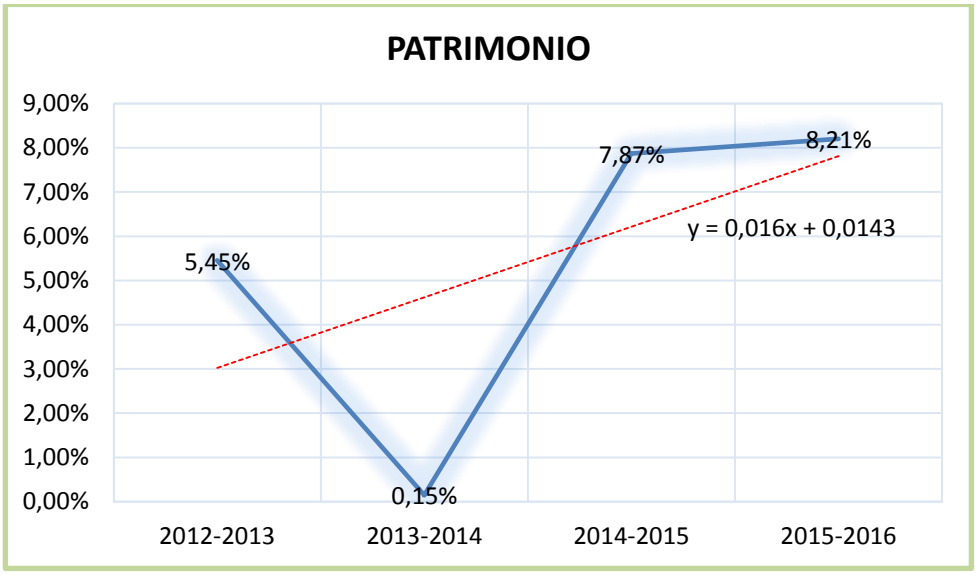

Figura 11. Valores Relativos Patrimonio

Pronósticos

Tabla 27

Pronósticos de las Cuentas- Novacero

CUENTA	2016-2017	2017-2018	2018-2019	2019-2020
Activo	5,17%	2,47%	2,41%	2,35%
Activo No Corriente	11,46%	8,52%	7,85%	7,28%
Pasivo	7,10%	1,24%	1,23%	1,21%
Patrimonio	2,34%	4,36%	4,18%	4,01%
Equipo de Cómputo y Software	13,00%	9,87%	8,98%	8,24%

Interpretación

La empresa para el año 2016 con relación al año 2015 presenta en la cuenta Activo un incremento de 2,79% por una cantidad de $ 6.105.829,26 y se estima

un incremento de 2,35% dentro de cuatro años. En el Activo No Corriente se observa un incremento de 3,57% por una cantidad de $6.105.829,26 y a cuatro años se estima un incremento de 7,28% si las políticas tanto internas como externas se mantienen. En Equipo de Computación y Software existe un incremento del 9,99% por una cantidad de $101.810,20 y se estima un incremento no tan significativo de 8,64% en los próximos cuatro años. En la cuenta Pasivo por el contrario se observa una disminución de 0,59% por una cantidad de $ 793.795,47 y para la cuenta Patrimonio presenta un incremento de 8,21% lo que representa una cantidad de $6.899.624,73.

Según (Smith, 2017) en el Informe menciona que las principales cuentas del activo Corriente son Efectivo y Equivalentes al Efectivo, y para el año 2016 representa el 2,39 del total de activos por una cantidad de $5.372.743, en el año 2015 representó el 1,09%. Los Créditos por ventas y otro Deudores alcanzaron un valor de $34.661.630 y representa el 15,42% del total de Activos, en el año 2015 representaron el 13,11%, estos incrementos debe a la flexibilización de la política de crédito por movimiento de mercado. Los Inventarios presenta $47.877.928 representando el 21.30% del total de Activos, en el 2015 fueron de $53.253.677, está baja se básicamente a la optimización en los niveles de inventario de producto terminado.

En el año 2016 se realizó la apropiación de la Reserva Legal, por lo que este valor ascendió a $8.754.935,26 lo que representa el 9,62% del total de Patrimonio, la utilidad generada fue de $ 36.928.308,18 el cual representa el 40,59% del total de Patrimonio.

Análisis y Diagnóstico

Se observa que las cuentas del Activo, Pasivo presentan una tendencia decreciente al 2016 y se establece que existió un incremento en la cuenta efectivo y Equivalentes al Efectivo de 125,42% con relación al año 2015 esto se debe porque la empresa tenía reservas de $243.343 toneladas que fueron compradas en el año 2015 y se las vendieron en el 2016, se observa además

un incremento en la cuenta ganancias de 512,14% versus el 2015 esto es gracias a que según (Smith, 2017) en el mercado de laminados Novacero lidera con el 43% y las ventas a nivel nacional de varilla de construcción recta y figurada significó un crecimiento de 5,8% versus el 2015, lo que refleja una tendencia creciente del Patrimonio.

AGLOMERADOS COTOPAXI S. A.

Según Moscoso (2016) el objetivo de la empresa es "la producción con fines industriales, de tableros de Aglomerados y MDF, recubiertos de chapa de madera y/o papel, también es establecimiento de plantaciones, explotaciones forestales y otros productos afines a la industria maderera." (p.1)

Tabla 28

A. Valores Relativos Eq. de Computación y Software

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
EQUIPO DE COMPUTACIÓN Y SOFTWARE	-0,28%	5,71%	14,23%	2,00%

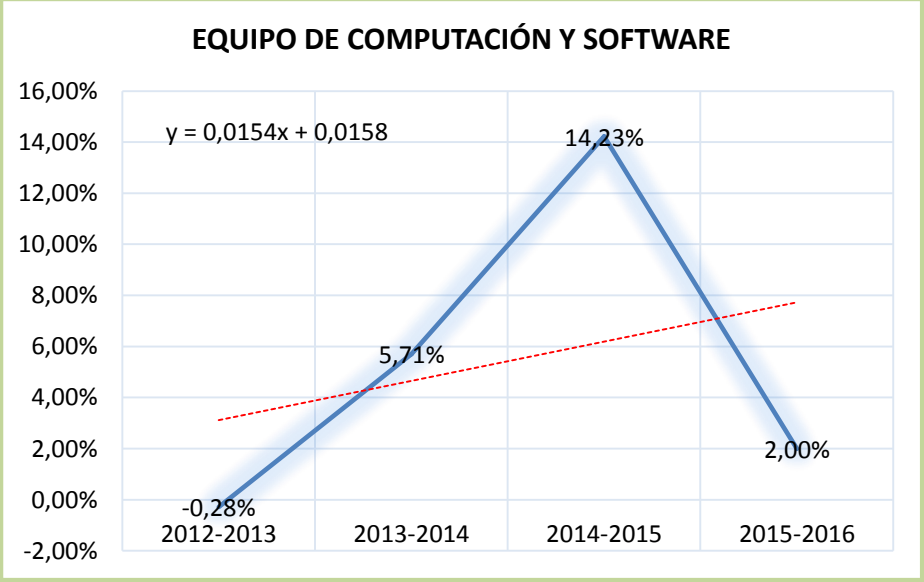

Figura 12. A. Valores Relativos Eq. de Computación y Software

Tabla 29

A. Valores Relativos Activo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO	-2,25%	7,16%	-7,21%	0,49%

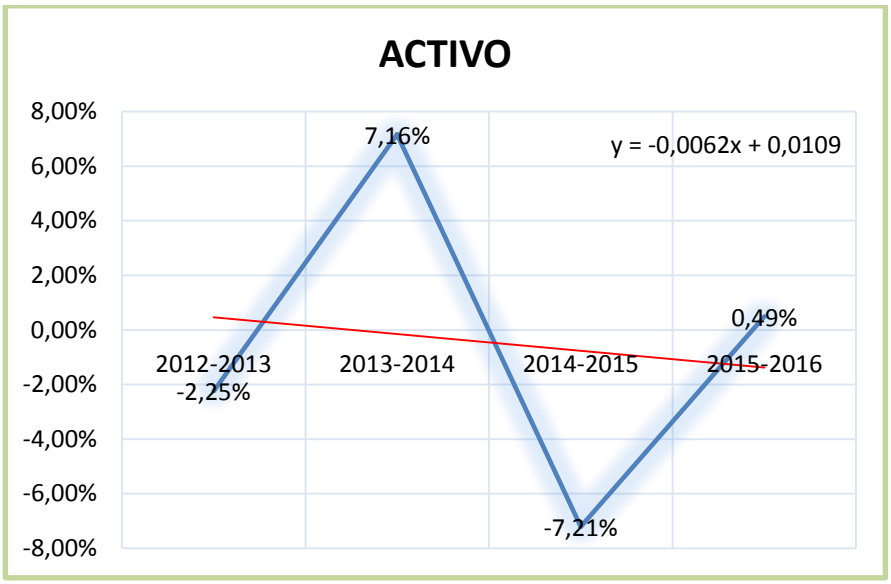

Figura 13. A. Valores Relativos Activo

Tabla 30

A. Valores Relativos Activo No C.

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO NO CORRIENTE	-1,42%	2,20%	-2,00%	-2,39%

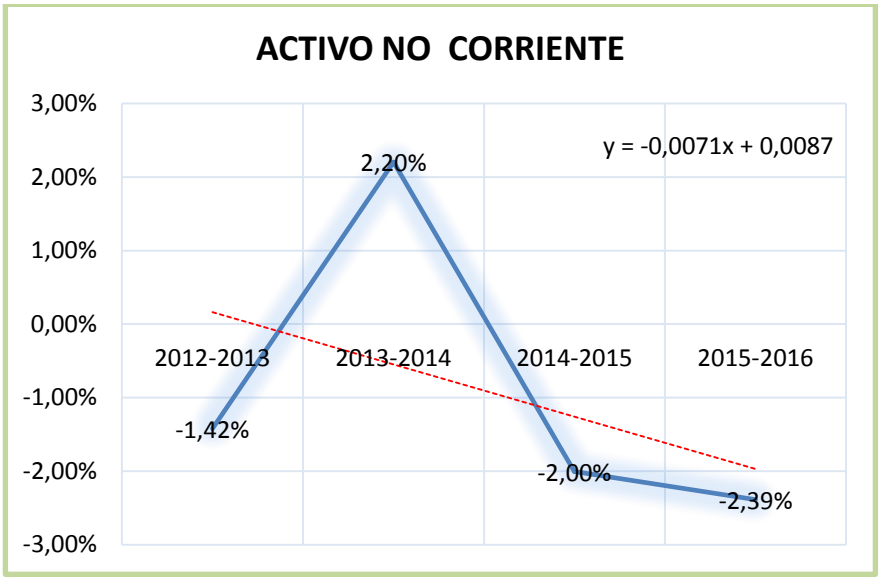

Figura 14. A. Valores Relativos Activo No C.

Tabla 31

A. Valores Relativos Activo Intangible

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO INTANGIBLE	333,67%	-75,53%	-9,04%	-38,32%

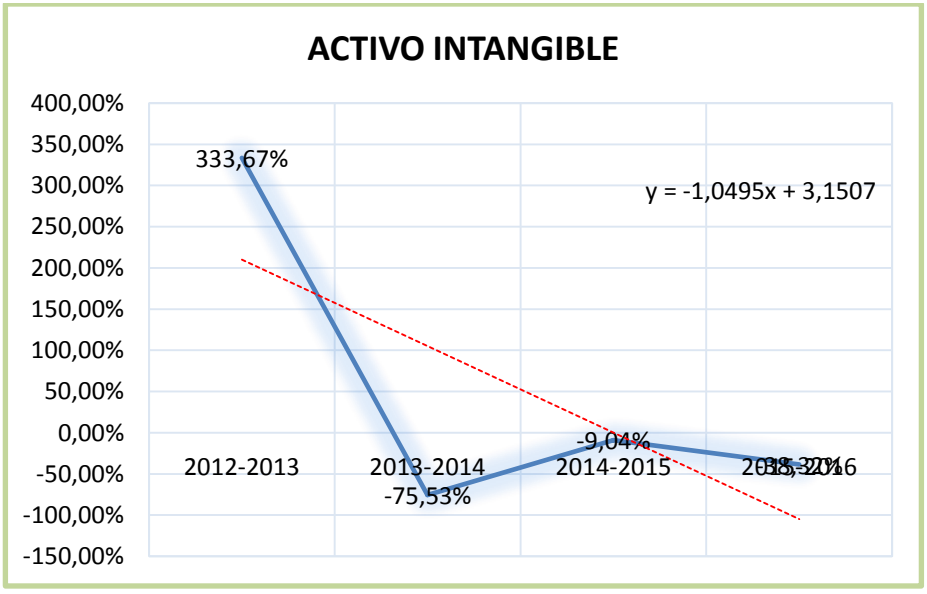

Figura 15. A. Valores Relativos Activo Intangible

Tabla 32

A. Valores Relativos Pasivo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PASIVO	-16,87%	16,54%	-27,06%	-4,44%

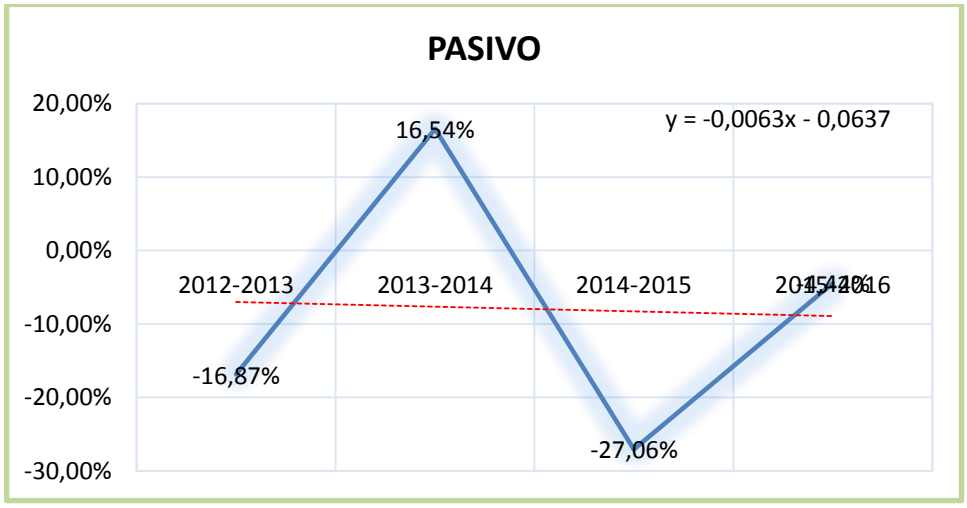

Figura 16. A. Valores Relativos Pasivo

Tabla 33

A. Valores Relativos Patrimonio

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PATRIMONIO	6,50%	2,77%	3,31%	2,33%

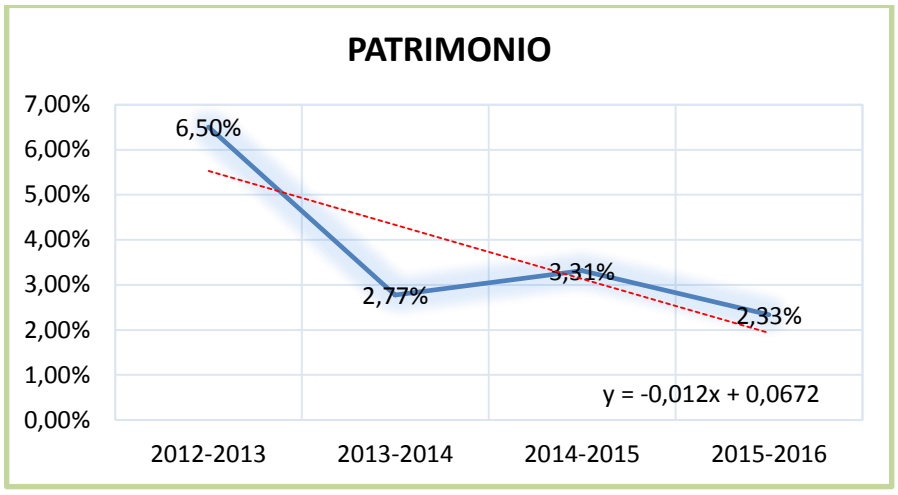

Figura 17. A. Valores Relativos Patrimonio

Pronóstico

Tabla 34

Pronóstico de las cuentas- E. Aglomerados

CUENTA	2016-2017	2017-2018	2018-2019	2019-2020
Activo	0,24%	-0,533%	-0,535%	-0,54%
Activo No Corriente	0,40%	-0,73%	-0,74%	-0,74%
Activo Intangible	-43,34%	-123,96%	517,30%	83,80%
Pasivo	-10,53%	-12,81%	-14,70%	-17,23%
Patrimonio	4,01%	3,16%	3,06%	2,97%
Equipo de Cómputo y Software	5,50%	5,12%	4,87%	4,65%

Interpretación

En el año 2016 versus el 2015 la empresa incremento sus activos en 0,49% por una cantidad de $ 414.305,29 pero se observa una tendencia decreciente y se estima a cuatro años una disminución en la cuenta del 0,54%. Se observa en el año 2015 un incremento de 14,23% en Equipo de Computación y Software y para el 2016 en relación al año 2015 un incremento del 2% por una cantidad de $ 16.653,63 reflejando una tendencia creciente y si se estima un incremento a cuatro años en la cuenta del 4,65%. La cuenta Pasivo se encuentra en $ 1.027.668,5 lo que representa para el año 2016 una disminución del 4,44%, reflejando así una tendencia decreciente. El Patrimonio incremento en 2,33% con referencia al año anterior por una cantidad de $ 1.441.973,8 y se estima un incremento paulatino a cuatro años de 2,97%.

Las principales cuentas del activo No Corriente son Maquinaria y Equipo en el cual se presenta para el año 2016 el 26,1% del total de activos por una cantidad de $22.282.083,5. Equipo de Computación y software alcanzaron un valor de $847.522,57 y representa el 1,0% del total de Activos, en el año 2015 representaron el 0,98% del total de Activos.

Análisis y Diagnóstico

En la cuenta del Activo se observó que dentro de otras cuentas por cobrar uno de sus componentes es seguros por cobrar está pertenece a una póliza general de todo riesgo que la empresa ha venido renovando anualmente.

Además según (Arteta, 2016)

> Con la crisis de Brasil, la demanda interna de tableros de MDF y aglomerado ha caído significativamente, situación que ha generado una sobre oferta de tableros, debido a la incertidumbre del mercado ecuatoriano es necesario fortalecer la posición financiera de la compañía por ello la administración propone a la Junta un aumento de capital por la suma de $1.700.000. (p.4)

Corporación Ecuatoriana de Aluminio S.A.

CEDAL

Ubicada en la Ciudad de Latacunga, en el barrio Sigsicalle Sur, en la avenida de la Unidad Nacional y Ángel Subía, provincia de Cotopaxi, dedicada a la fabricación y comercialización de perfiles de aluminio y otros artículos metálicos, especialmente no ferrosos.

Tabla 35

C. Valores Relativos Equipo de Computación

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
EQUIPO DE COMPUTACIÓN	32,91%	14,45%	5,50%	0,12%

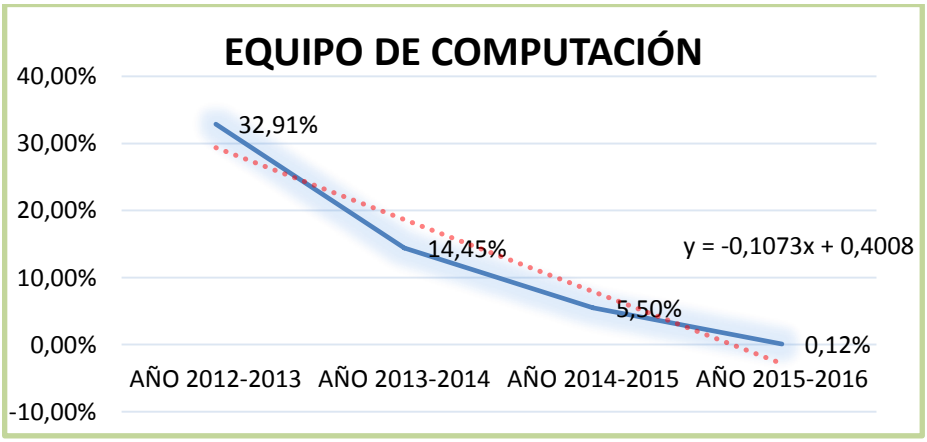

Figura 18. C. Valores Relativos Equipo de Computación

Tabla 36

C. Valores Relativos Activo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO	10,60%	18,20%	5,23%	-3,46%

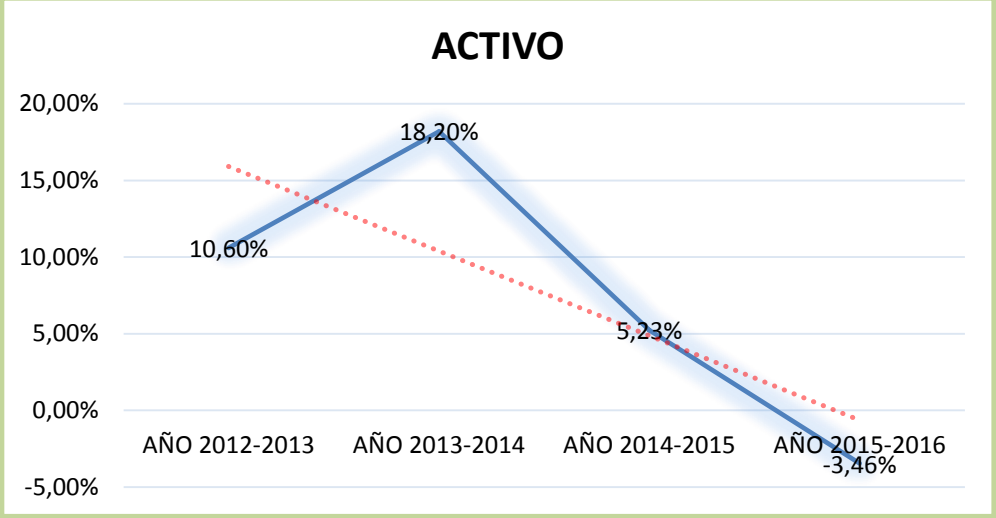

Figura 19. C. Valores Relativos Activo

Tabla 37

C. Valores Relativos Activo No C.

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO NO CORRIENTE	16,67%	-9,26%	36,28%	0,09%

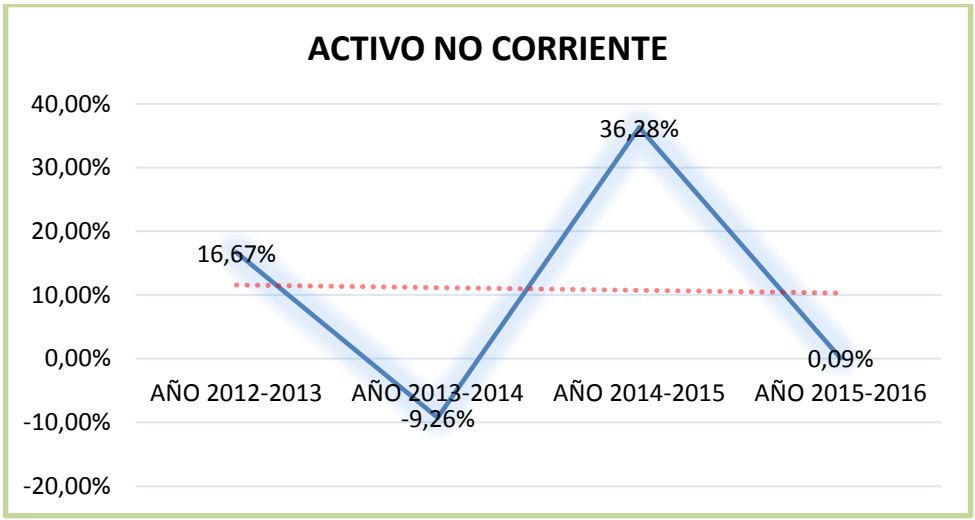

Figura 20. C. Valores Relativos Activo No C.

Tabla 38

C. Valores Relativos Pasivos

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PASIVO	8,39%	30,70%	9,75%	-6,20%

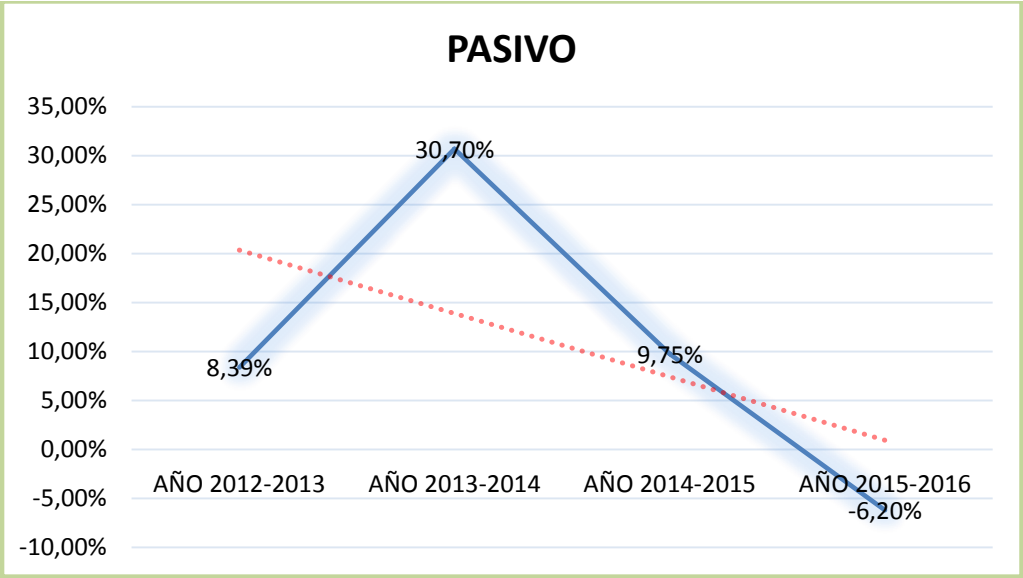

Figura 21. C. Valores Relativos Pasivos

Tabla 39

C. Valores Relativos Patrimonio

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PATRIMONIO	12,28%	9,00%	1,24%	-10,30%

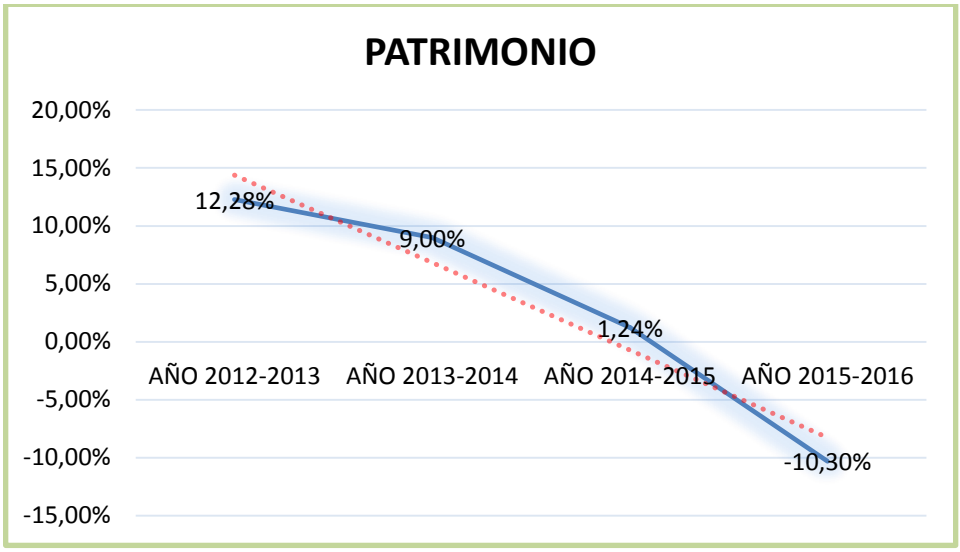

Figura 22. C. Valores Relativos Patrimonio

Pronóstico

Tabla 40

Pronóstico-E. CEDAL

CUENTA	2016-2017	2017-2018	2018-2019	2019-2020
ACTIVO	13,03%	6,17%	5,81%	5,49%
ACTIVO NO CORRIENTE	8,84%	7,87%	9,90%	3,64%
PASIVO	17,87%	7,05%	3,32%	6,10%
PATRIMONIO	11,67%	-1,31%	-1,27%	1,00%
EQUIPO DE COMPUTACIÓN	15,71%	8,01%	7,42%	6,90%

Interpretación

Con la información reflejada en los estados de situación financiera se presenta en la Cuenta del Activo para el año 2016 en relación al año 2015 se presentó un decrecimiento del 3,46%, en la cuenta del Activo no Corriente se presentó un crecimiento del 0,09%, en la cuenta del Equipo de Cómputo y software en el año 2015 con un valor de $637.329,69 en el año 2016 con un valor $638.071,29 se presentó un incrementó del 0,12%, en la cuenta del Pasivo se presentó un decrecimiento del 6,20%, en la cuenta del Patrimonio de presentó un decrecimiento del 10,30%.

Análisis y Diagnóstico

La empresa tiene un porcentaje importante de crecimiento ya que sus productos se dan a conocer mediante estrategias comerciales, con la implementación de nuevos equipos y el nivel tecnológico y de automatización, a más de ello se crea otra sucursal en Duran, permitiendo a la empresa a extenderse y tener la capacidad de atraer nuevas inversiones en Tecnología y herramientas de seguridad y protección de datos, y con sus proyecciones para los próximos años la empresa mantendrá niveles estables.

Molinos Poultier S.A.

Ubicada en la avenida Rumiñahui y Quito a media cuadra de la escuela Velasco Ibarra en la Ciudad de Latacunga Cantón Cotopaxi, Dedicada la molienda de cereales, producción de harina, se molina, sémola y gránulos de: trigo, centeno, avena, maíz y otros cereales.

Tabla 41

M. Valores Relativos Eq. de Computación

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
EQUIPO DE COMPUTACIÓN	6,75%	0,31%	6,10%	0,67%

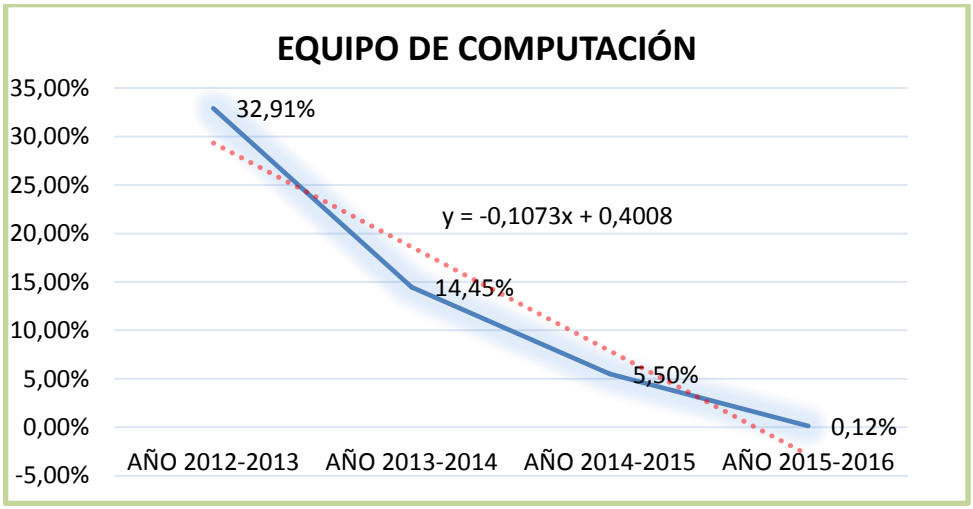

Figura 23. M. Valores Relativos Eq. de Computación

Tabla 42

M. Valores Relativos Activo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO	-98,53%	8306%	-21,08%	35,59%

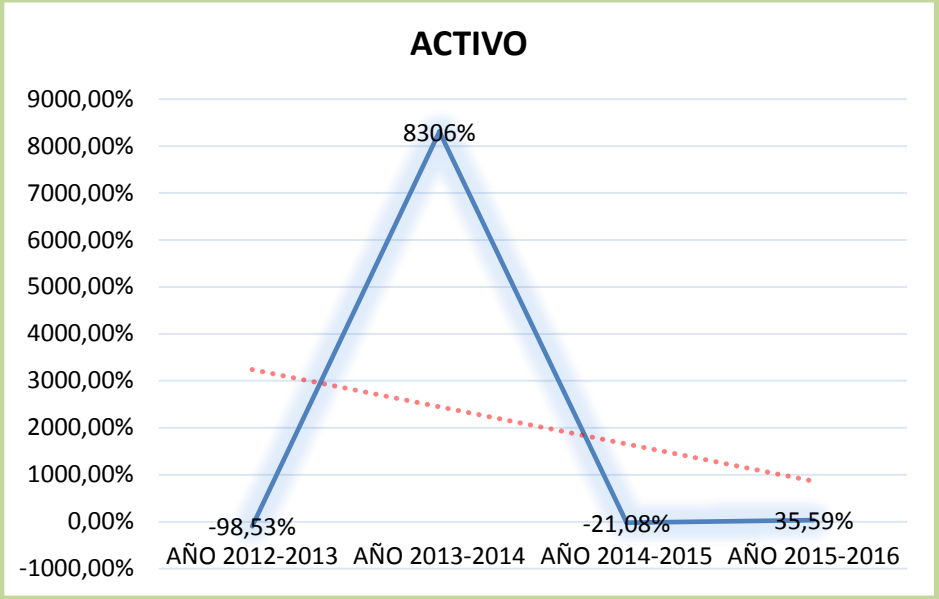

Figura 24. M. Valores Relativos Activo

Tabla 43

M. Valores Relativos Activo no C.

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO NO CORRIENTE	-10,58%	-11%	-98%	3646,95%

Figura 25. M. Valores Relativos Activo no C.

Tabla 44

M. Valores Relativos Pasivo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PASIVO	36,52%	26,39%	-51,95%	139,24%

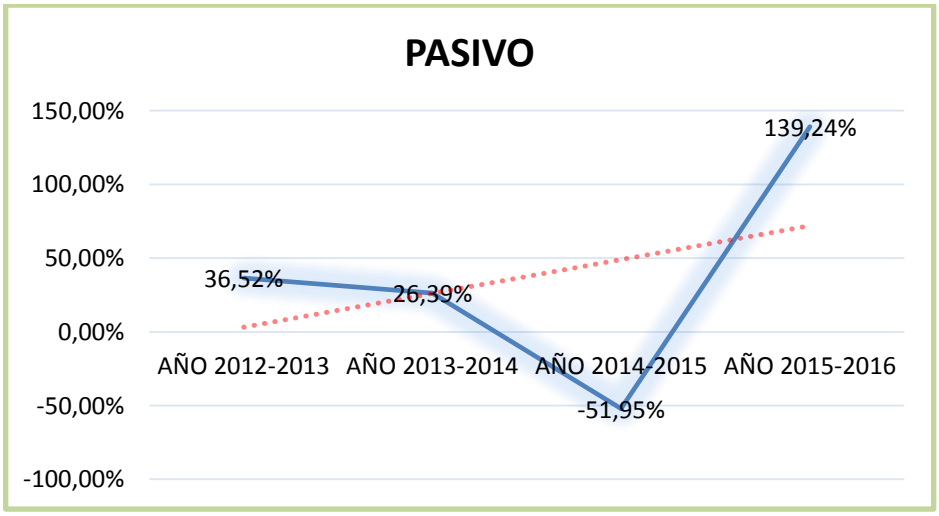

Figura 26. M. Valores Relativos Pasivo

Tabla 45

M. Valores Relativos Patrimonio

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PATRIMONIO	1,68%	1,60%	0,23%	1,28%

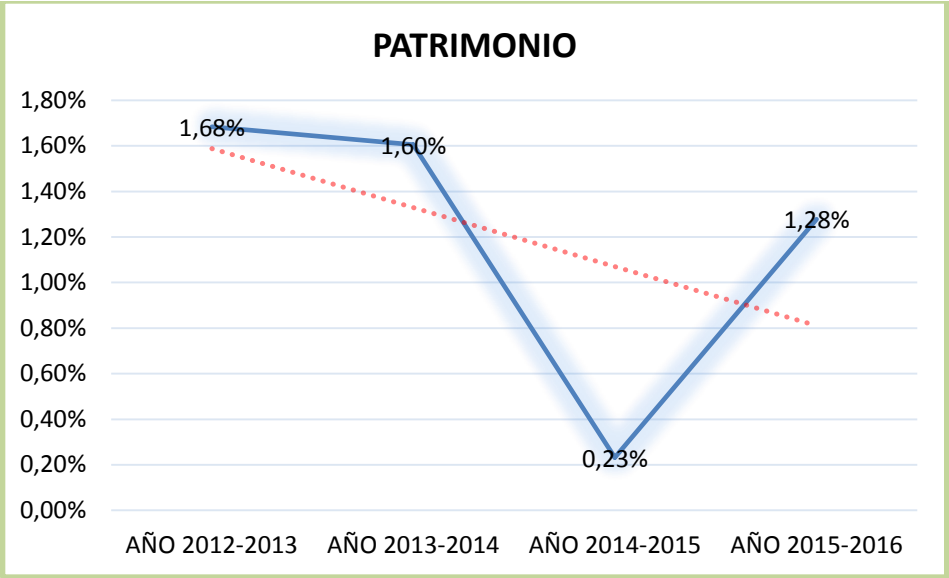

Figura 27. M. Valores Relativos Patrimonio

Pronóstico

Tabla 46

Pronóstico de Cuentas E. Molinos

CUENTA	2016-2017	2017-2018	2018-2019	2019-2020
ACTIVO	5,20%	11,54%	10,34%	9,37%
ACTIVO NO CORRIENTE	-67,95%	-71,45%	-250,23%	166,56%
PASIVO	-8,75%	7,91%	7,33%	6,83%
PATRIMONIO	1,24%	1,09%	1,08%	1,07%
EQUIPO DE COMPUTACIÓN	4,09%	2,99%	2,90%	2,82%

Interpretación

Con la información reflejada en los estados de situación financiera se constata en la Cuenta del Activo para el año 2016 en relación al año 2015 se presenta un incremento de 35,59%, en la cuenta del Activo no Corriente se

presenta un crecimiento muy significativo del 3646,95% además se registró en los años anteriores porcentajes bajos en la cuenta, en la cuenta del Equipo de Cómputo y software en el año 2015 con un valor de $183.064,20 en el año 2016 con un valor $184.294,05 se presenta un incremento del 0.67%, en la cuenta del Pasivo se presentó un crecimiento característico del 139,24%, en la cuenta del Patrimonio se presenta un incremento del 1,28%.

Análisis y Diagnóstico

La empresa entre los años 2012-2016 años de análisis presentó tendencias altas en las cuentas Activo no Corriente y Pasivo, y en las cuentas Equipo de computación, Activo y Patrimonio indicó tendencias decrecientes pero son porcentajes mínimos, a más de ello la empresa presenta en su cuenta Equipo de computación y software una inversión importante de $184294,05 ya que con la inversión realizada en tecnología la empresa cumple con las exigencias del mercado nacional y para las proyecciones se estima que la empresa se mantenga con economías estables para los próximos años.

Pasteurizadora El Ranchito Cía. Ltda.

Su actividad principal, es la elaboración, fabricación, colocación y venta de productos lácteos, además la producción y envasado de yogurt. En si todas las actividades relacionadas con la producción de leche y crema.

Tabla 47 R. Valores Relativos Eq. de computación

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
EQUIPO DE COMPUTACIÓN Y SOFTWARE	24,18%	162,63%	3,97%	19,12%

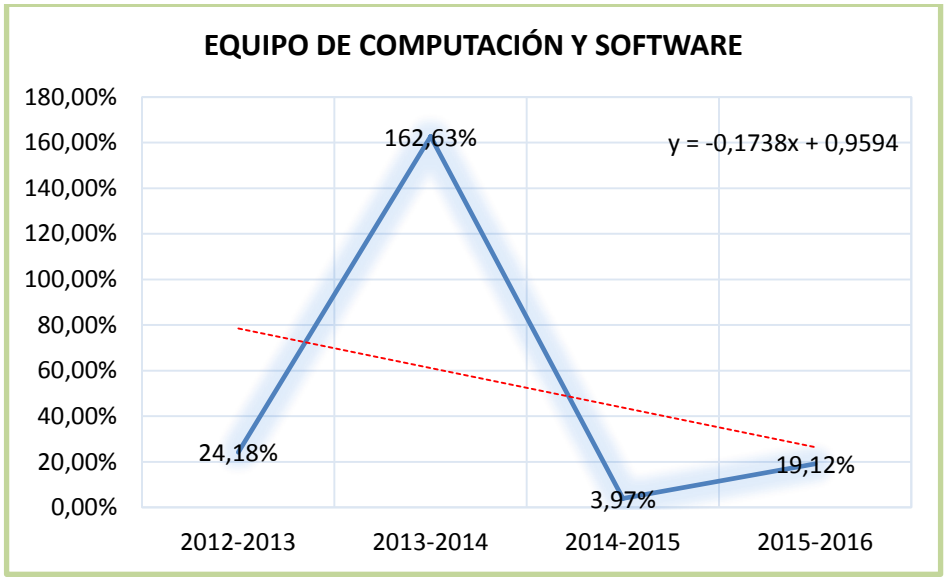

Figura 28. R. Valores Relativos Eq. de computación

Tabla 48

R. Valores Relativos Activo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO	19,97%	-6,88%	13,76%	-7,43%

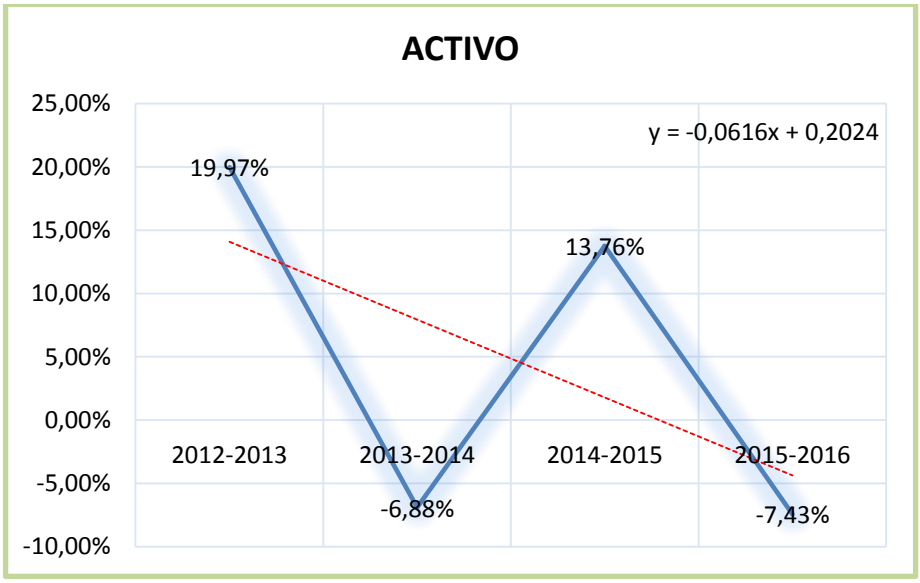

Figura 29. R. Valores Relativos Activo

Tabla 49

R. Valores Relativos Activo No C

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO NO CORRIENTE	11,24%	2,80%	-21,55%	-3,95%

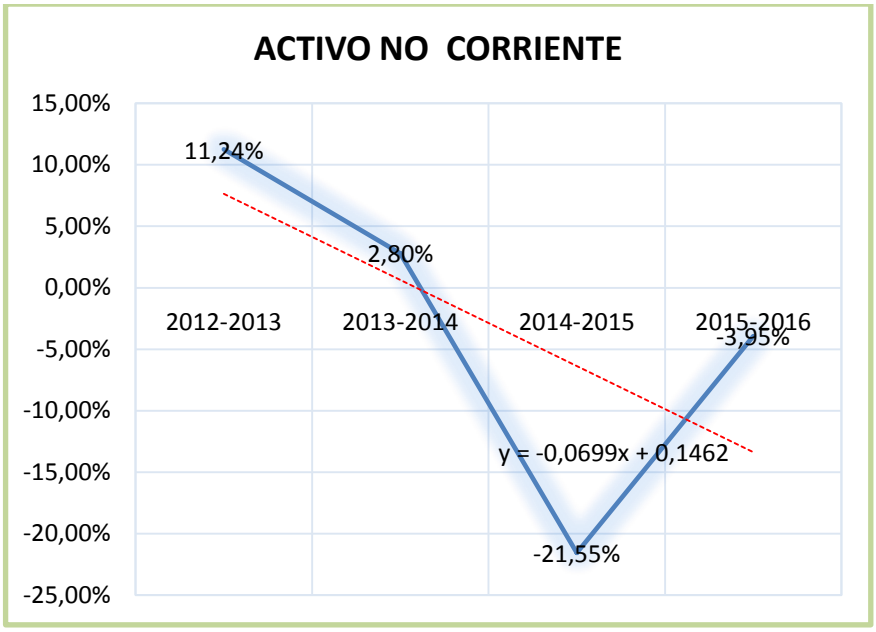

Figura 30. R. Valores Relativos Activo No C

Tabla 50

R. Valores Relativos Pasivo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PASIVO	34,16%	-14,73%	-16,52%	-18,24%

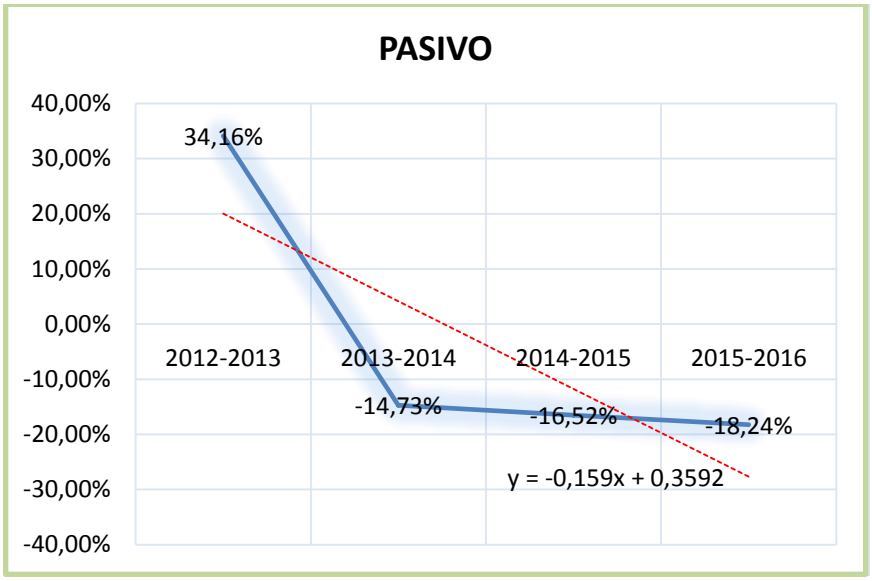

Figura 31. R. Valores Relativos Pasivo

Tabla 51

R. Valores Relativos Patrimonio

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PATRIMONIO	5,69%	3,13%	30,28%	3,61%

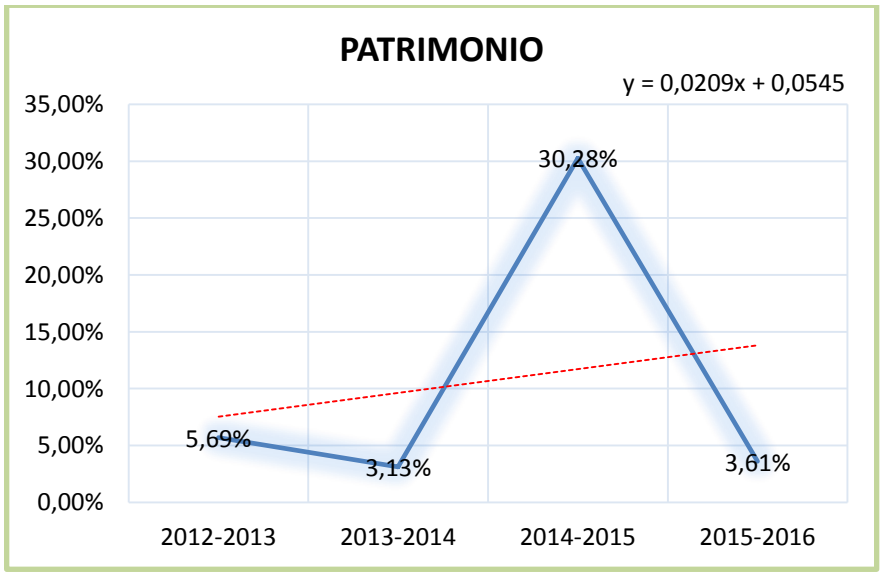

Figura 32. R. Valores Relativos Patrimonio

Pronóstico

Tabla 52

Pronóstico de las Cuentas E. El Ranchito

CUENTA	2016-2017	2017-2018	2018-2019	2019-2020
Activo	5,48%	0,012%	0,012%	0,012%
Activo No Corriente	6,06%	1,67%	1,64%	1,62%
Pasivo	8,13%	-3,61%	-3,75%	-3,89%
Patrimonio	3,34%	3,07%	2,98%	2,89%
Equipo de Cómputo y Software	25%	17%	15%	13%

Interpretación

Como resultado del análisis horizontal para el año 2016 en relación al año anterior en la cuenta Activo presenta una disminución de 7,43% por una cantidad de $ 501.172,82 con una tendencia decreciente y se estima un incremento de 0,012%, en la cuenta Activo No Corriente existe una disminución de 3,95% lo que representa una cantidad de $ 190.259,37 con una tendencia decreciente y dentro de cuatro años se estima un incremento de 1,62%, además la empresa presenta en Equipo de Cómputo y software un incremento para el año 2014 en relación al año 2013 de 162,63% por una cantidad de $ 34.411,10 desde ahí se observan incrementos para los años consecutivos por ello para el año 2016 versus el 2015 la cuenta incrementó en 19,12% por una cantidad de $ 12.439,25 y si se mantienen las políticas económicas se estima un incremento del 13% en los próximos cuatro años, por el contrario la cuenta Pasivo presenta una disminución de 18,24% por una cantidad de $ 621.818,44 y con un incremento en el Patrimonio de 3,61% por una cantidad de $120.645,62 reflejando una tendencia creciente.

Las principales cuentas del activo No Corriente son Propiedad Planta y Equipo, y para el año 2016 representa el 74,02% del total de activos por una cantidad de $4.623.133,28, en el año 2015 representó el 71,34%. Equipo de

Cómputo y software alcanzaron un valor de $77.487,31 y representa el 1,24% del total de Activos, en el año 2015 representaron el 0,96%.

Análisis y Diagnóstico

El incremento en la cuenta Equipo de Cómputo y Software se evidencia según (Guato, 2016) en su Informe por “la implementación del nuevo sistema ERP SAP Bussiness One, a mediados del año con el objetivo de obtener una mejor trazabilidad física y digital de adquisiciones, producción, ventas y calidad del producto.” El incremento del patrimonio es representativo por las ganancias acumuladas debido a que en el periodo se generaron pérdidas por gastos incurridos en la implementación de estrategias para mantener la posición de marca y la inversión realizada para la modificación y funcionamiento adecuado de la planta de tratamiento.

Prodicereal

Es una empresa que se dedica a la importación y exportación de productos agrícolas como maíz, quinua, lenteja, trigo, harinas, además productos de limpieza.

Tabla 53

P. Valores Relativos Eq. de Computación y Software

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
EQUIPO DE COMPUTACIÓN Y SOFTWARE	3,74%	7,11%	5,22%	22,70%

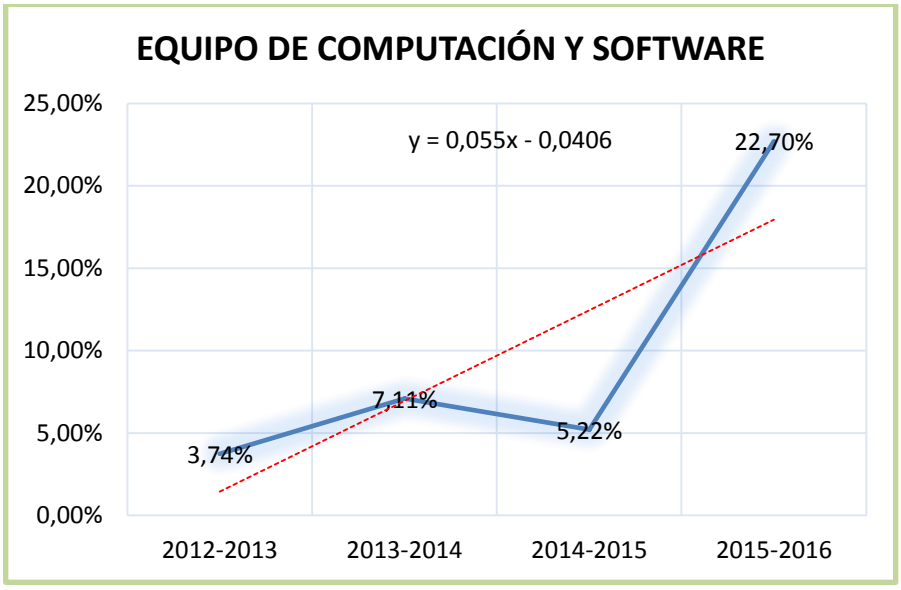

Figura 33. P. Valores Relativos Eq. de Computación y Software

Tabla 54

P. Valores Relativos Activo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO	12,61%	0,11%	-6,56%	14,56%

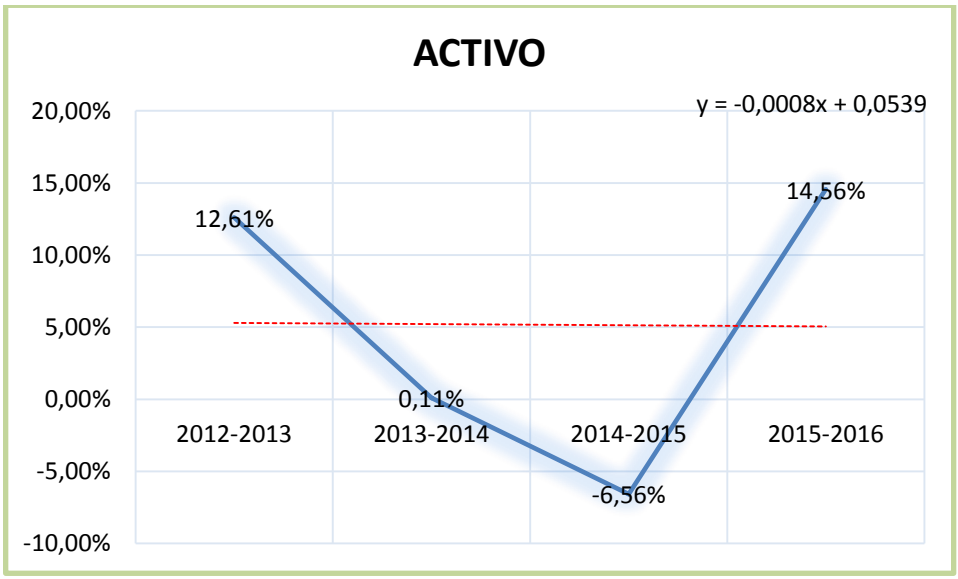

Figura 34. P. Valores Relativos Activo

Tabla 55

P. Valores Relativos Activo No C.

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO NO CORRIENTE	-13,51%	1,20%	5,64%	-4,87%

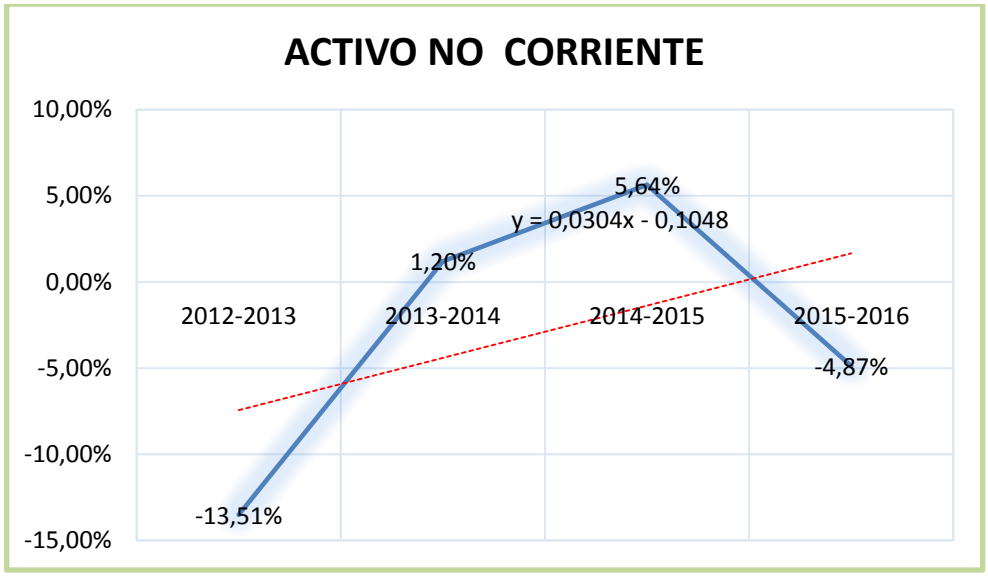

Figura 35. P. Valores Relativos Activo No C.

Tabla 56

P. Valores Relativos Pasivo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PASIVO	20,95%	-5,43%	-16,67%	37,46%

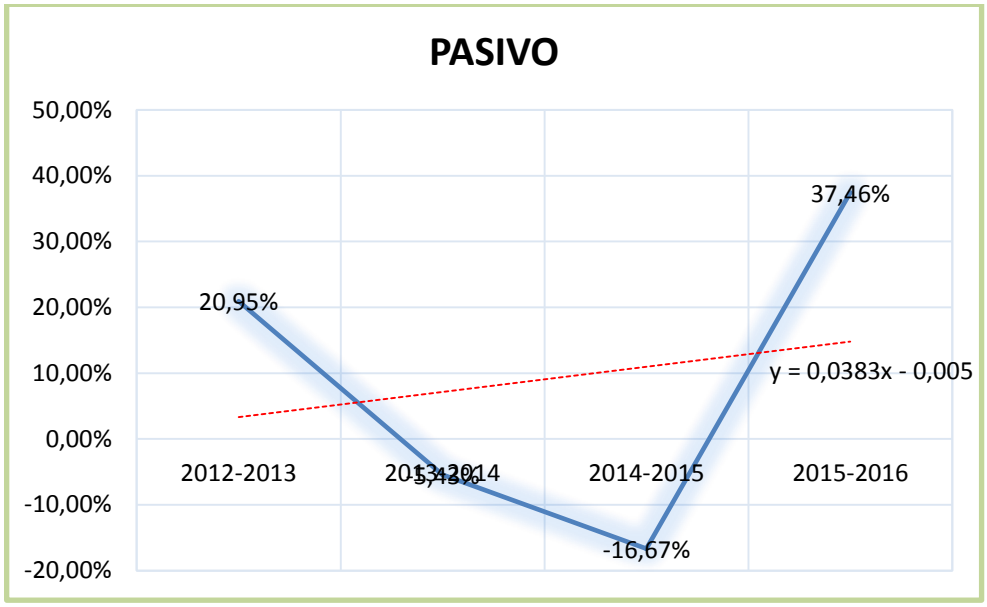

Figura 36. P. Valores Relativos Pasivo

Tabla 57

P. Valores Relativos Patrimonio

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PATRIMONIO	-8,63%	18,81%	20,59%	-27,95%

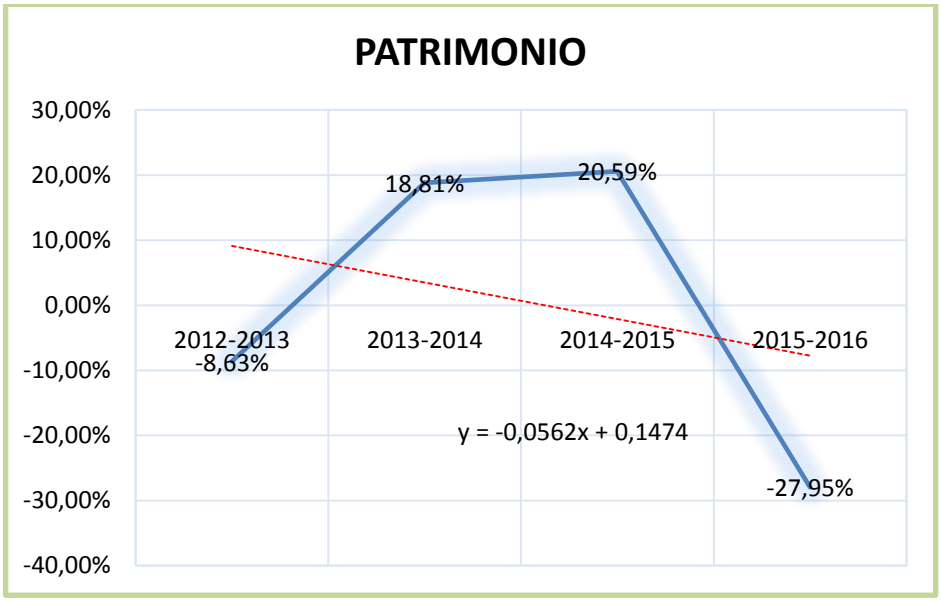

Figura 37. P. Valores Relativos Patrimonio

Pronóstico

Tabla 58

Pronóstico de las cuentas E. Prodicereal

CUENTA	2016-2017	2017-2018	2018-2019	2019-2020
Activo	-0,15%	2,828%	2,750%	2,677%
Activo No Corriente	-2,85%	-2,12%	-2,16%	-2,21%
Pasivo	-5,93%	2,95%	2,87%	2,79%
Patrimonio	20,32%	2,48%	2,42%	2,36%
Equipo de Cómputo y Software	1,13%	6,90%	6,45%	6,06%

Interpretación

Según los estados financieros publicados en la Superintendencia se puede observar que en el año 2015 los activos tienen un valor de $3.601.821,87, a diferencia del año 2016 con un valor de 4.126.291,41, lo que representa que los activos incrementaron en 14,56%. La cuenta Equipo de Computación y Software para el año 2016 en referencia al año 2015 incremento con el 22,70% por una cantidad de $2.539,00. Los Pasivos presentan un incremento del 37,46% con una cantidad de $876.913,02. EL patrimonio finalizó el año 2016 con una disminución de 27,95% por una cantidad de $352.4443,48 y se estima un incremento paulatino en los próximos cuatro años de 2,36%.

En el año 2016 la cuenta Equipo de computación y software representa el 0,33% del total de Activo y en el año 2015 representó el 0,31%. La cuenta Obligaciones con Instituciones Financieras representa el 31,44% del total del pasivo y la empresa tiene un capital de $682.073,76 que representa el 75,07% del total de Patrimonio.

Análisis y Diagnóstico

Dentro de la cuenta Propiedad Planta y Equipo tenemos presente la cuenta equipo de computación y software en la cual podemos observar que desde el

año 2012 al 2016 se presentan incrementos en la cuenta ocasionando una tendencia creciente y se estima que para los próximos tres años seguirá incrementando en un 6,45% es decir la empresa se preocupa por mantener actualizados sus equipos y software informáticos.

Parmalat

Ubicada en el Sector de Lasso Centro, panamericana Norte km.20, del Cantón Cotopaxi, dedicada a la elaboración, recolección, pasteurización, producción, comercialización, importación y exportación de toda clase de productos alimenticios, especialmente de derivados de leche, de frutas y de vegetales.

Tabla 59

Pt. Valores Relativos Equipo de Computación

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
EQUIPO DE COMPUTACIÓN	36,57%	56,41%	38,11%	-1,80%

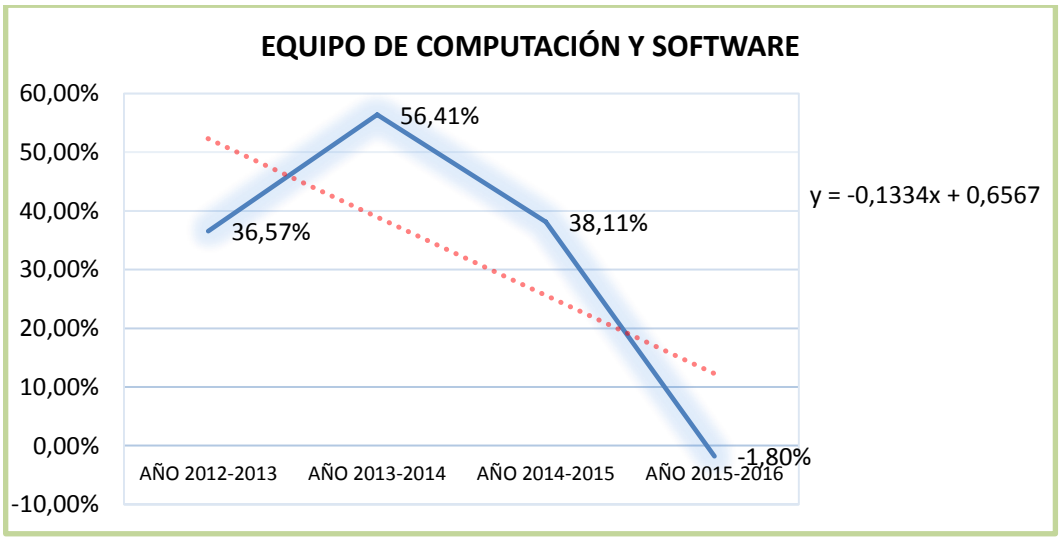

Figura 38. Pt. Valores Relativos Equipo de Computación

Tabla 60

Pt. Valores Relativos Activo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO	13,01%	27,04%	5,81%	-12,14%

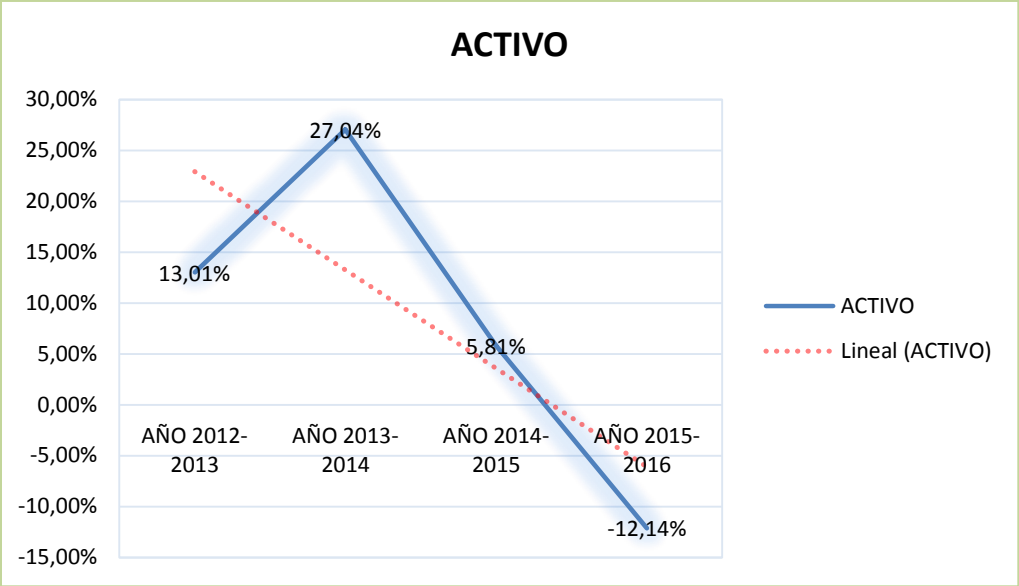

Figura 39. Pt. Valores Relativos Activo

Tabla 61

Pt. Valores Relativos Activo No C.

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO NO CORRIENTE	18,78%	12,26%	-0,89%	0,98%

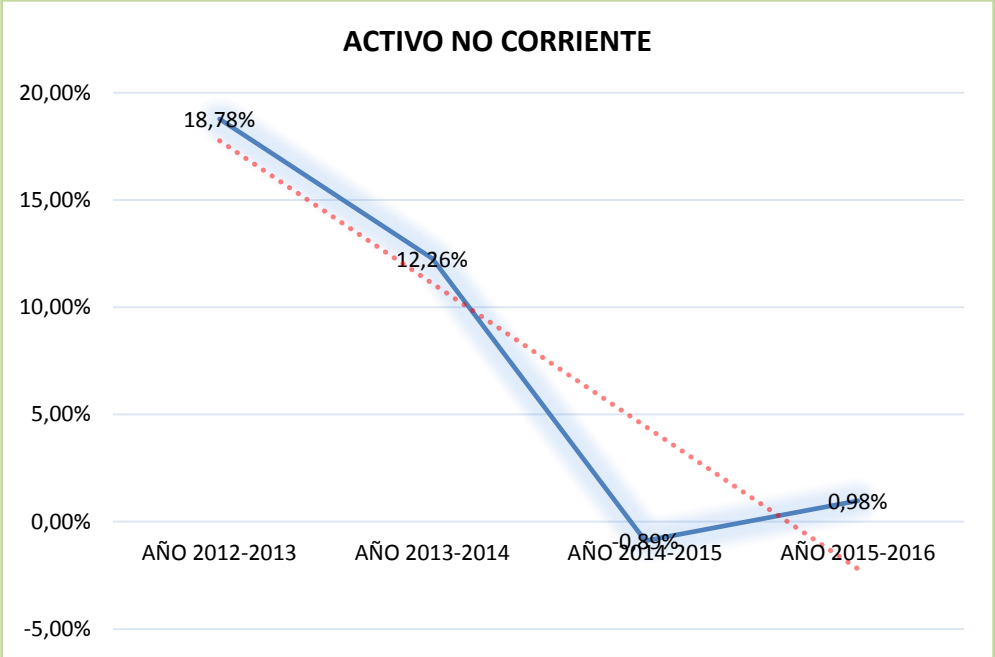

Figura 40. Pt. Valores Relativos Activo No C.

Tabla 62

Pt. Valores Relativos Pasivo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PASIVO	20,73%	-64,13%	22,20%	-39,07%

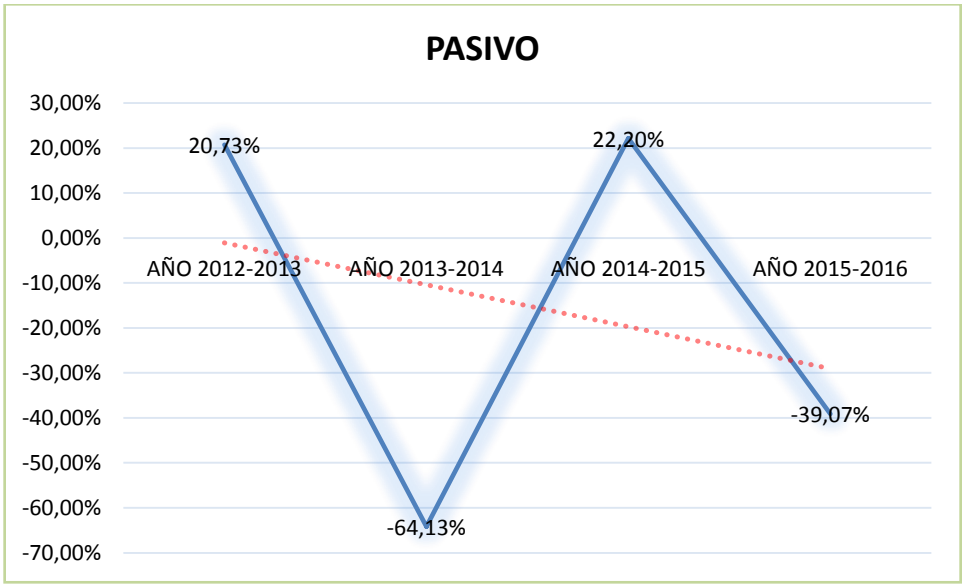

Figura 41. Pt. Valores Relativos Pasivo

Tabla 63

Pt. Valores Relativos Patrimonio

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PATRIMONIO	-50,88%	1881,71%	-0,22%	0,00%

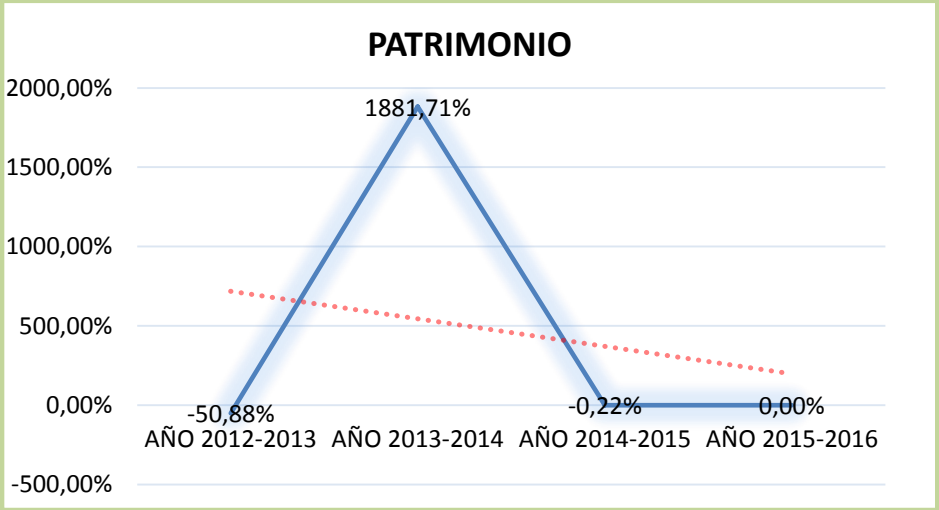

Figura 42. Pt. Valores Relativos Patrimonio

Pronósticos

Tabla 64

Pronósticos de las Cuentas E. Parmalat

CUENTA	2016-2017	2017-2018	2018-2019	2019-2020
Activo	19,99%	6,61%	6,20%	5,84%
Activo no corriente	10,63%	1,89%	2,57%	4,97%
Pasivo	-72,59%	-313,36%	42,31%	99,46%
Patrimonio	45,42%	19,85%	4,45%	16,38%
Equipo de computación	27,14%	14,60%	12,74%	11,30%

Interpretación

Mediante los respectivos estados de situación financiera de la empresa se presenta en la Cuenta del Activo para el año 2016 en relación al año 2015 una disminución de 12,14%, en la cuenta del Activo no Corriente se presenta un

incremento del 0,98%, en la cuenta del Equipo de Cómputo y software en el año 2015 con un valor de $32.236,56 en el año 2016 con un valor negativo de $2.099,36 que representa una disminución del 1,80%, en la cuenta del Pasivo se presenta una disminución del 39,07%, en la cuenta del Patrimonio de presenta un decrecimiento del 39,07% en los últimos años 2015-2016.

Análisis y Diagnóstico

En la cuenta de Equipo de cómputo y Software se visualiza una tendencia decreciente en el que la empresa no realiza inversiones en tecnología, equipos, computadores, a más de ello la empresa trabajó en varios proyectos para su mejoramiento económico, la calidad y ampliación productiva, la empresa presenta proyecciones estables para sus próximos años.

Familia Sancela

Empresa forma parte del grupo SCA Hygiene Products y se dedica a la fabricación de productos higiénicos de aseo personal, así también productos de papel, plásticos y cosméticos.

Tabla 65

F. Valores Relativos Equipo de Computación

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
EQUIPO DE COMPUTACIÓN Y SOFTWARE	10,65%	0,77%	12,83%	8,16%

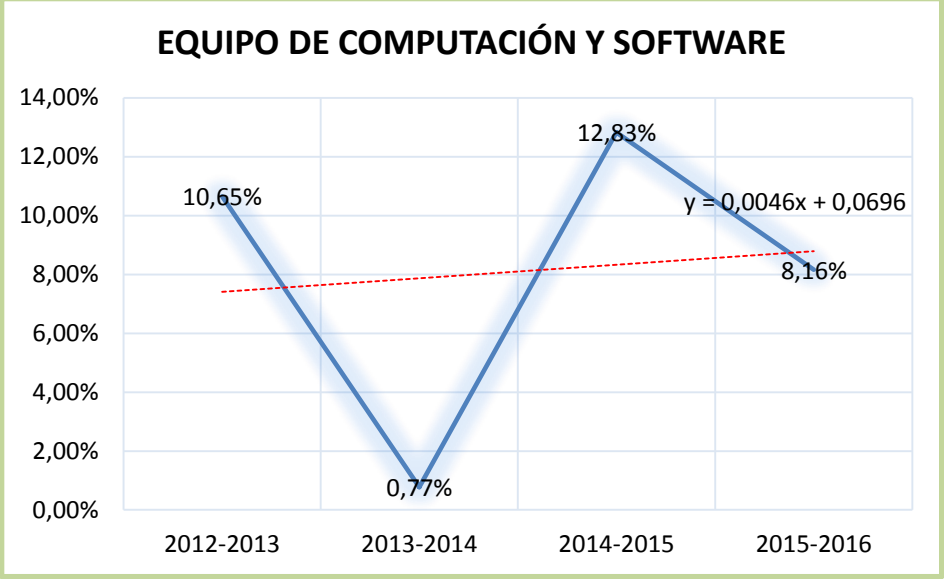

Figura 43. F. Valores Relativos Equipo de Computación

Tabla 66

F. Valores Relativos Activo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO	24,71%	14,71%	-0,10%	-2,65%

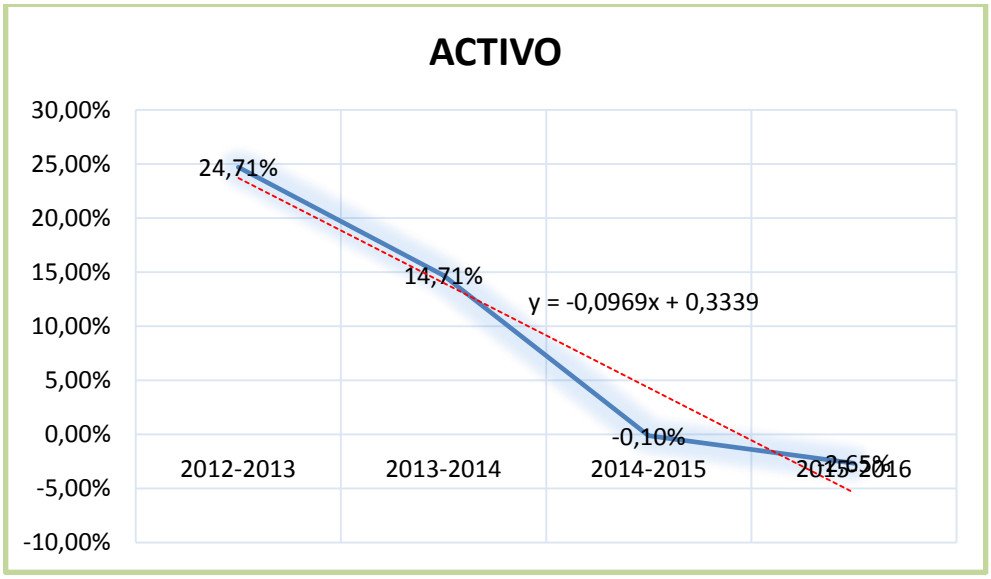

Figura 44. F. Valores Relativos Activo

Tabla 67

F. Valores Relativos Activo No C.

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO NO CORRIENTE	14,59%	6,99%	2,90%	5,11%

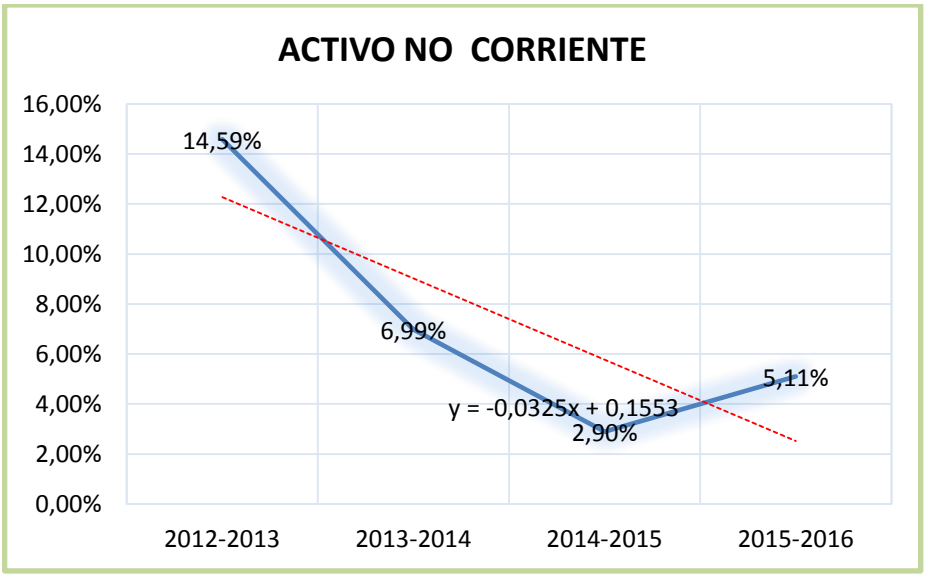

Figura 45. F. Valores Relativos Activo No C.

Tabla 68

F. Valores Relativos Pasivo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PASIVO	13,35%	13,28%	-12,98%	9,03%

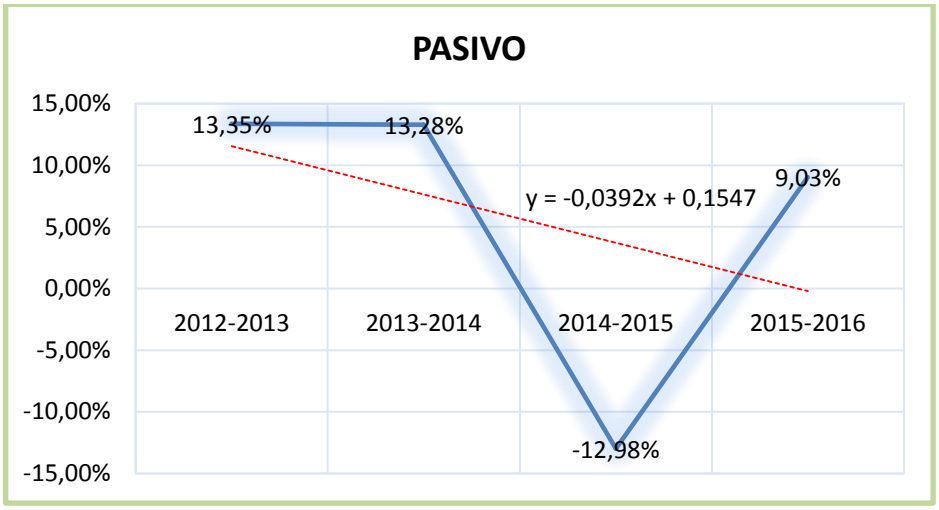

Figura 46. F. Valores Relativos Pasivo

Tabla 69

R. Valores Relativos Patrimonio

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PATRIMONIO	30,74%	15,37%	5,71%	-6,99%

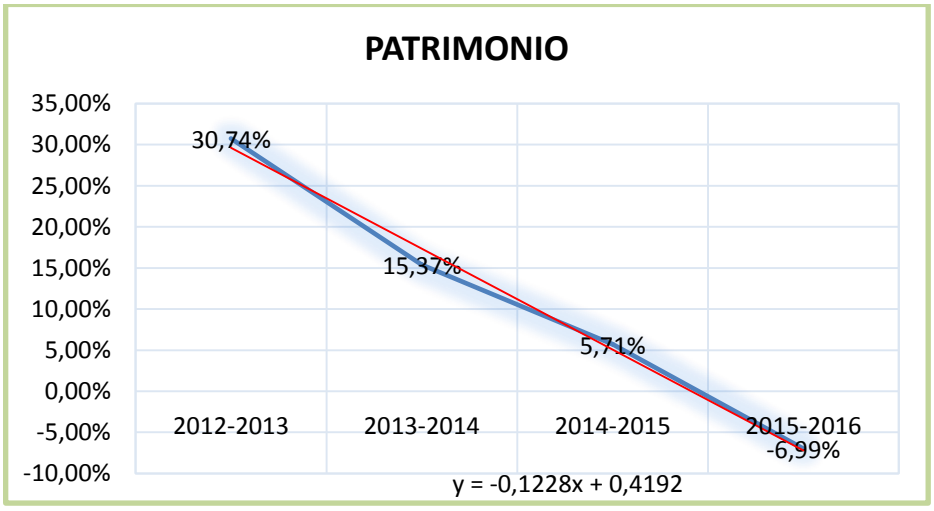

Figura 47. R. Valores Relativos Patrimonio

Pronóstico

Tabla 70

Pronósticos de las Cuentas E. Familia

CUENTA	2016-2017	2017-2018	2018-2019	2019-2020
Activo	14,21%	6,07%	5,72%	5,41%
Activo No Corriente	7,25%	5,40%	5,12%	4,87%
Pasivo	4,80%	3,29%	3,19%	3,09%
Patrimonio	18,31%	7,14%	6,67%	6,25%
Equipo de Cómputo y Software	5,09%	6,11%	5,75%	5,44%

Interpretación

La empresa para el año 2016 con relación al año 2015 presenta en la cuenta Activo una disminución de 2,65% por una cantidad de $ 2.741.636,00 y se estima un incremento de 5,41% dentro de cuatro años, en base a datos históricos. En el Activo No Corriente se observa un incremento de 5,11% por una cantidad de $ 1.998.426,20 y a cuatro años se estima un incremento de 4,8% si las políticas tanto internas como externas se mantienen. En Equipo de Computación y Software existe un incremento del 8,16% por una cantidad de $ 155.802,28 y se estima un incremento de 5,75% al en los próximos tres años. En la cuenta Pasivo se observa un incremento de 9,03% por una cantidad de $ 2.530.728,60 y para la cuenta Patrimonio presenta una disminución de 6,99% lo que representa una cantidad de $5.272.364,90. La cuenta Efectivo y Equivalentes al Efectivo representan el 23,54% del total de activos, equipo de cómputo y software el 2,05%, el capital de la empresa representa el 49,08% por una cantidad de $34.419.695 del total de patrimonio.

Análisis y Diagnóstico

Se puede observar en sus estados financieros que la empresa posee una gran inversión en equipo de computación y software y a través de los años han ido incrementando su inversión por ello se observa una tendencia creciente,

además los activos de la empresa para el año 2016 disminuyeron considerablemente y reflejan una tendencia decreciente al igual que el patrimonio.

Provefrut S.A.

Establecida en 1989 es una compañía que produce y comercializa vegetales de alta calidad, competitivos en grandes volúmenes, además de ser exportadora de productos congelados agroindustriales a los mercados de Norte América, Europa y Asia.

Tabla 71

Pr. Valores Relativos Equipo de Computación

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
EQUIPO DE COMPUTACIÓN Y SOFTWARE	-81,02%	70,60%	411,41%	19,37%

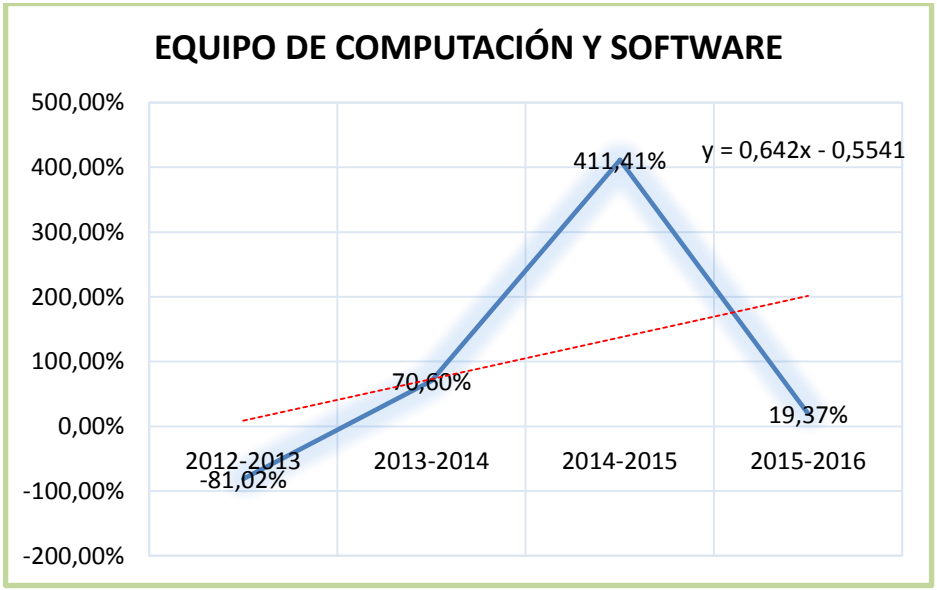

Figura 48. Pr. Valores Relativos Equipo de Computación

Tabla 72

Pr. Valores Relativos Activo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO	4,69%	13,09%	14,87%	-3,18%

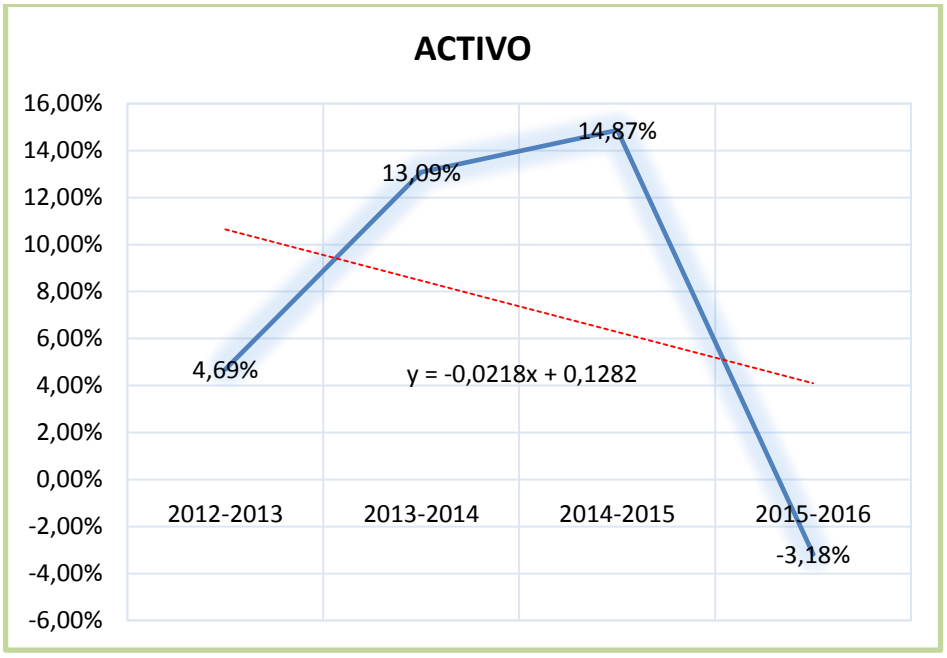

Figura 49. Pr. Valores Relativos Activo

Tabla 73

Pr. Valores Relativos Activo No C.

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO NO CORRIENTE	-6,07%	0,87%	25,04%	-16,53%

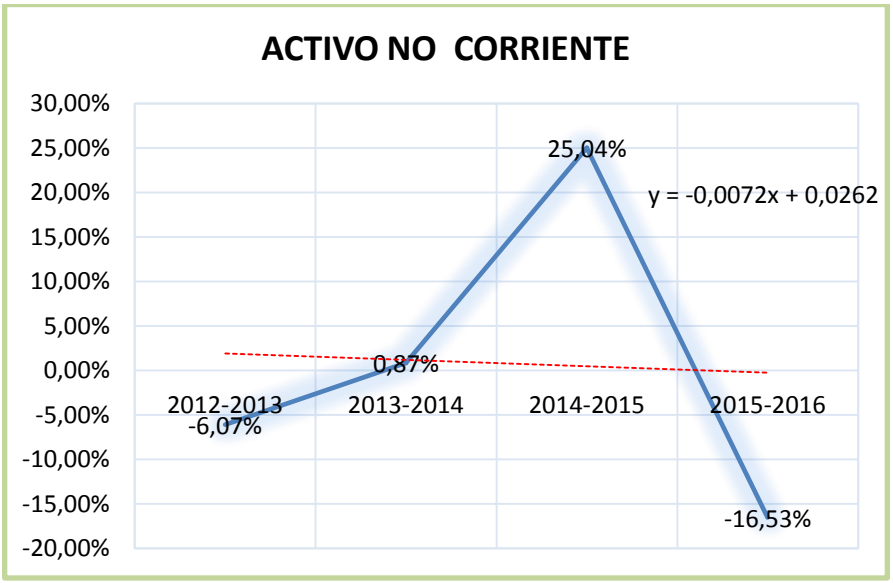

Figura 50. Pr. Valores Relativos Activo No C.

Tabla 74

Pr. Valores Relativos Pasivo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PASIVO	4,21%	7,10%	15,24%	-16,75%

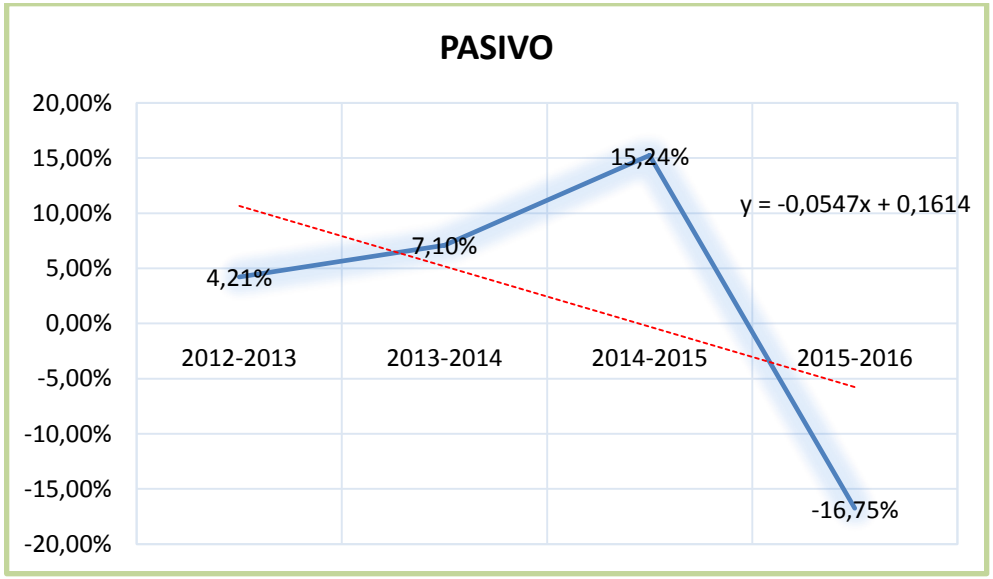

Figura 51. Pr. Valores Relativos Pasivo

Tabla 75

Pr. Valores Relativos Patrimonio

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PATRIMONIO	5,04%	17,46%	14,63%	5,91%

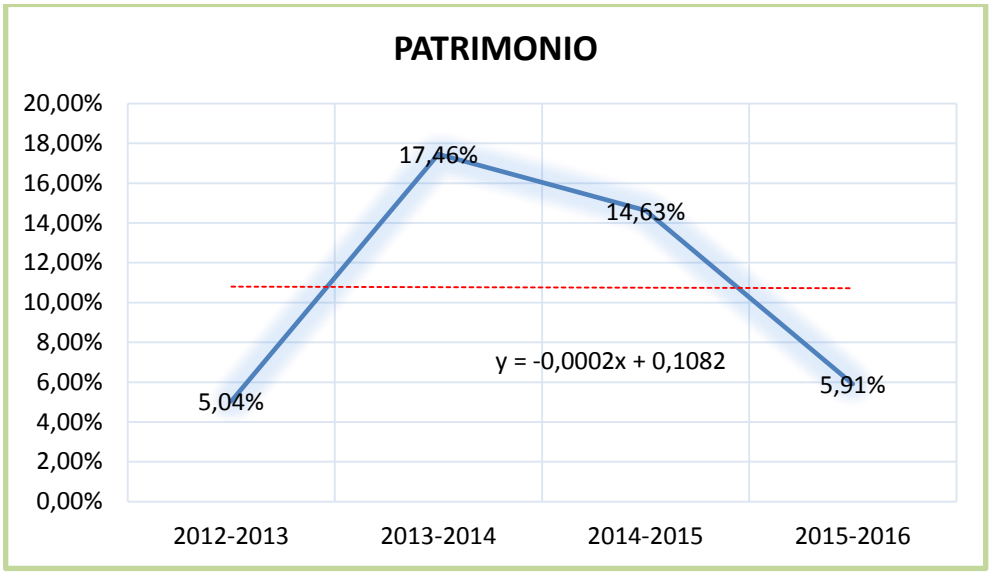

Figura 52. Pr. Valores Relativos Patrimonio

Interpretación

Según Velásquez (2016) en su informe de calificación de riesgo establece que las cuentas de:

> Los activos totales de la compañía presentaron una tendencia creciente desde USD 29,07 millones en 2012 hasta USD 40,05 millones en 2015, los incrementos se concentraron en los activos corrientes, Para octubre de 2016 el total de los activos fue de USD 38,65 millones; reflejando un decrecimiento del 3,49% frente a diciembre de 2015, debido a una baja en sus cuentas por cobrar relacionadas y propiedad planta y equipo. Al 31 de octubre de 2016, los pasivos descendieron en relación a diciembre de 2015, ubicándose en USD 13,76 millones, específicamente por el decremento de las obligaciones con costo de corto plazo.

La cuenta patrimonio incrementó el 5,91% para el año 2016 versus 2015 por una cantidad de $1.419.370,18, no presentan tendencia alguna y se estima que en cuatro años la cuenta incrementará en un 7,09%.

Dentro de los activos la cuenta principal son los activos financieros con el 57,78% del total de activos por una cantidad de $22.421.450, la cuenta Equipo de computación y software apenas representa el 0,56% del total de activos para el año 2016 por una cantidad de $217.106. Dentro de los pasivos tenemos la cuenta con mayor representatividad a provisiones por beneficios a empleados con el 19,23% del total de pasivos por un valor de $2.573.493. Las ganancias netas del periodo representan el 4,64% del total del Patrimonio por un valor de $1.179.034.

Análisis y Diagnóstico

La situación financiera al 31 de diciembre del 2016 guarda positiva consistencia entre las cuentas de activos, pasivos y patrimonio; tanto en valores como en relaciones porcentuales, reflejando una buena posición pese a la crisis internacional y la recesión ecuatoriana, además se observa que la utilidad guarda consistencia con los ejercicios anteriores.

Industria de Licores Ecuatorianos Licorec S.A.

Ubicada en la parroquia de Tanicuchi, Nuevo Lasso, Paso lateral S/N y Panamericana Sur, Cotopaxi, dedicada la producción de licores.

Tabla 76

L. Valores Relativos Eq. de Computación

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
EQUIPO DE COMPUTACIÓN	3366,17%	17,59%	13,73%	0,22%

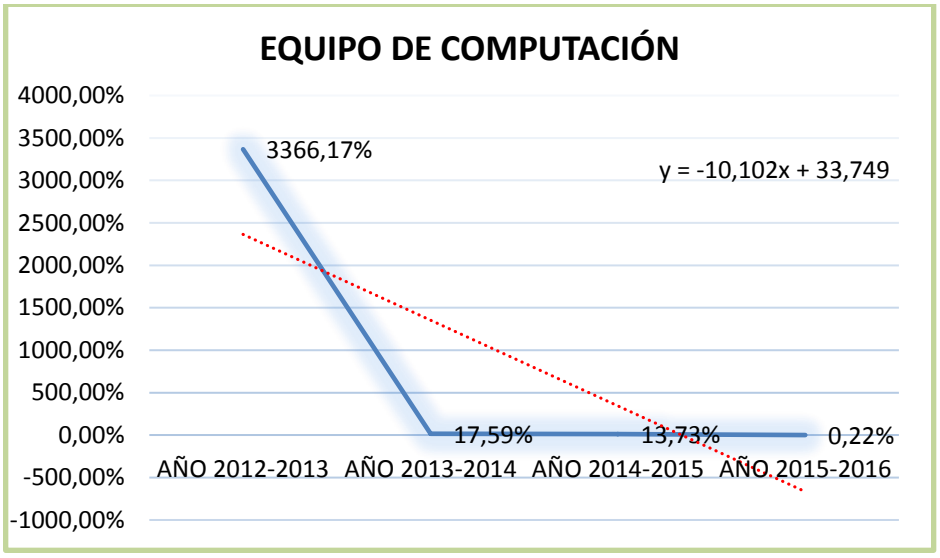

Figura 53. L. Valores Relativos Eq. de Computación

Tabla 77

L. Valores Relativos Activo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO	130,43%	34,31%	29,91%	-8,83%

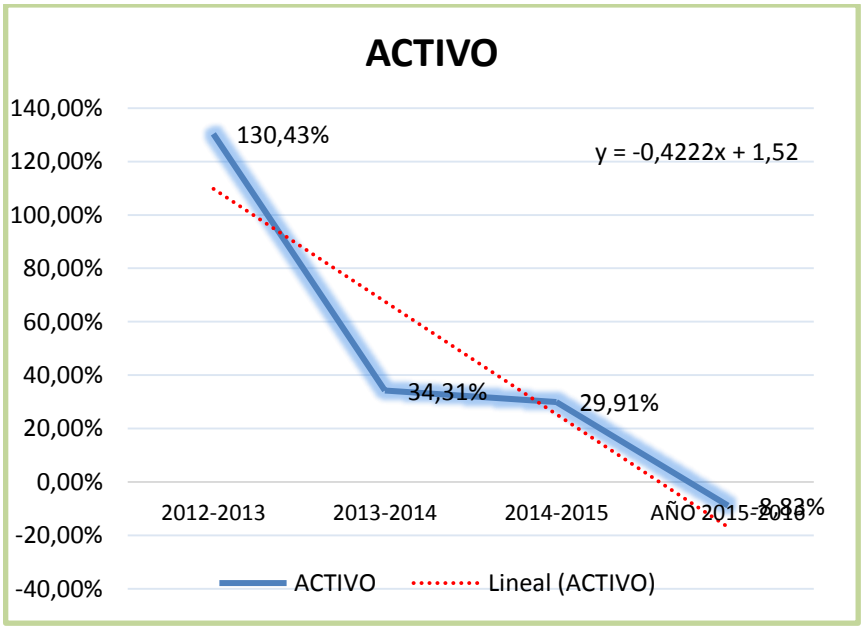

Figura 54. L. Valores Relativos Activo

Tabla 78

L. Valores Relativos Activo No C.

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO NO CORRIENTE	233,88%	-0,97%	43,79%	-25,98%

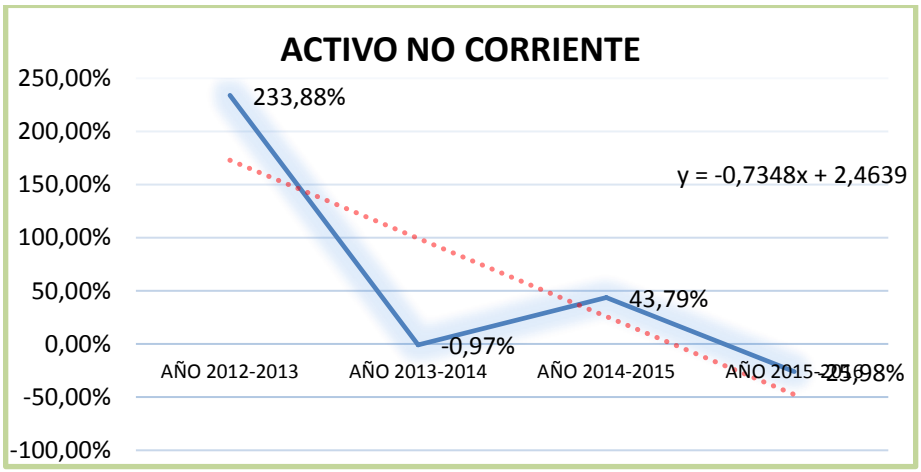

Figura 55. L. Valores Relativos Activo No C.

Tabla 79

L. Valores Relativos Pasivo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PASIVO	145,05%	36,20%	-2,45%	-8,10%

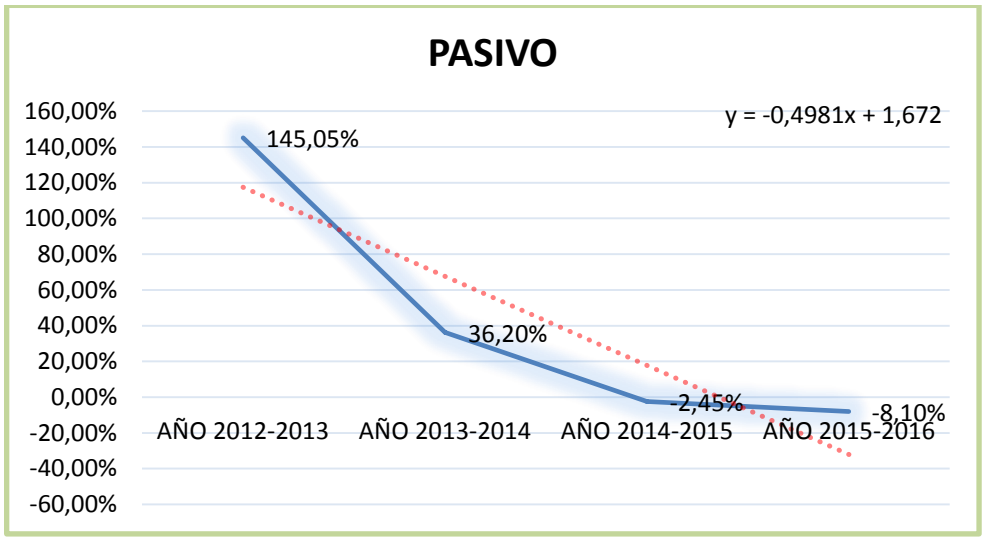

Figura 56. L. Valores Relativos Pasivo

Tabla 80

L. Valores Relativos Patrimonio

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PATRIMONIO	-2942,42%	68,62%	-443,76%	-11,87%

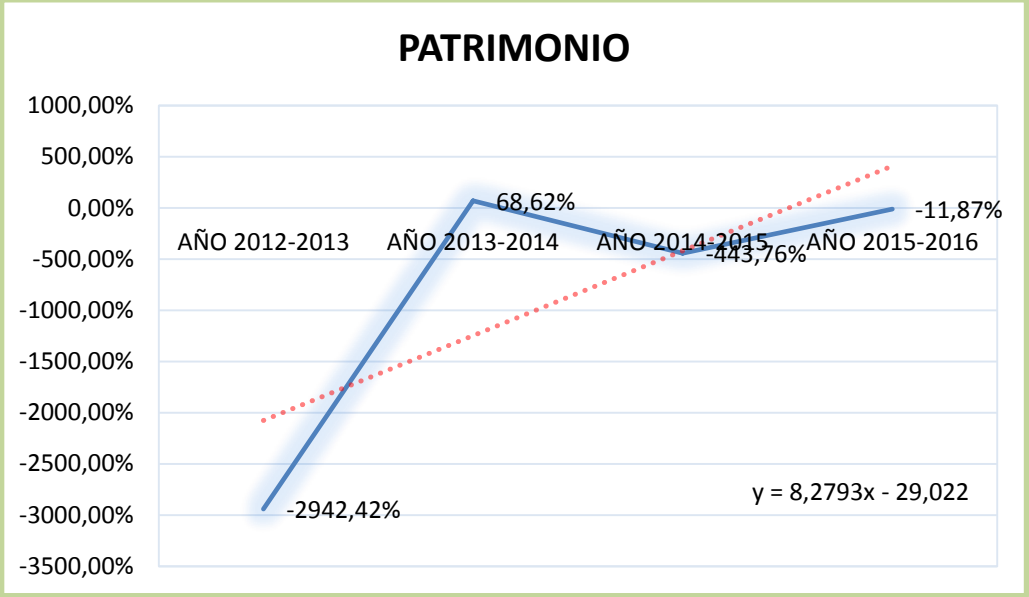

Figura 57. L. Valores Relativos Patrimonio

Pronósticos

Tabla 81

Pronósticos de las Cuentas E. Licorec

CUENTA	2016-2017	2017-2018	2018-2019	2019-2020
Activo	34,53%	14,29%	12,50%	11,11%
Activo no corriente	0,45	12,61%	11,19%	10,07%
Pasivo	35,16%	11,84%	10,59%	9,58%
Patrimonio	31,81%	25,16%	20,10%	16,74%
Equipo de Computación	39,11%	15,88%	13,70%	12,05%

Interpretación

Con la información reflejada en los estados de situación financiera se presenta en la Cuenta del Activo para el año 2016 en relación al año 2015 una

disminución del 8,83%, en la cuenta del Activo no Corriente se presenta una disminución del 35,98%, en la cuenta del Equipo de Cómputo y software en el año 2015 con un valor de $8.555.642,73 en el año 2016 con un valor $7.862.765,63 se presenta un incremento del 0,22%, en la cuenta del Pasivo se presenta una disminución del 8,10%, en la cuenta del Patrimonio de presenta una disminución del 11,87%.

Análisis y Diagnóstico

Las variaciones históricas que presenta la Industria en las cuentas del Activo se presenta una reducción donde se realiza inversiones del mismo modo las cuenta del Pasivo va disminuyendo hasta llegar con valores negativos, en el patrimonio se visualiza en un periodo que hay un incremento, al mismo tiempo se presenta la cuenta Equipo de cómputo y software que del año 2012 al año 2013 hubo un incremento del 3366,17% y en los próximos años hasta el año 2016 se visualiza variaciones mínimas ya que hubo la inversión necesaria siendo un factor importante para el funcionamiento de la Industria.

El comportamiento de las proyecciones que presenta la empresa para los años 2017 al 2020 se muestra una tendencia normal, este sería en el caso en el que se mantengan las condiciones de impuestos, leyes, entre otras normativas.

Dávalos Larreategui Industrias Procesadoras DLIP S.A.

Ubicada en la parroquia de Tanicuchi, Nuevo Lasso, Panamericana Norte, Cotopaxi, dedicada al procesamiento de alimentos para obtener materias primas.

Tabla 82

D. Valores Relativos Eq. de Computación

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
EQUIPO DE COMPUTACIÓN	125,52%	156,88%	-47,31%	188,18%

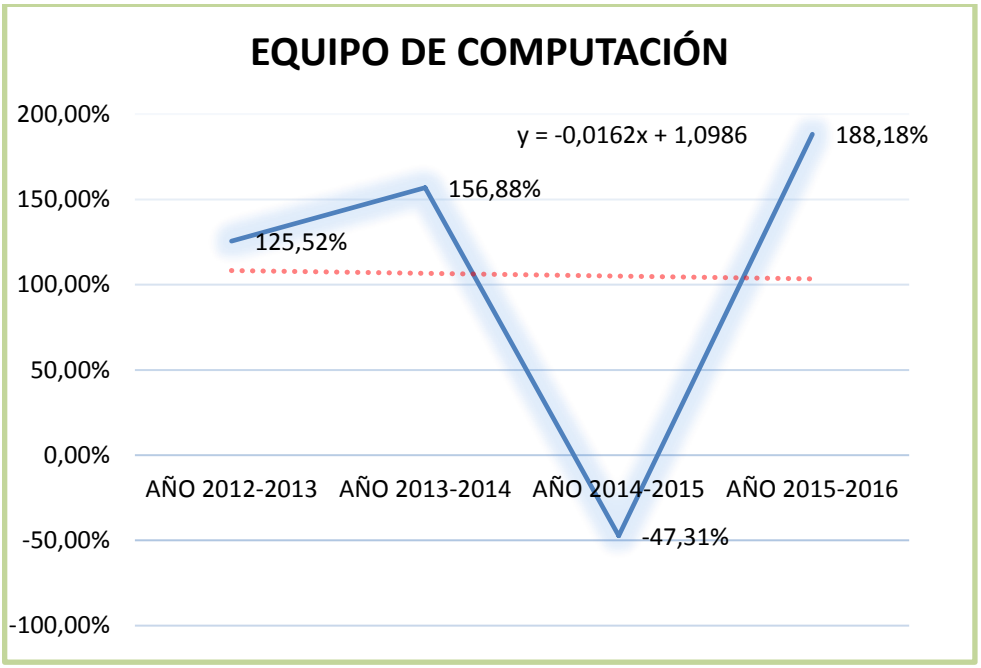

Figura 58. D. Valores Relativos Eq. de Computación

Tabla 83

D. Valores Relativos Activos Intangibles

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVOS INTANGIBLES	-86,72%	-26%	2429%	41%

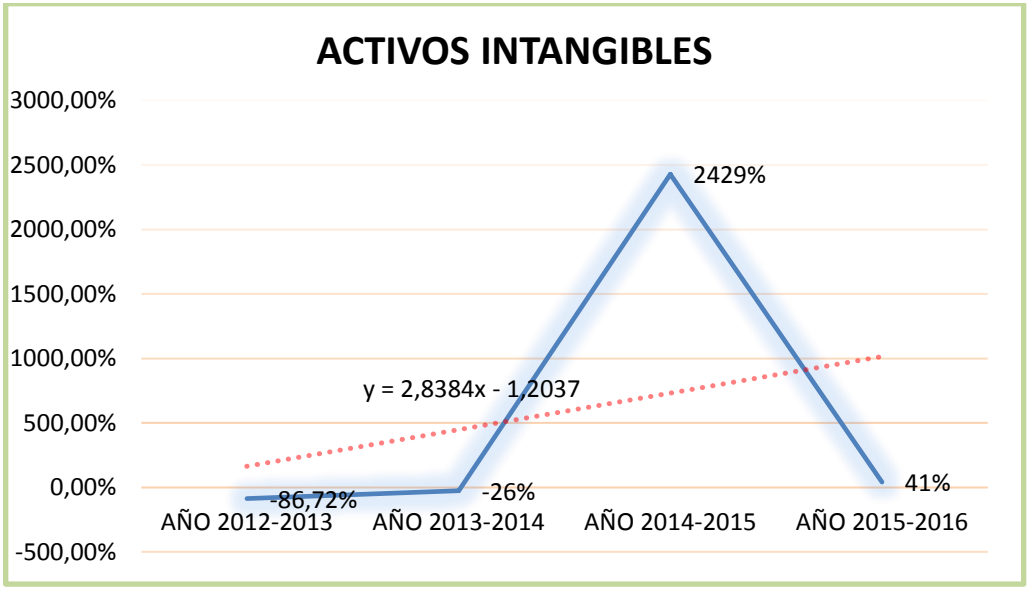

Figura 59. D. Valores Relativos Activos Intangibles

Tabla 84

D. Valores Relativos Activo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO	57,96%	138,55%	14,61%	27,97%

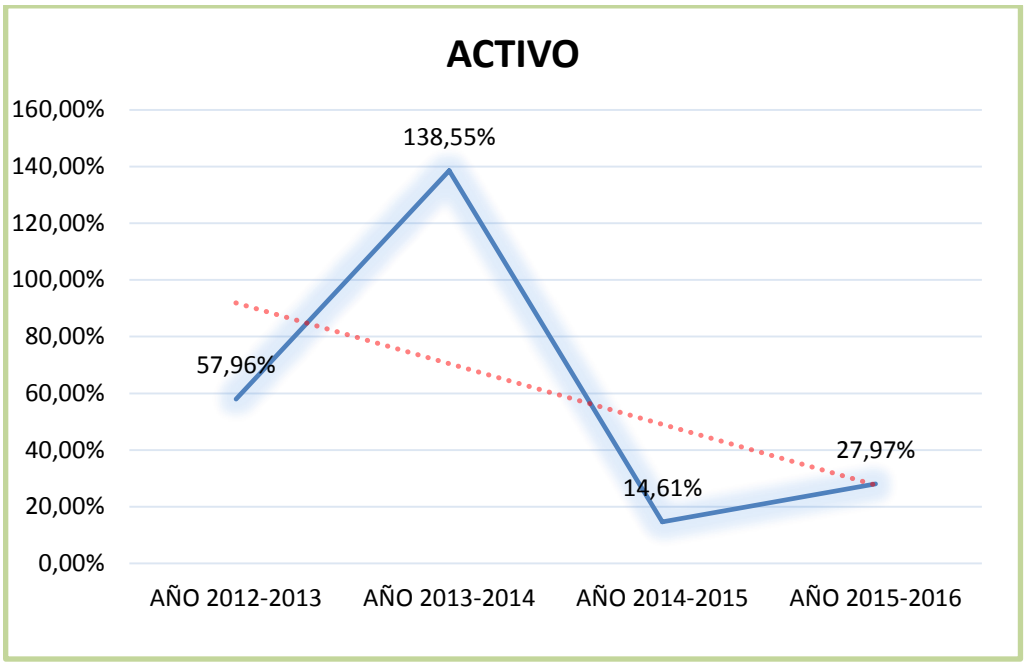

Figura 60. D. Valores Relativos Activo

Tabla 85

D. Valores Relativos Activos No Corriente

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO NO CORRIENTE	56,15%	-100,00%	0,00	10,90%

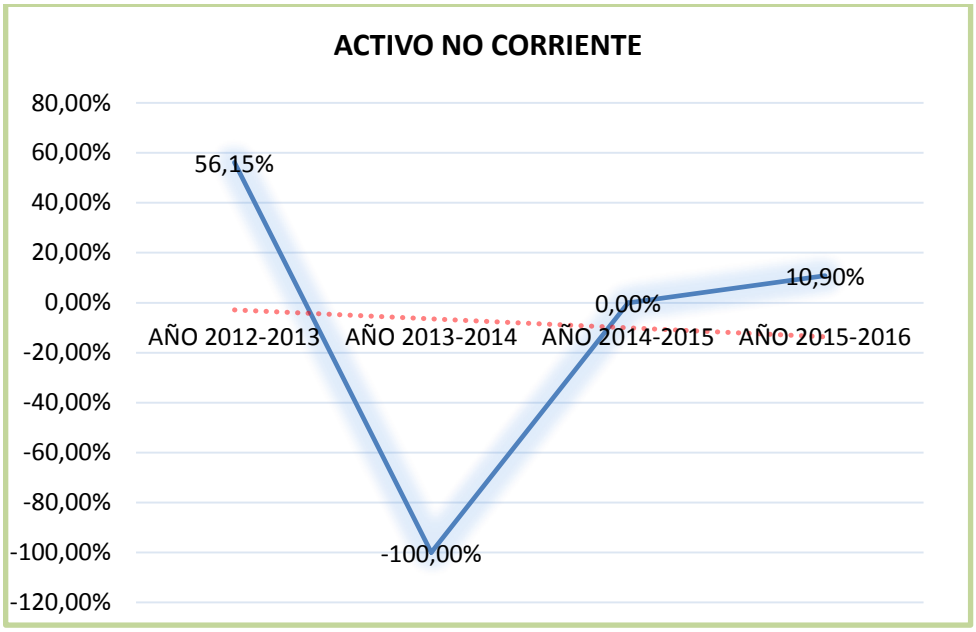

Figura 61. D. Valores Relativos Activos No Corriente

Tabla 86

D. Valores Relativos Pasivo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PASIVO	54,63%	-6,06%	54,15%	53,56%

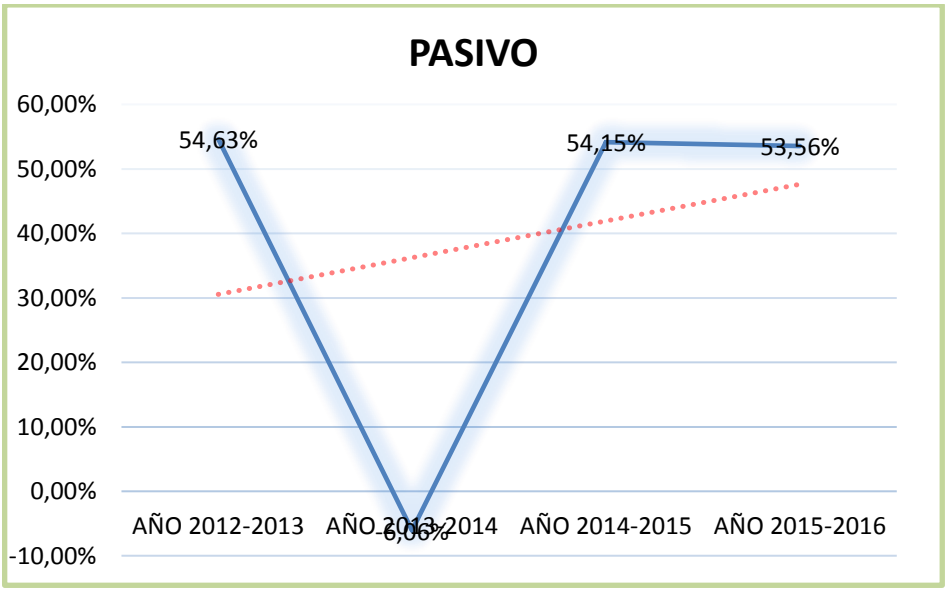

Figura 62. D. Valores Relativos Pasivo

Tabla 87

D. Valores Relativos Patrimonio

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PATRIMONIO	819,52%	5705,05%	-10,01%	0,67%

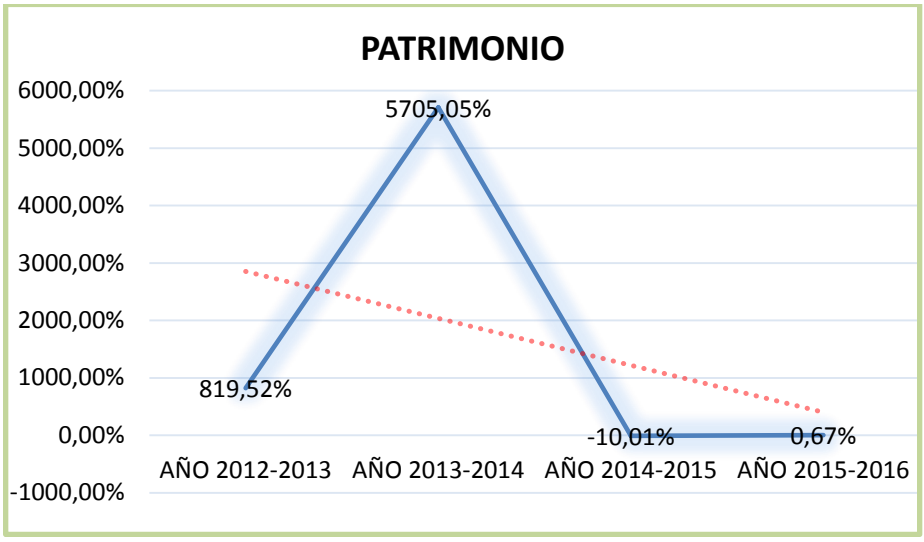

Figura 63. D. Valores Relativos Patrimonio

Pronósticos

Tabla 88

Pronósticos de las cuentas E. DLPA

CUENTA	2016-2017	2017-2018	2018-2019	2019-2020
Activo	22,61%	17,40%	14,82%	12,91%
Activo no corriente	14,31%	28,93%	26,23%	7,13%
Pasivo	4,88%	18,91%	19,31%	11,78%
Patrimonio	51,47%	18,34%	3,23%	17,93%
Equipo de computación	3,41%	18,02%	15,27%	13,25%
Activo intangible	4,18%	20,14%	16,76%	14,36%

Interpretación

Con la información reflejada en los estados de situación financiera se presenta en la Cuenta del Activo para el año 2016 en relación al año 2015 se presenta un incremento de 27,97%, en la cuenta del Activo no Corriente se presenta un incremento del 10,90%, en la cuenta del Equipo de Cómputo y software en el año 2015 con un valor de $5.379,01 en el año 2016 con un valor $15.501,48 se presenta un incremento del 188,18%, en la cuenta de Activo Intangible presenta un incremento del 40,99%, en la cuenta del Pasivo se presenta un incremento del 53,56%, en la cuenta del Patrimonio de presenta un incremento del 0,67%.

Análisis y Diagnóstico

En la industria presentó una inversión considerable en la Cuenta Equipo de Cómputo y software en relación con el año 2015 con $5.379,01 para el año 2016 de $15.501,48 obtenido un incremento del 188,18% la cual es importante, pues se nota que tiene mayor inversión en tecnología y mayor control en la misma, dentro de sus proyecciones la cuenta Equipo de Cómputo presenta proyecciones estables de crecimiento donde se estima que adquieren nuevos implementos en tecnología, a la vez se visualiza que la empresa tiene porcentajes positivos donde se presume un buen desarrollo de crecimiento empresarial y económico.

Industria De Acero Del Ecuador Cía. Ltda. Induacero

Ubicada en la Provincia de Cotopaxi, Cantón Latacunga, Parroquia Ignacio Flores, Barrió el Niagara en la Panamericana Sur, Dedicada a la Fabricación de Equipo Industrial, Tanques, Intercambiadores de calor, Remolques, Maquinaria Utilizada en la Industria Lechera, Ensamblaje de carros de Bomberos.

Tabla 89

I. Valores Relativos Eq. de Computación

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
EQUIPO DE COMPUTACIÓN	4,23%	-3,67%	0,00%	0,00%

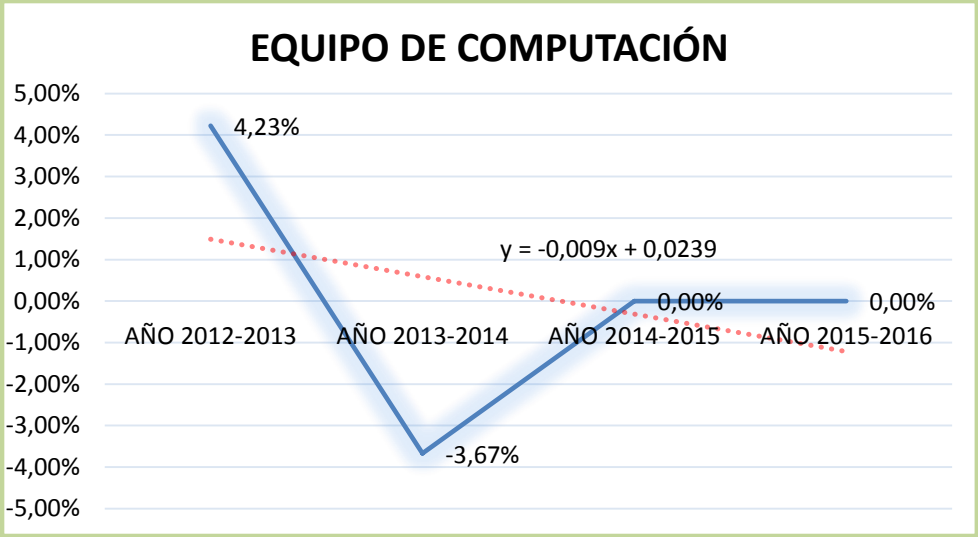

Figura 64. I. Valores Relativos Eq. de Computación

Tabla 90

I. Valores Relativos Activos

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO	12,78%	36,69%	-27,11%	9,02%

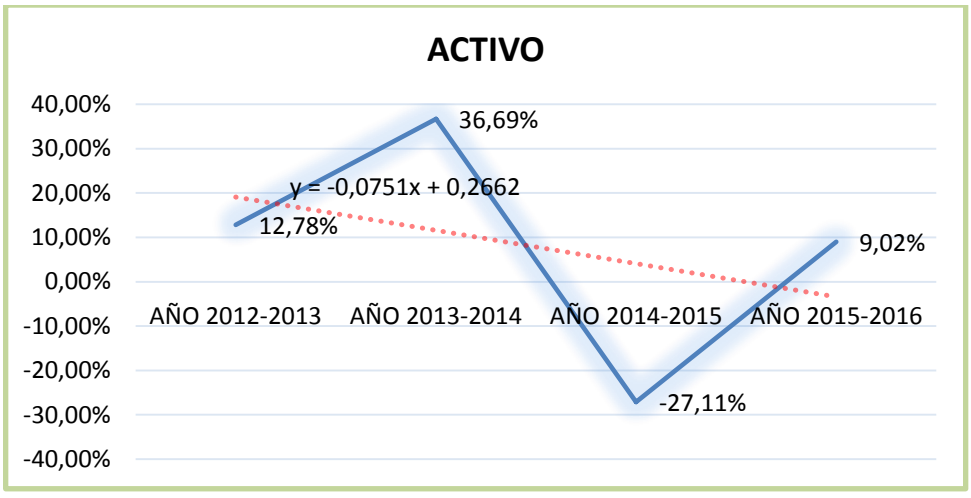

Figura 65. I. Valores Relativos Activos

Tabla 91

I. Valores Relativos Activos

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO NO CORRIENTE	17,91%	-100%	0%	-2,46%

Figura 66. I. Valores Relativos Activos

Tabla 92

I. Valores Relativos Pasivo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PASIVO	11,98%	45,76%	-40,30%	21,43%

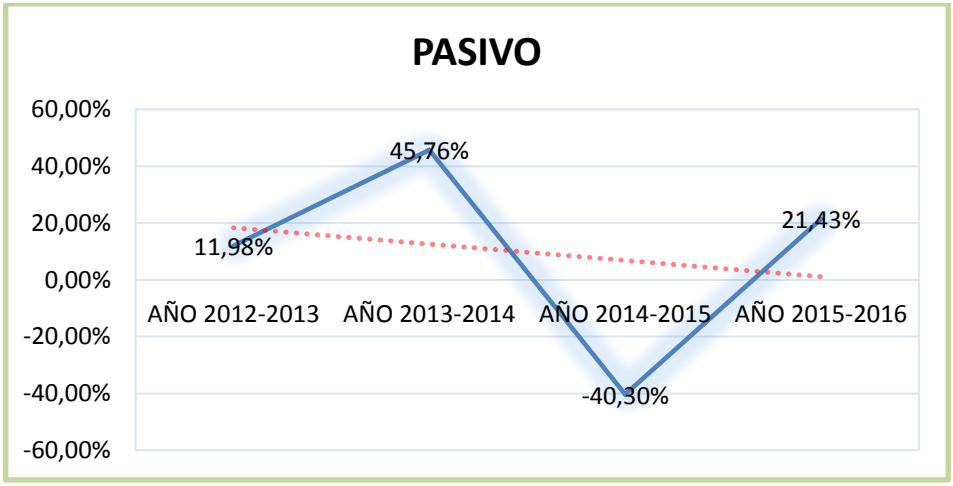

Figura 67. I. Valores Relativos Pasivo

Tabla 93

I. Valores Relativos Patrimonio

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PATRIMONIO	14,94%	12,95%	17,44%	-12,31%

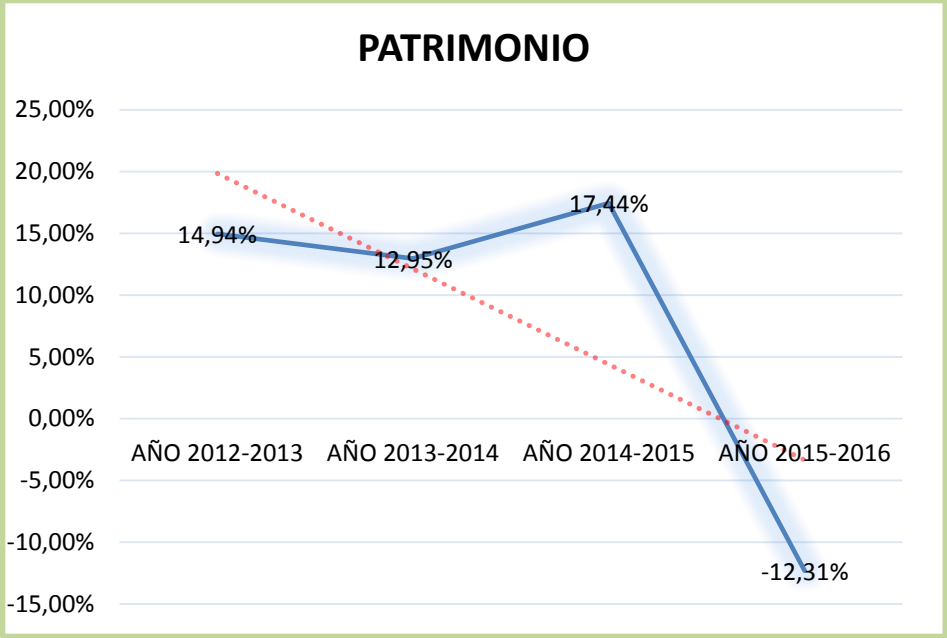

Figura 68. I. Valores Relativos Patrimonio

Pronóstico

Tabla 94

Pronósticos de las cuentas E. Induacero

CUENTA	2016-2017	2017-2018	2018-2019	2019-2020
Activo	9,18%	3,33%	3,23%	3,13%
Activo no corriente	16,26%	6,84%	6,41%	6,02%
Pasivo	5,50%	1,77%	1,74%	1,71%
Patrimonio	17,93%	6,66%	6,24%	5,87%
Equipo de computación	-0,22%	-0,30%	-0,30%	-0,30%

Interpretación

Con la información reflejada en los estados de situación financiera se presenta en la Cuenta del Activo para el año 2016 en relación al año 2015 se

presenta un incremento de 9,02%, en la cuenta del Activo no Corriente se presenta una disminución del 2,46%, en la cuenta del Equipo de Cómputo y software no existe incremento, en la cuenta del Pasivo se presenta un incremento del 21,43%, en la cuenta del Patrimonio de presenta una Disminución del 12,31%.

Análisis y Diagnóstico

Según el Gerente de la empresa (2016), La crisis económica que se agudizo en el Ecuador, durante el año 2016, afectó directamente al crecimiento empresarial de Induacero; dejando ganancias poco rentables para la empresa, dentro de sus proyecciones en los próximos 4 años en su cuenta Equipo de Cómputo se presenta un decrecimiento con sus porcentajes no representativos de preocupación más bien se diría que en la cuenta se presentarán las depreciaciones de las activos.

Fuentes San Felipe S.A. SANLIC

Ubicada en la ciudad de Latacunga, Barrio San Felipe, en las calles Cuba y en el pasaje Eloy Alberto Sánchez, dedicada a La extracción, embotellamiento y venta al mercado nacional e internacional de toda clase de aguas minerales y naturales, etc.

Tabla 95

S. Valores Relativos Eq. de Computación

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
EQUIPO DE COMPUTACIÓN	9,50%	15,33%	13,14%	6,29%

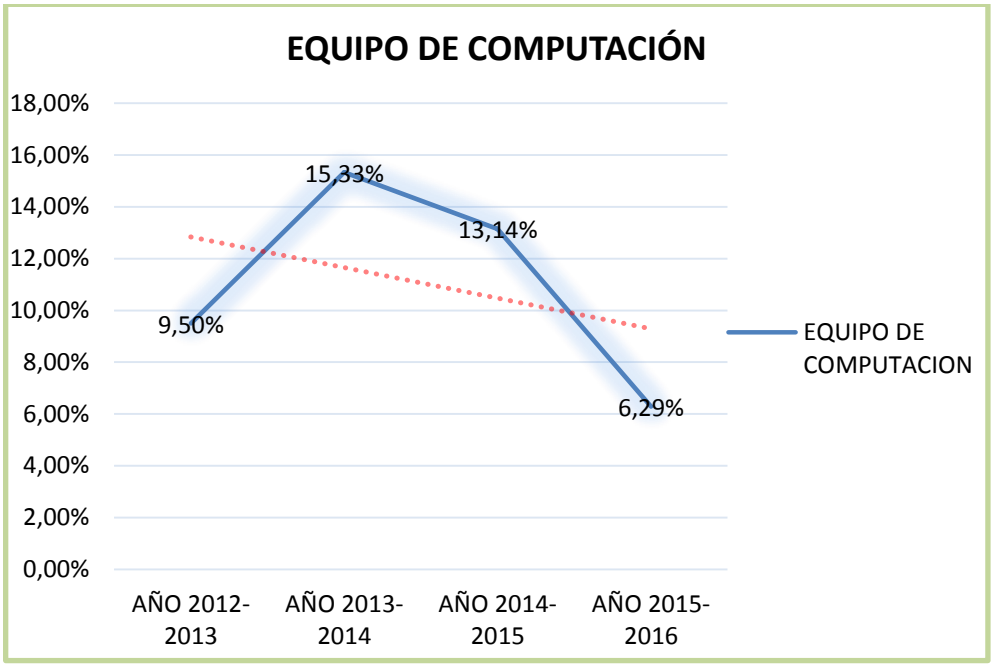

Figura 69. S. Valores Relativos Eq. de Computación

Tabla 96

S. Valores Relativos Activo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO	9,40%	1,53%	-5,07%	13,34%

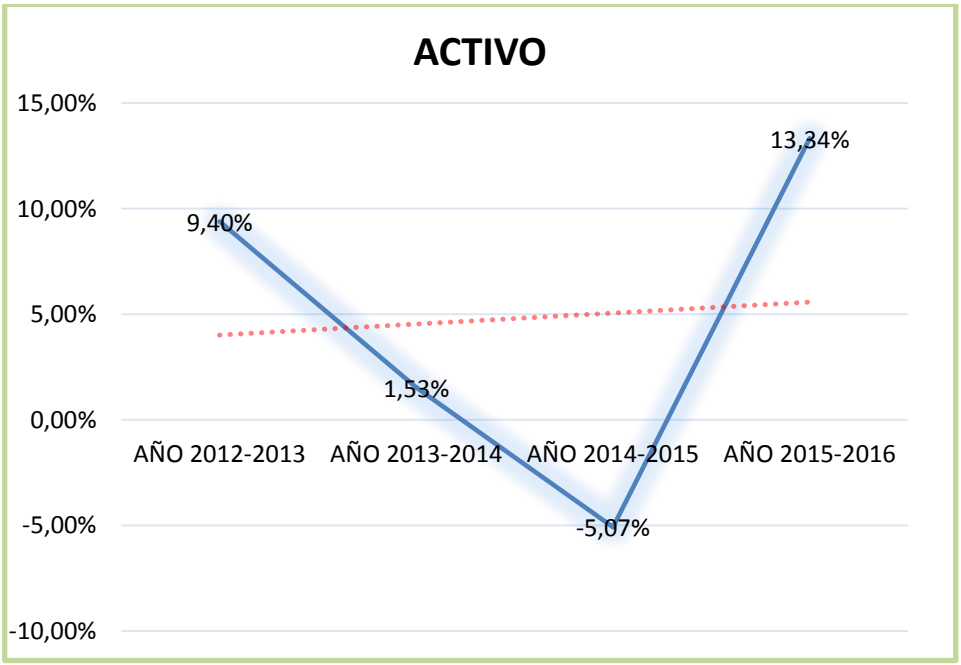

Figura 70. S. Valores Relativos Activo

Tabla 97

S. Valores Relativos Activo No C.

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO NO CORRIENTE	27,96%	9,69%	-3,65%	-9,85%

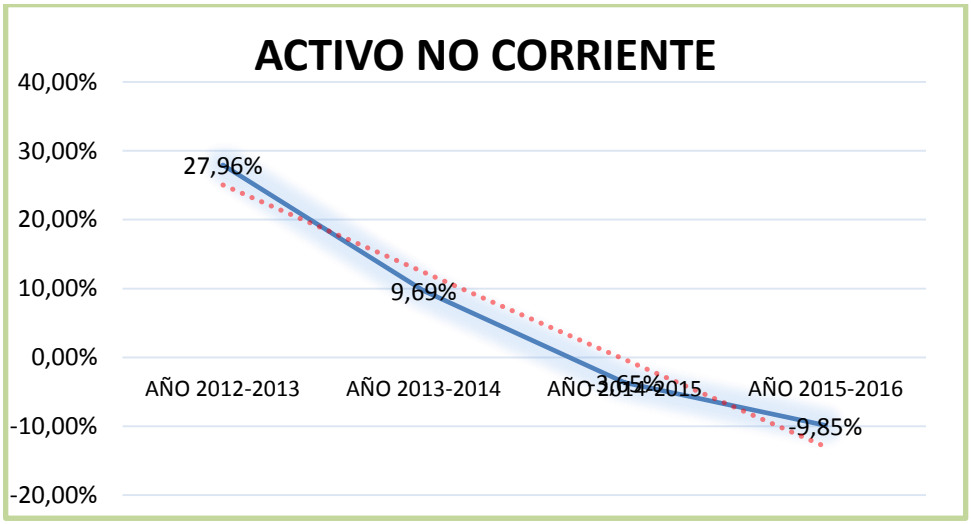

Figura 71. S. Valores Relativos Activo No C.

Tabla 98

S. Valores Relativos Pasivo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PASIVO	19,60%	6,02%	1,77%	18,02%

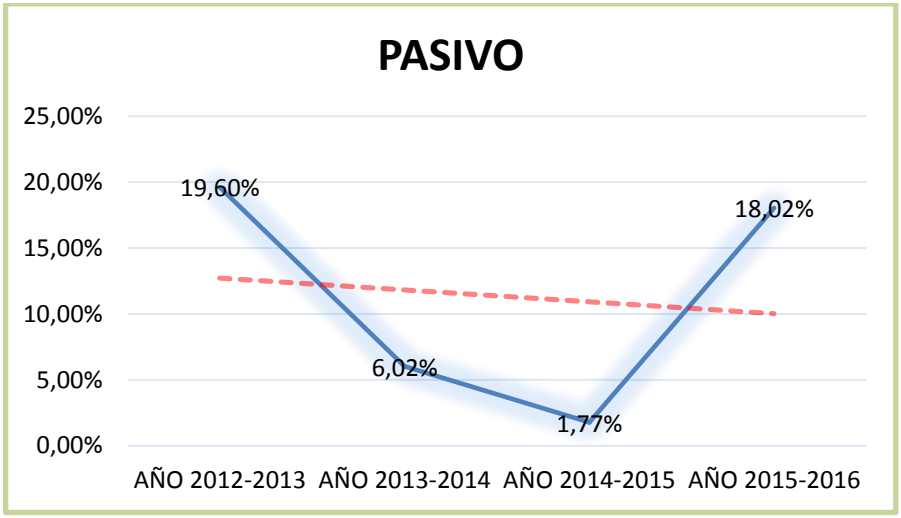

Figura 72. S. Valores Relativos Pasivo

Tabla 99

S. Valores Relativos Patrimonio

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PATRIMONIO	1,51%	-2,57%	-11,87%	7,97%

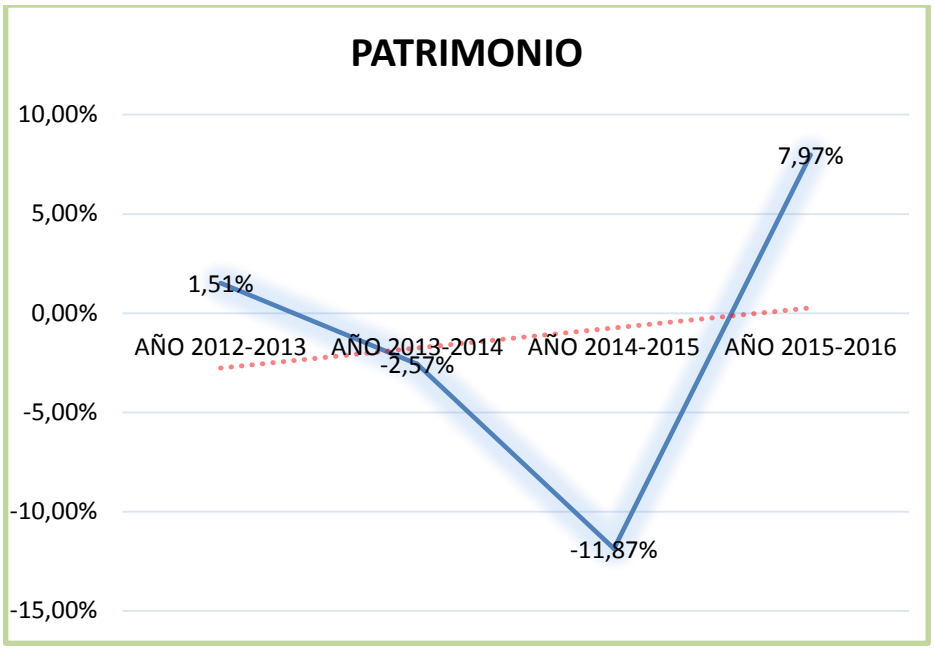

Figura 73 S. Valores Relativos Patrimonio

Pronóstico

Tabla 100

Pronósticos de las Cuentas Patrimonio

CUENTA	2016-2017	2017-2018	2018-2019	2019-2020
Activo	0,08%	2,93%	2,85%	2,77%
Activo no corriente	15,19%	3,64%	3,51%	3,39%
Pasivo	4,90%	7,14%	6,66%	6,25%
Patrimonio	-5,96%	-2,95%	-3,04%	-3,14%
Equipo de computación	20,45%	4,64%	8,33%	7,69%

Interpretación

Con la información reflejada en los estados de situación financiera de la empresa se constatan en la Cuenta del Activo para el año 2016 en relación al

año 2015 se presentó un incremento de 13,34%, en la cuenta del Activo no Corriente se presenta una disminución del 9,85%, en la cuenta del Equipo de Cómputo y software en el año 2015 con un valor de $64.499,32 en el año 2016 con un valor $68.555,72 se presenta un incremento del 6,29%, en la cuenta del Pasivo se presenta un incremento del 18,02%, en la cuenta del Patrimonio de presenta un incremento del 7,97%.

Análisis y Diagnóstico

La empresa en el año 2016 presentó bajos porcentajes de crecimiento económico debido a la economía baja Ecuatoriana ya que el Banco Central en los 9 meses del año índico en la parte Manufacturera decreció un 2,2% así afectando en el consumo de los productos de la empresa así lo menciona el gerente de la entidad, además de ello se estima que la empresa en los sus próximos años tenga crecimientos empresariales y económicos, también la empresa pueda adquirir nuevas activos de tecnología.

Construcciones Ulloa Cía. Ltda.

Ubicada en la Ciudad de Latacunga en el Barrio el Niagara, Ciudadela Ignacio Flores, Calles Panamericana Sur y Patuca, Provincia de Cotopaxi, dedicada a la fabricación, comercialización y mantenimiento de vehículos de emergencia como: motobombas, autobombas, vehículos de rescate, ambulancias.

Tabla 101

U. Valores Relativos Eq. de Cómputo

CUENTA	AÑO 2013-2014	AÑO 2014-2015	AÑO 2015-2016
EQUIPO DE COMPUTACIÓN	100,00%	0,00%	0,00%

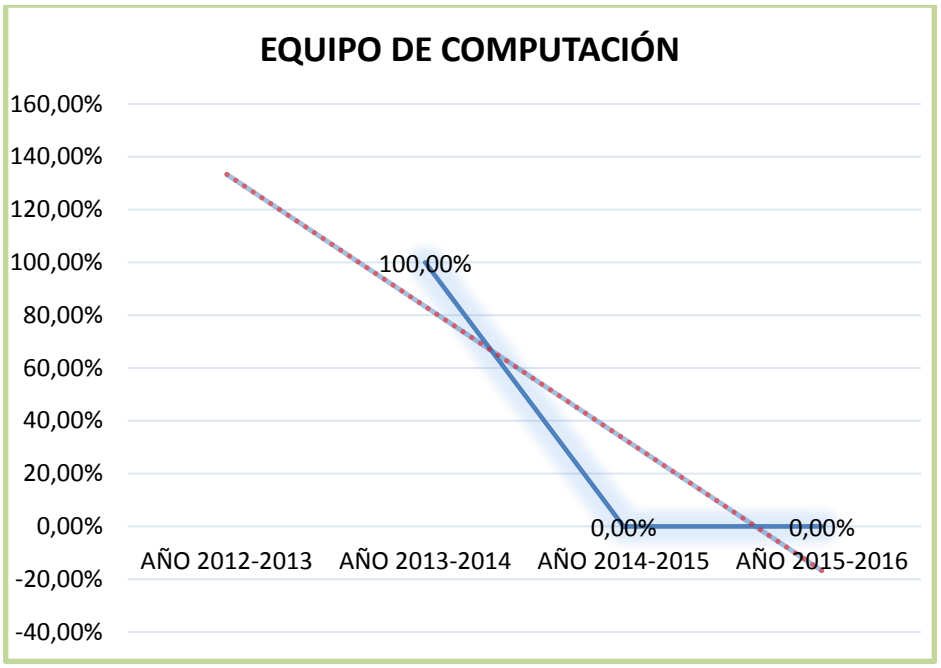

Figura 74 U. Valores Relativos Eq. de Cómputo

Tabla 102

U. Valores Relativos Activo

CUENTA	AÑO 2013-2014	AÑO 2014-2015	AÑO 2015-2016
ACTIVO	0%	-28,00%	-8,40%

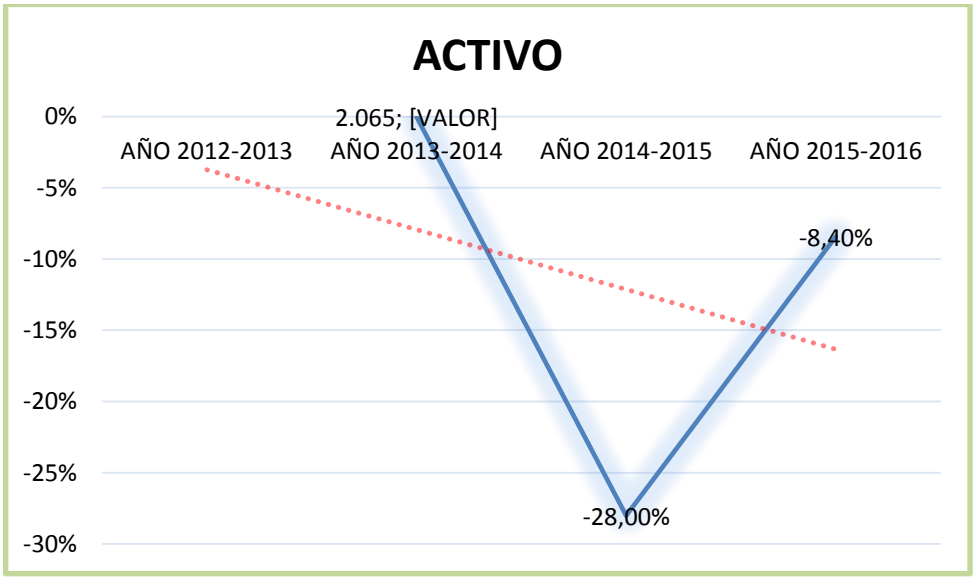

Figura 75 U. Valores Relativos Activo

Tabla 103

U. Valores Relativos Activo No C.

CUENTA	AÑO 2013-2014	AÑO 2014-2015	AÑO 2015-2016
ACTIVO NO CORRIENTE	0%	61,79%	-8,01%

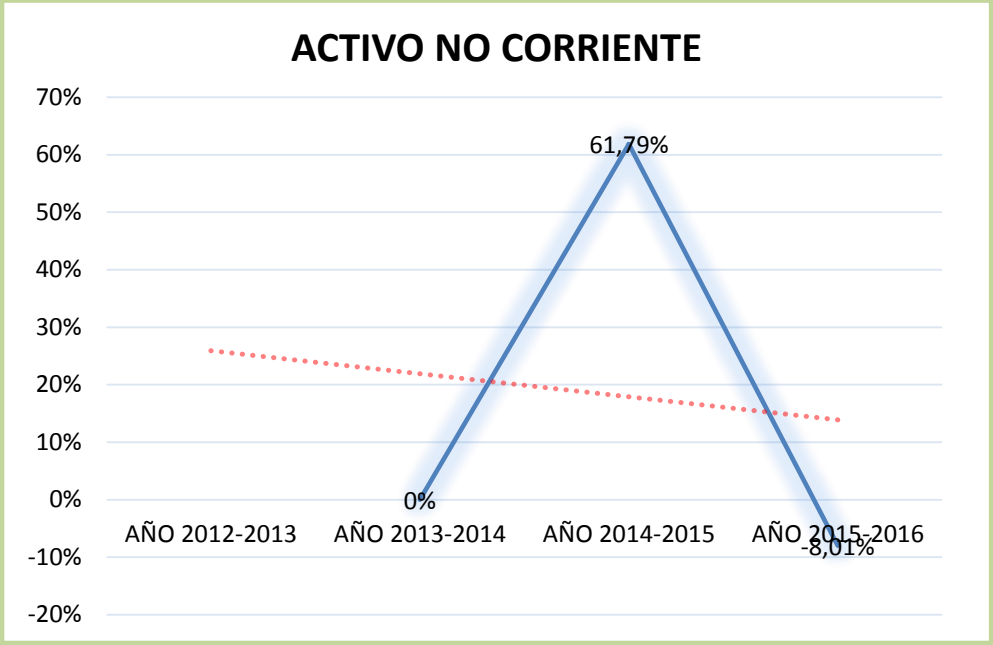

Figura 76 U. Valores Relativos Activo No C.

Tabla 104

U. Valores Relativos Pasivo

CUENTA	AÑO 2013-2014	AÑO 2014-2015	AÑO 2015-2016
PASIVO	100,00%	4,39%	-24,55%

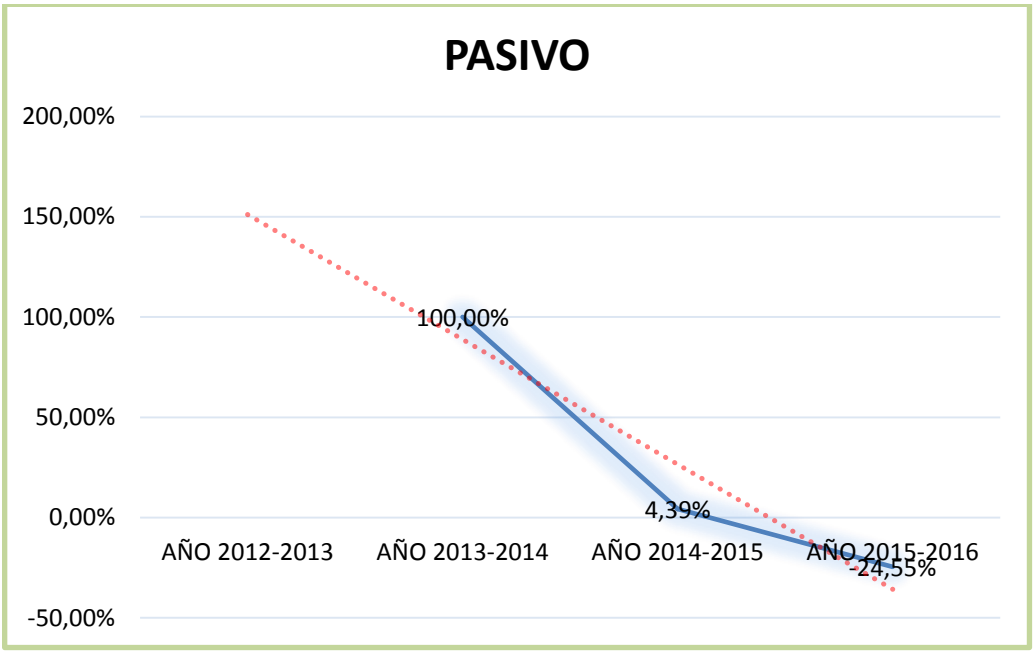

Figura 77 U. Valores Relativos Pasivo

Tabla 105

U. Valores Relativos Patrimonio

CUENTA	AÑO 2013-2014	AÑO 2014-2015	AÑO 2015-2016
PATRIMONIO	100,00%	-92,51%	439,87%

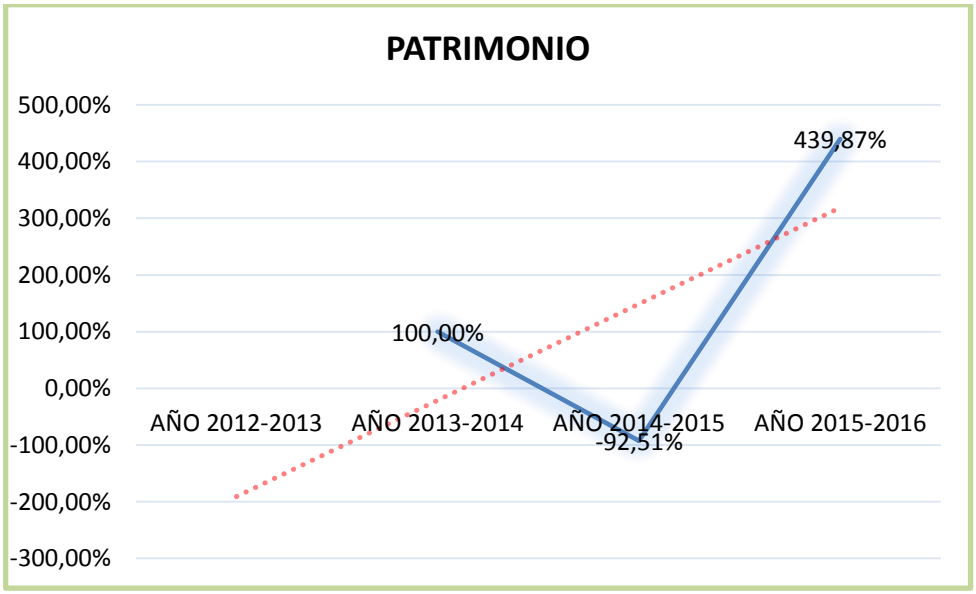

Figura 78 U. Valores Relativos Patrimonio

Interpretación

Con la información reflejada en los estados de situación financiera se presenta en la Cuenta del Activo para el año 2016 en relación al año 2015 una disminución del 8,40%, en la cuenta del Activo no Corriente, se presenta una disminución del 8,01%, en la cuenta del Equipo de Cómputo y software no hay variación en los años, en la cuenta del Pasivo se presenta una disminución del 24,55% y en la cuenta del Patrimonio de presenta un incremento del 439,87%.

Análisis y Diagnóstico

Para el año 2016 consta una disminución del activo de un 8,40%, así mismo existe en la cuenta del Pasivo una gran disminución del 24,55% entre los años 2015-2016, en compensación se demuestra un valor representativo de $249.316,68 en la cuenta del Patrimonio con un porcentaje del aumento del 439,87% en el año 2016, además el Gerente de la empresa menciona la difícil situación del país ya que incidió en una importante disminución de los ingresos; y en las proyecciones que se realiza para los próximos años 2017-2018 manifiestan leves variaciones de disminución en las cuentas mencionadas en el caso que las normas, leyes del país se mantengan; Dadas las actuales circunstancias el gerente menciona que es necesario ampliar la oferta de productos a equipos relacionados con las actuales líneas de producción.

Carnidem Cia. Ltda.

Ubicada en la Panamericana Norte Km 20 vía Latacunga-Quito, Dedicada a la producción de embutidos

Tabla 106

Ca. Valores Relativos Eq. de Computación

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
EQUIPO DE COMPUTACIÓN	12,33%	0,00%	0,00%	0,00%

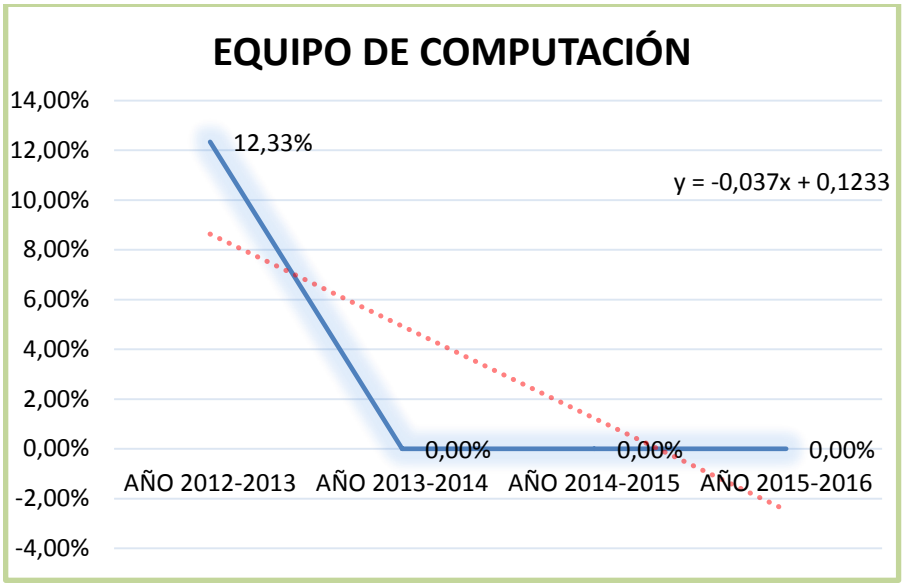

Figura 79 Ca. Valores Relativos Eq. de Computación

Tabla 107

Ca. Valores Relativos Activo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO	26,15%	-4,65%	-6,24%	0,35%

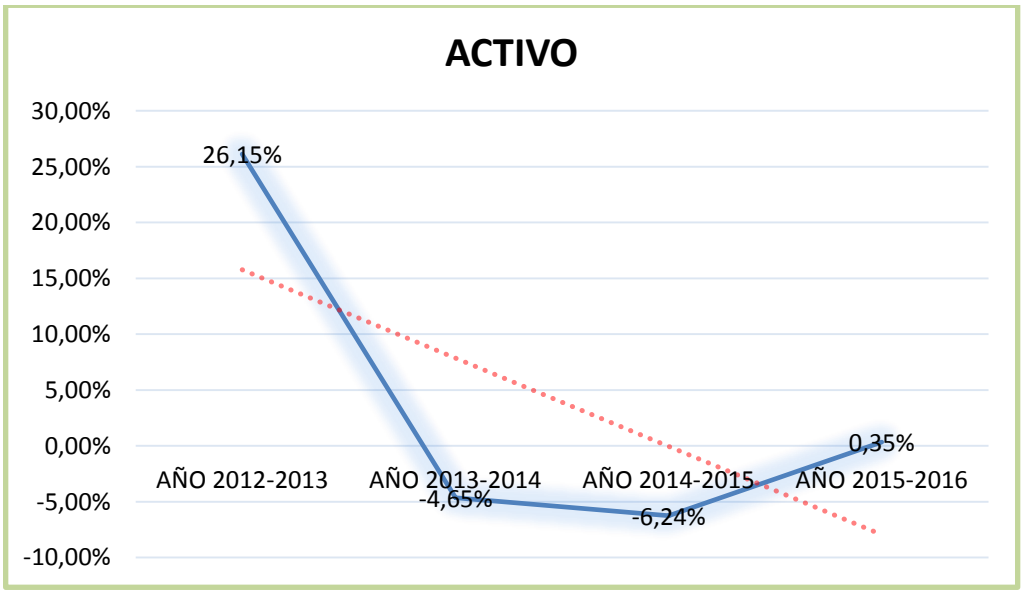

Figura 80. Ca. Valores Relativos Activo

Tabla 108

Ca. Valores Relativos Activo No C.

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO NO CORRIENTE	38,93%	-10,66%	-2,09%	-13,14%

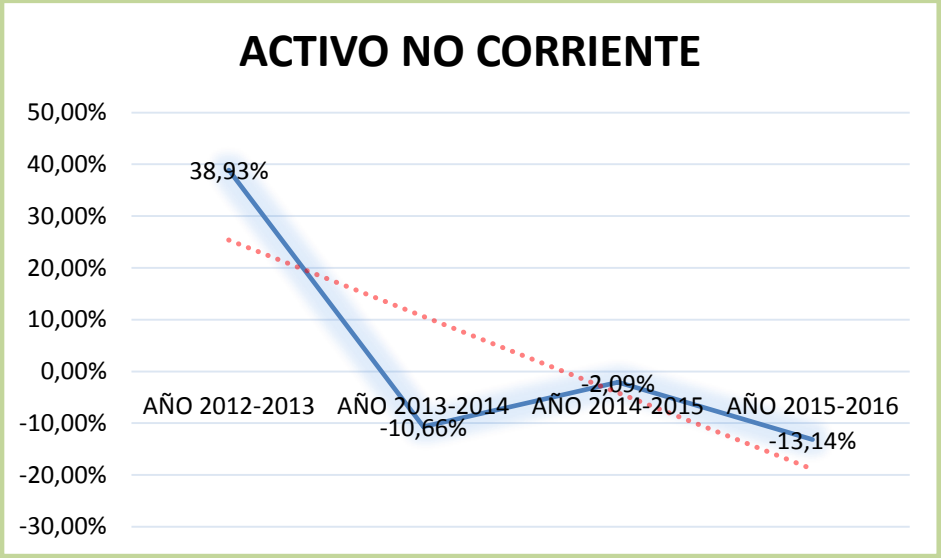

Figura 81 Ca. Valores Relativos Activo No C.

Tabla 109

Ca. Valores Relativos Pasivo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PASIVO	65,53%	-10,90%	-24,26%	-21,55%

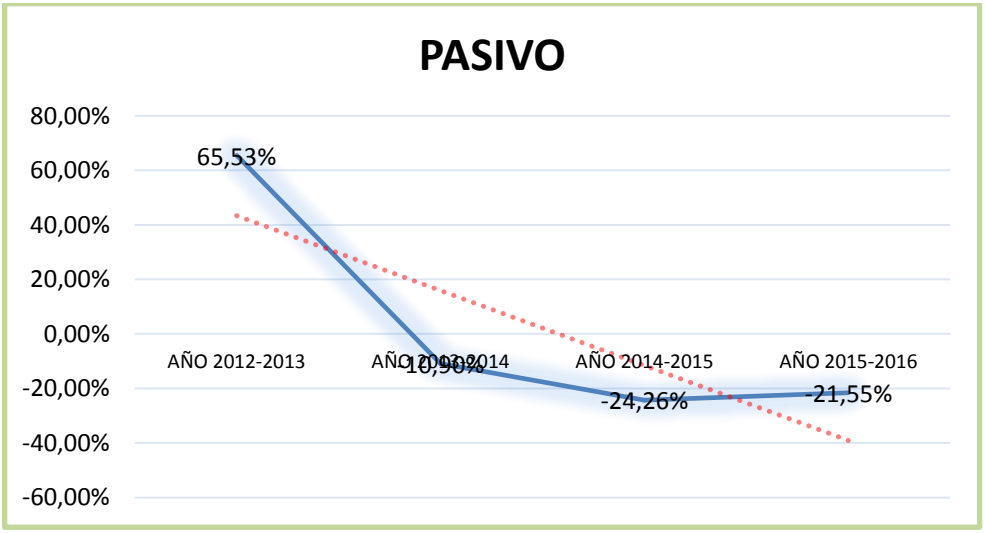

Figura 82. Ca. Valores Relativos Pasivo

Tabla 110

Ca. Valores Relativos Patrimonio

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PATRIMONIO	-6,34%	4,47%	16,17%	18,10%

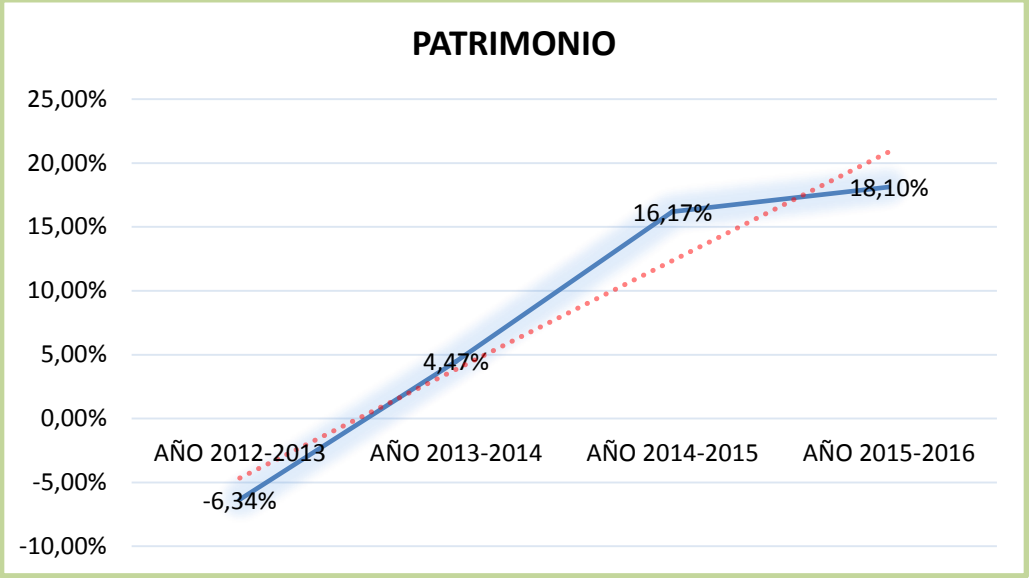

Figura 83. Ca. Valores Relativos Patrimonio

Pronósticos

Tabla 111

Pronósticos de las cuentas E- Ulloa

CUENTA	2016-2017	2017-2018	2018-2019	2019-2020
Activo	4,59%	1,10%	1,08%	1,07%
Activo no corriente	10,02%	-12,17%	-2,96%	-4,78%
Pasivo	12,86%	-34,96%	-24,95%	-23,11%
Patrimonio	0,14%	11,70%	9,01%	6,31%
Equipo de computación	4,39%	2,10%	2,06%	2,02%

Interpretación

Con la información reflejada en los estados de situación financiera de la empresa en las Cuentas: Activo para el año 2016 en relación al año 2015 se presentó un incremento de 0,35%, en la cuenta del Activo no Corriente se constató una disminución del 13,14%, en la cuenta del Equipo de Cómputo y software en el año 2015 y año 2016 con un valor similar del $16758,01 se visualizó que no tienen movimientos en la cuenta, en la cuenta del Pasivo se presenta una disminución del 21,55%, en la cuenta del Patrimonio de presenta un crecimiento del 18,10%.

Análisis y Diagnóstico

Se pudo identificar que en la empresa se mantuvo valores constantes en la cuenta Equipo de computación y Software en los últimos años desde 2013 al 2016 y para las proyecciones se estima que la empresa realice inversiones en tecnología mínimos, así mismo en el crecimiento empresarial como en económico la empresa se mantendrá estable.

Productora y Comercializadora de los Helados de Salcedo Corpicecream S.A.

La empresa se encarga de la producción y comercialización de los Helados de Salcedo.

Tabla 112

H. Valores Relativos Eq. de Computación

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
EQUIPO DE COMPUTACIÓN Y SOFTWARE	133,98%	0,00%	1,96%	-8,01%

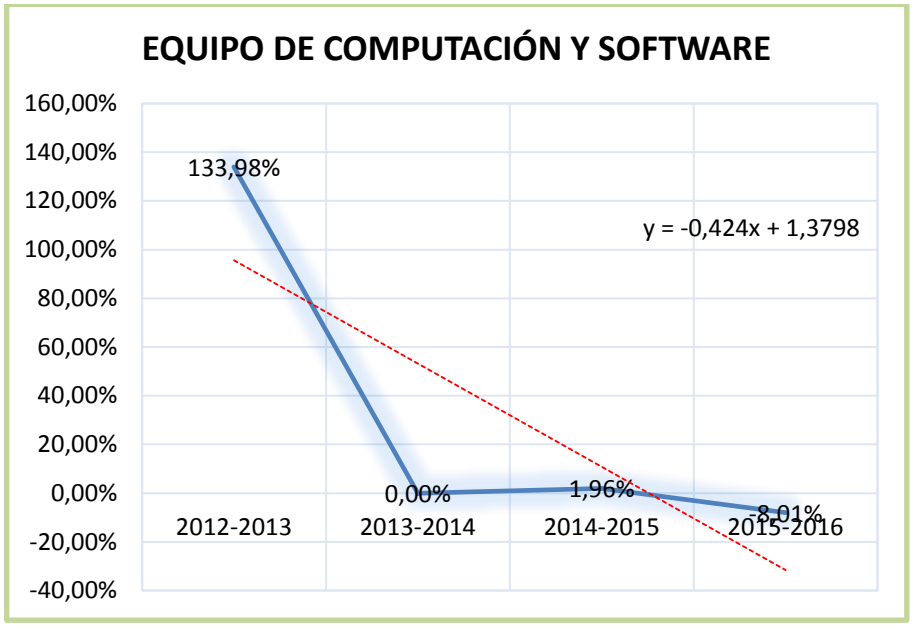

Figura 84. H. Valores Relativos Eq. de Computación

Tabla 113

H. Valores Relativos Activo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO	-14,58%	58,57%	21,53%	22,57%

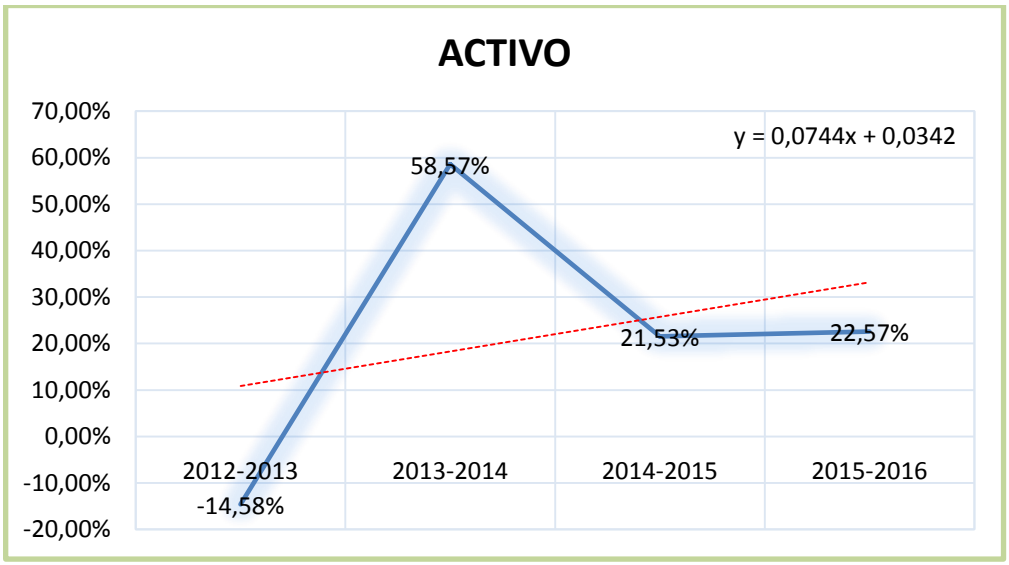

Figura 85 H. Valores Relativos Activo

Tabla 114

H. Valores Relativos Activo No C.

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO NO CORRIENTE	3,11%	78,41%	17,23%	5,66%

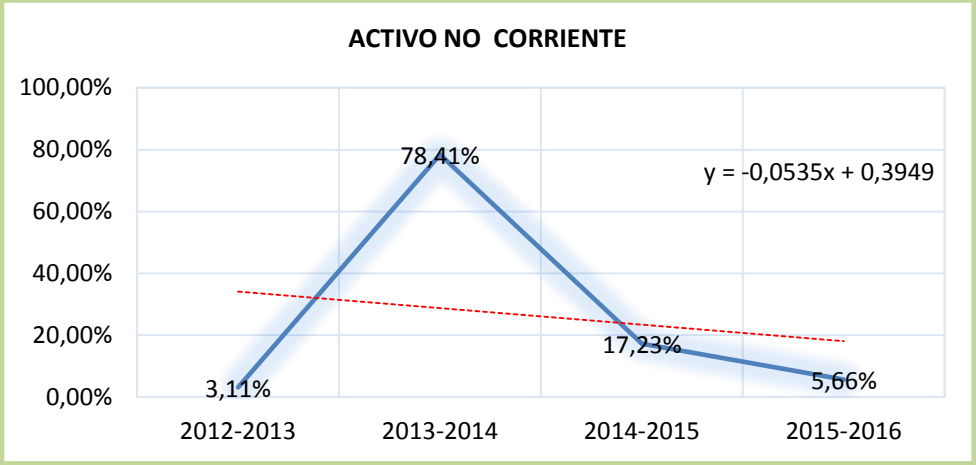

Figura 86 H. Valores Relativos Activo No C.

Tabla 115

H. Valores Relativos Pasivo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PASIVO	-30,96%	171,41%	25,36%	14,80%

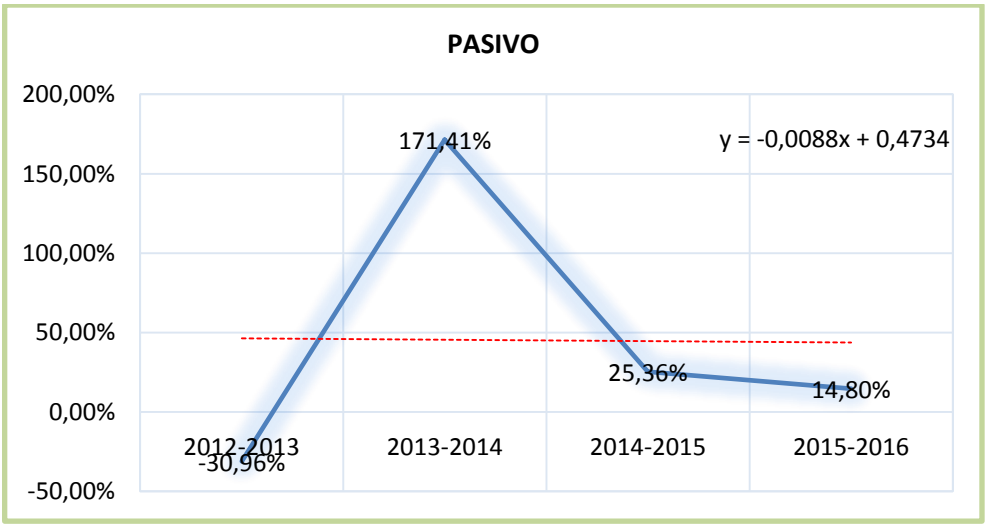

Figura 87 H. Valores Relativos Pasivo

Tabla 116

H. Valores Relativos Patrimonio

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PATRIMONIO	0,87%	-14,32%	13,68%	40,11%

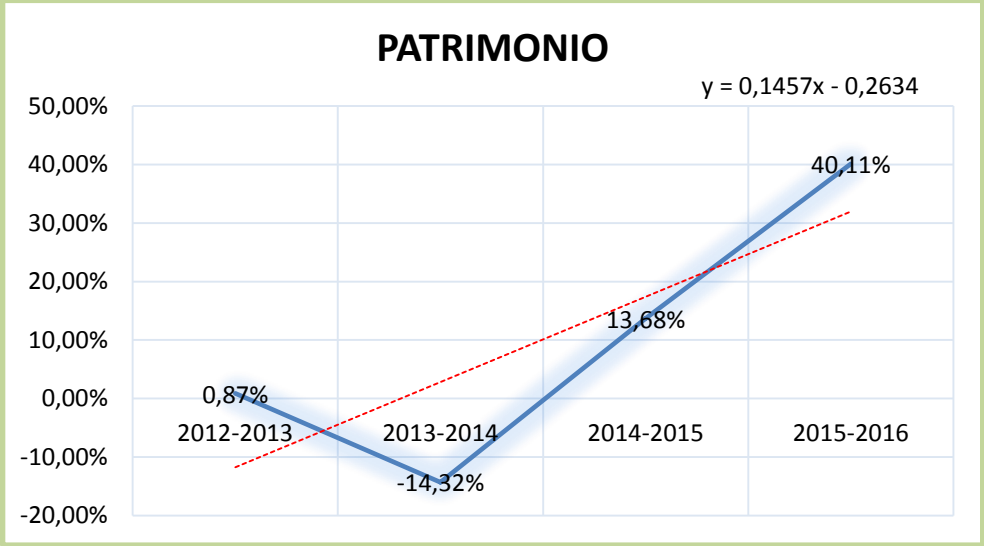

Figura 88 H. Valores Relativos Patrimonio

Interpretación

Entre las variaciones más representativas para el año 2016 versus el 2015 tenemos dentro del Activo la cuenta Inventarios con un incremento de 275,67% por la cantidad de $44.118 siendo el año con un mayor incremento después de los cuatro últimos años por lo que representa una tendencia creciente y se estima un incremento de 10,14%, Equipo de Computación y Software presenta una disminución en la cuenta de 8,01% por una cantidad de $1.108,13, generando una tendencia decreciente. El Pasivo para el año 2016 incrementó el 14,80% por la cantidad de $ 43.697,99 dentro del cual se puede destacar la cuenta Anticipo clientes con un incremento de 6049,87% por una cantidad de $29.165,83. La cuenta Patrimonio en el año 2016 versus 2015 presenta un incremento de 40,11% por una cantidad de $52.474,24 lo que refleja una tendencia creciente y se estima un incremento si las políticas se mantienen del 5,16% además dentro de este grupo la cuenta con un mayor incremento son las

ganancias netas del periodo por un valor de $48.715,8 representado por 1673,12%.

Las principales cuentas del Activo Corriente son Activos Financieros, y para el año 2016 representa el 13,46% del total de activos por una cantidad de $70.271,56, en el año 2015 representó el 6,51%. Equipo de Computación y Software alcanzaron un valor de $12.731,43 y representa el 2,44% del total de Activos, en el año 2015 representaron el 3,25%. Obligaciones con Instituciones Financieras presenta $ 83.291,69 representando el 24,57% del total de Pasivos, en el 2015 fueron de $ 95.631,17 lo que representa que la empresa está cumpliendo sus obligaciones. La cuenta Capital suscrito o asignado en el año 2016 presenta un valor de $ 131.940,00 representado por el 71,98% del total de Patrimonio.

Análisis y Diagnóstico

El incremento considerable en inventarios se debe a que también incrementó la producción gracias a la implementación de la nueva maquinaria que ayuda a la empresa a solventar los pedidos, anticipos de los clientes y generar ganancias para la empresa de forma significativa. Además podemos observar una disminución en la cuenta Equipo de Computación y Software lo cual representa que la empresa vendió esto activos fijos, también se puede observar que los valores reflejados en cuenta del pasivo se debe a la suma de las deudas que se mantiene con CFN, y demás instituciones públicas y privadas, los cuales se han ido cancelando al día.

Calzacuba Cia. Ltda.

Ubicada en las calles 2 de Mayo en la Ciudad de Latacunga Cantón Cotopaxi, dedicada a la fabricación, importación, exportación, distribución, representación y comercialización de calzado de todo tipo.

Tabla 117

Ca. Valores Relativos Eq. de Computación

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
EQUIPO DE COMPUTACIÓN	4,49%	0,00%	53,36%	3,57%

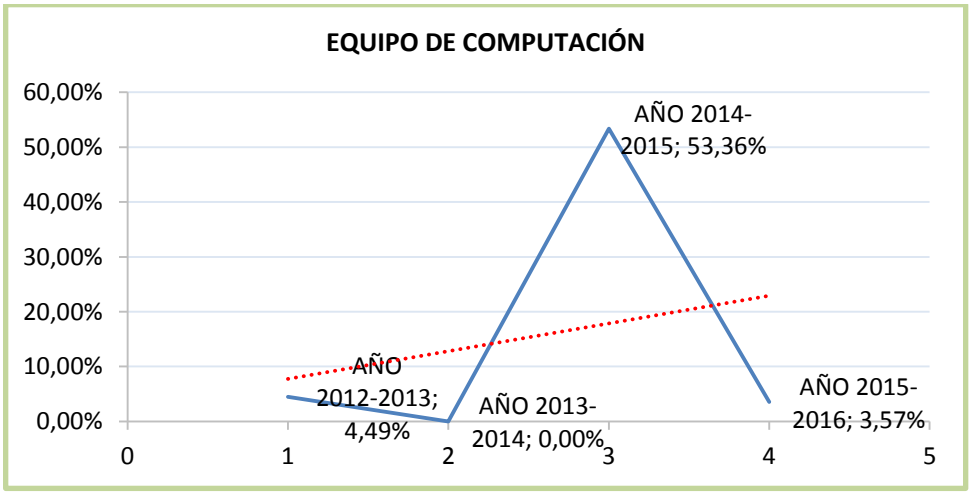

Figura 89 Ca. Valores Relativos Eq. de Computación

Tabla 118

Ca. Valores Relativos Activo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO	67,86%	80,15%	11,81%	-12,13%

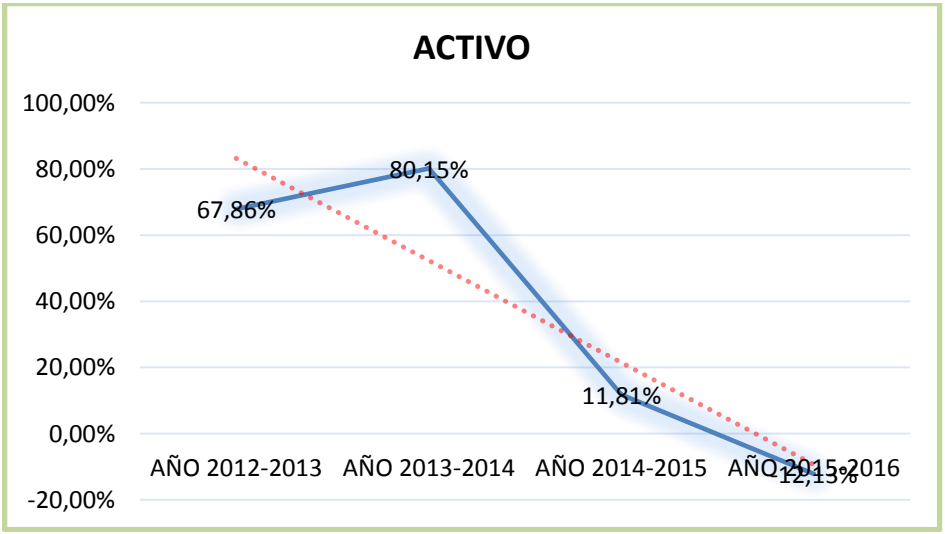

Figura 90 Ca. Valores Relativos Activo

Tabla 119

Ca. Valores Relativos Activo No C.

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO NO CORRIENTE	-7,18%	-11%	162%	695,30%

Figura 91 Ca. Valores Relativos Activo No C.

Tabla 120

Ca. Valores Relativos Pasivo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PASIVO	66,78%	70,89%	22,25%	-13,63%

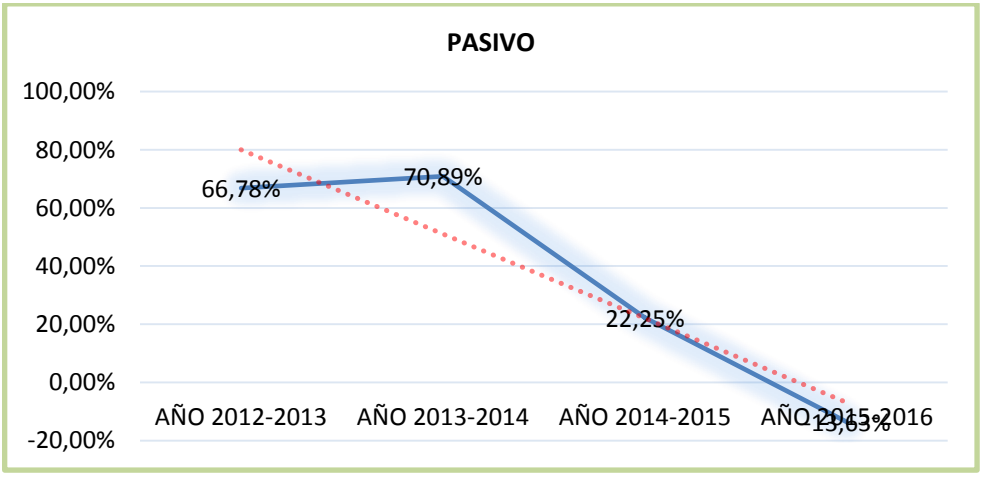

Figura 92 Ca. Valores Relativos Pasivo

Tabla 121

Ca. Valores Relativos Patrimonio

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PATRIMONIO	92,90%	264,82%	-85,68%	107,02%

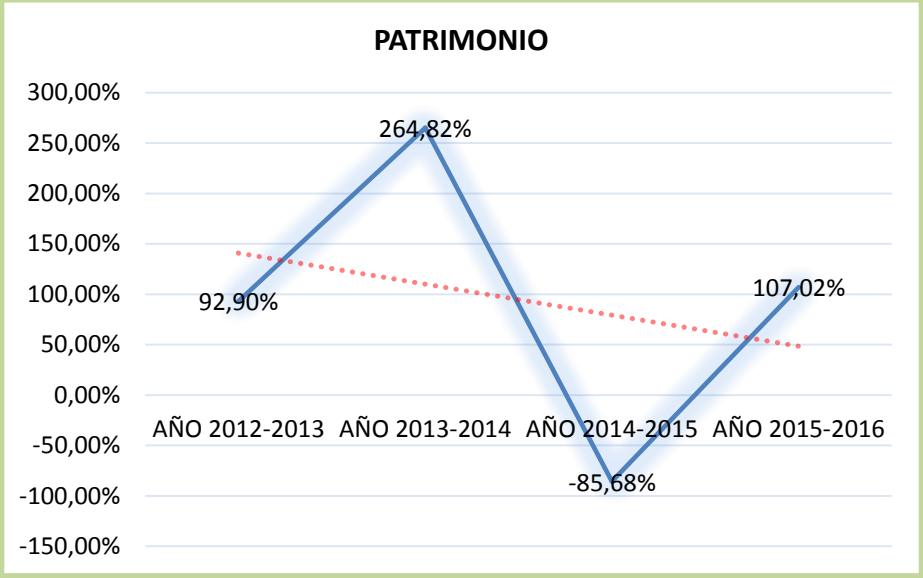

Figura 93 Ca. Valores Relativos Patrimonio

Pronósticos

Tabla 122

Pronósticos de las cuentas E. Carnidem

CUENTA	2016-2017	2017-2018	2018-2019	2019-2020
ACTIVO	38,15%	13,75%	12,09%	10,79%
ACTIVO NO CORRIENTE	8.021,10	8.842,17	9.663,24	10.484,31
PASIVO	38,00%	14,05%	12,32%	10,97%
PATRIMONIO	43,20%	4,19%	4,02%	3,87%
EQUIPO DE COMPUTACIÓN	10,47%	10,24%	9,29%	8,50%

Interpretación

Con la información reflejada en los estados de situación financiera de la empresa en las Cuenta: Activo para el año 2016 en relación al año 2015 se presentó una disminución de 12,13%, en la cuenta del Activo no Corriente se presentó un porcentaje significativo de crecimiento del 695,30%, en la cuenta del Equipo de Cómputo y software en el año 2015 con un valor de $7.010,74 en el año 2016 con un valor $7.260,74 se presentó un incremento del 3,57%, en la cuenta del Pasivo se constató un porcentaje bajo del 13,63%, en la cuenta del Patrimonio de presenta un porcentaje de crecimiento significativo para la empresa del 107,02%.

Análisis y Diagnóstico

La empresa presentó tendencias bajas en sus cuentas del activo, pasivo, patrimonio, en sus cuentas del Activo no Corriente y Equipo de computación y software presentó su tendencia creciente, la empresa menciona que su situación económica bajo debido a la economía del país, en lo sucedido del volcán Cotopaxi, los robos que fue víctima la empresa ha causado saldos negativos en sus estados financieros.

Editorial la Gaceta

La gaceta es una compañía dedicada a la impresión y distribución del diario

Tabla 123

G. Valores Relativos Eq. de Computación

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
EQUIPO DE COMPUTACIÓN Y SOFTWARE	40,85%	4,73%	0,00%	0,00%

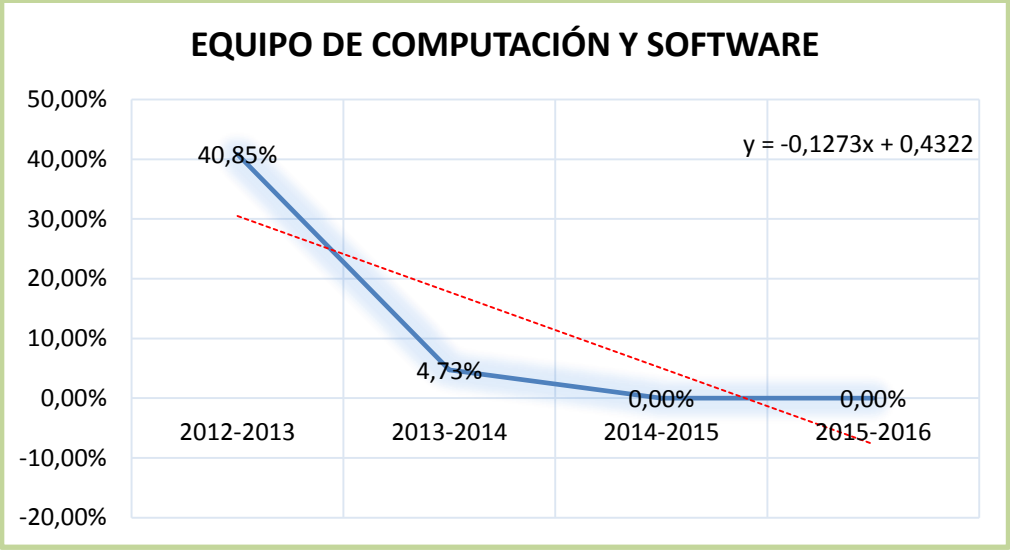

Figura 94 G. Valores Relativos Eq. de Computación

Tabla 124

G. Valores Relativos Activo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO	37,73%	24,94%	10,47%	4,27%

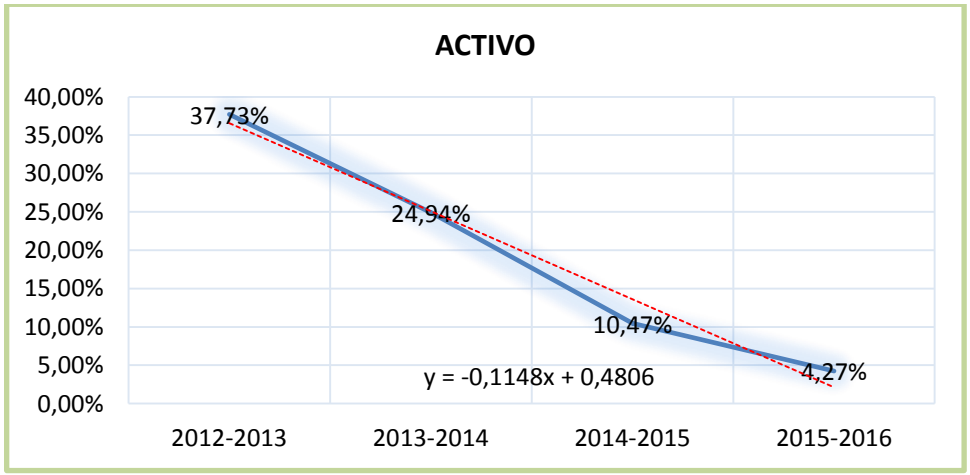

Figura 95 G. Valores Relativos Activo

Tabla 125

G. Valores Relativos Activo No Corriente

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO NO CORRIENTE	-16,03%	-19,41%	-25,09%	-17,25%

Figura 96 G. Valores Relativos Activo No Corriente

Tabla 126

G. Valores Relativos Pasivo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PASIVO	-28,01%	19,52%	0,05%	-0,21%

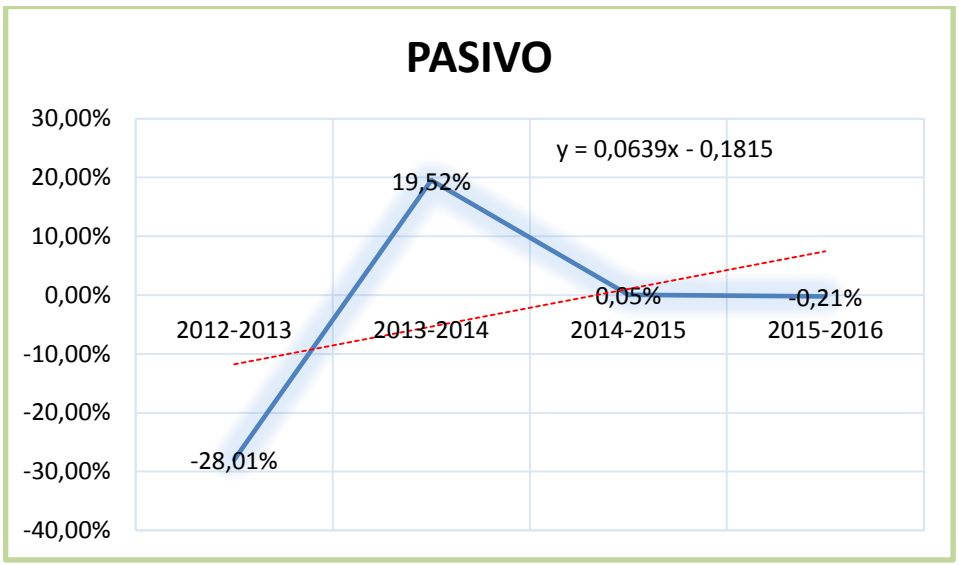

Figura 97 G. Valores Relativos Pasivo

Tabla 127

G. Valores Relativos Patrimonio

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PATRIMONIO	167,65%	27,82%	15,65%	6,19%

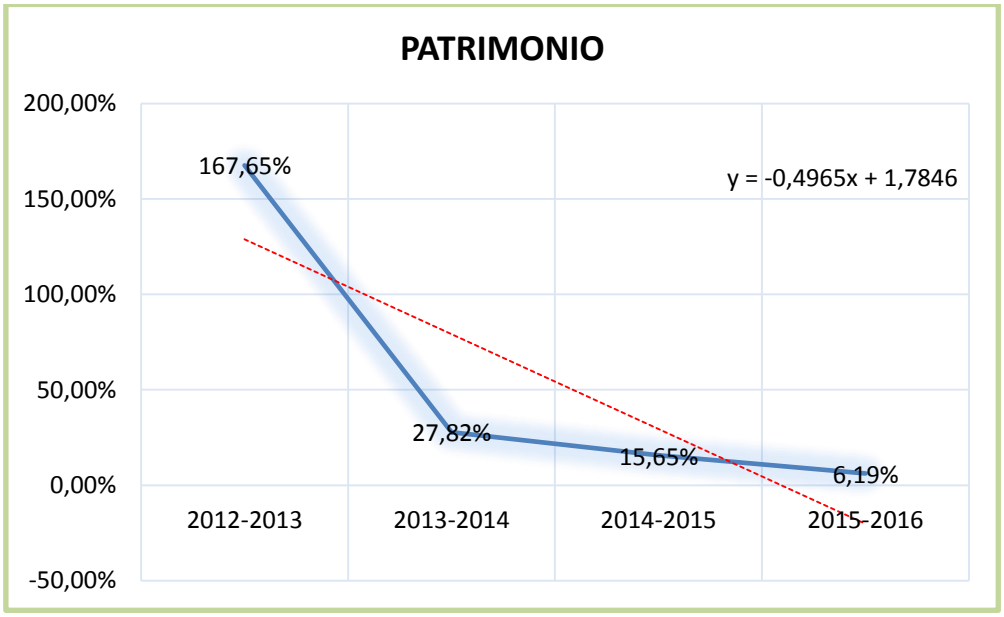

Figura 98 G. Valores Relativos Patrimonio

Pronóstico

Tabla 128

Pronóstico de las cuentas E. la Gaceta

CUENTA	2016-2017	2017-2018	2018-2019	2019-2020
Activo	18,19%	10,62%	9,60%	8,76%
Activo No Corriente	-42,67%	-62,10%	-163,86%	256,59%
Pasivo	-4,81%	-1,72%	-1,75%	-1,78%
Patrimonio	27,48%	14,34%	12,54%	11,15%
Equipo de Cómputo y Software	13,34%	6,08%	5,73%	5,42%

Interpretación

Se puede observar que para el año 2016 en referencia al año 2015 los activos de la compañía incrementaron en 4,27% por una cantidad de $12.613,82, en la cuenta Equipo de Computación y software no existió variación alguna la cuenta se mantuvo constante desde el año 2014, los pasivos de la empresa para el año 2016 disminuyeron en 0,21% por una cantidad de $184,27, el patrimonio por el contrario incrementó para el año 2017 el 6,19% por un valor de $12.798,09.

La cuenta efectivo y Equivalentes al efectivo representan el 15,66% del total de los activos, equipo de computación y software para el año 2016 apenas representa el 8,25% del total de activos, el capital de la compañía representa el 0,729% del total del patrimonio.

Análisis y Diagnóstico

La gestión administrativa y financiera ha permitido que en el año 2016 se logre un crecimiento sostenido de operaciones, además en los estados se puede visualizar que en los tres últimos años la cuenta de equipo de computación y software no ha variado y presenta una tendencia decreciente.

MOLINOS OROBLANCO CIA. LTDA.

Se encuentra domiciliada en la ciudad de Latacunga, con la denominación social de Molinos Ripalda y Ripalda Cia.Ltda al 13 de noviembre del 2008, Su actividad económica es la explotación, industrialización, molienda de trigo, otros cereales y sus derivados.

Tabla 129

M. Valores Relativos Eq. de Computación

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
EQUIPO DE COMPUTACIÓN Y SOFTWARE	0,00%	0,00%	0,00%	0,00%

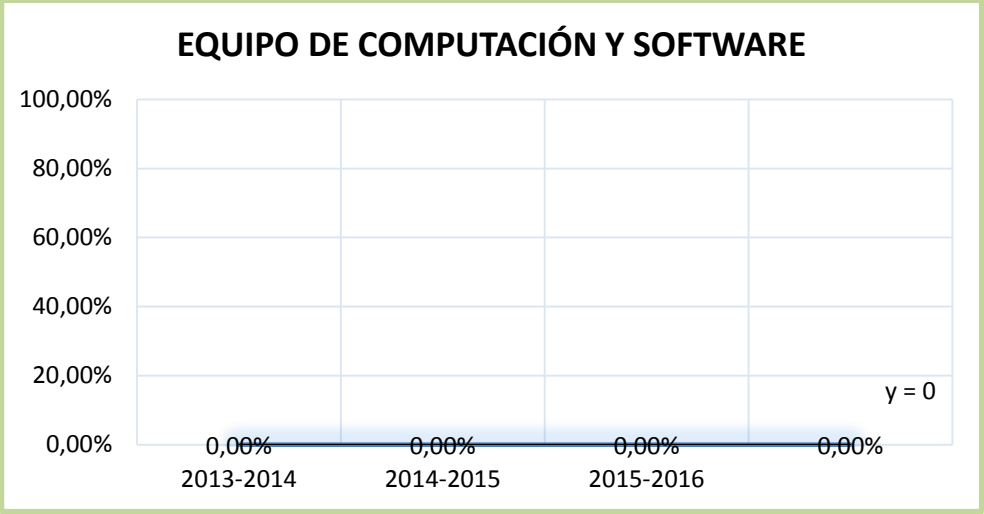

Figura 99 M. Valores Relativos Eq. de Computación

Tabla 130

M. Valores Relativos Activo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO	-6,02%	-2,46%	1,17%	-4,49%

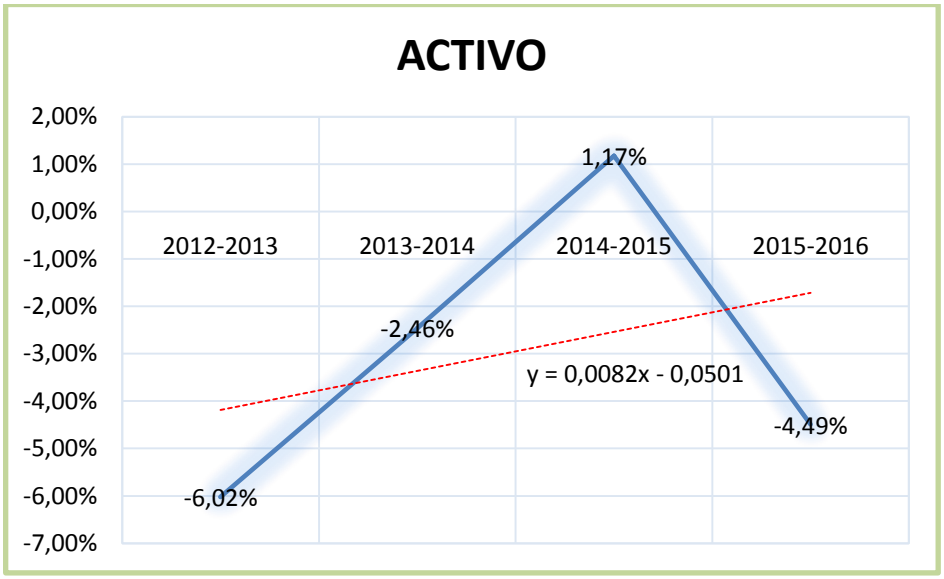

Figura 100 M. Valores Relativos Activo

Tabla 131

M. Valores Relativos Activo No Corriente

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
ACTIVO NO CORRIENTE	-14,31%	-16,21%	-1,55%	2,13%

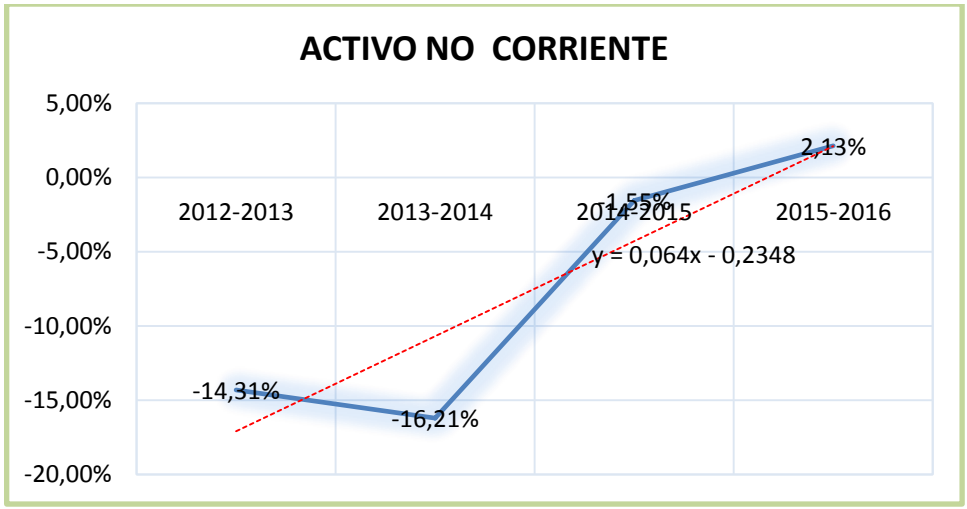

Figura 101 M. Valores Relativos Activo No Corriente

Tabla 132

M. Valores Relativos Pasivo

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PASIVO	-17,26%	-14,83%	-7,80%	18,79%

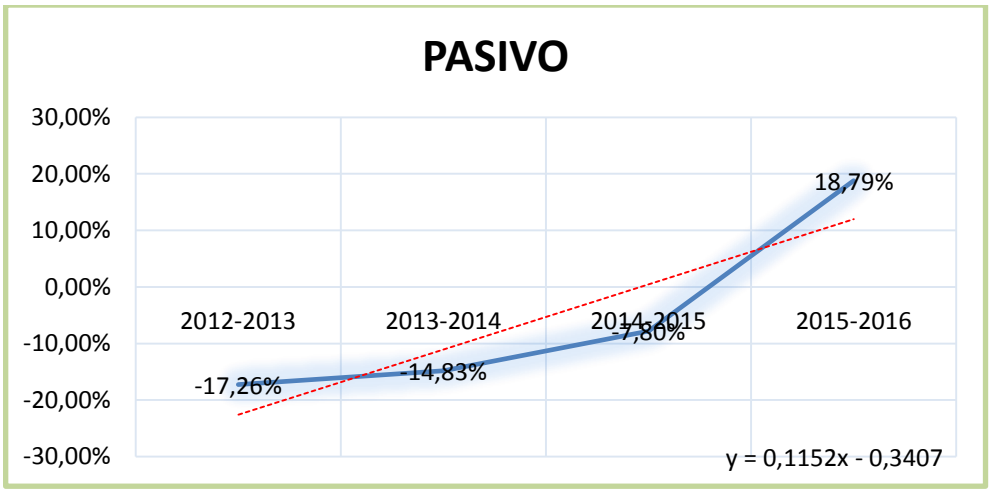

Figura 102 M. Valores Relativos Pasivo

Tabla 133

M. Valores Relativos Patrimonio

CUENTA	2012-2013	2013-2014	2014-2015	2015-2016
PATRIMONIO	0,47%	3,42%	4,69%	-12,52%

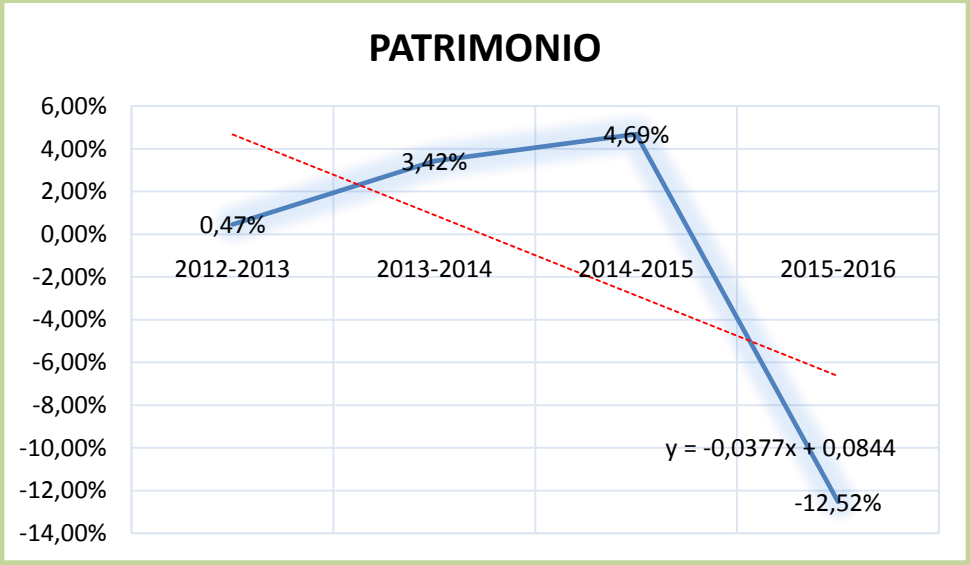

Figura 103 M. Valores Relativos Patrimonio

Interpretación

La Compañía en el año 2016 versus 2015 presenta en la cuenta Activo una disminución del 4,49% por una cantidad de $ 11.190,49 y presenta una tendencia creciente. En el Activo No Corriente se observa un incremento de 2,13% por una cantidad de $1.528,12 y a cuatro años se estima una disminución en la cuenta por el 15,77% si las políticas tanto internas como externas se mantienen. En Equipo de Computación y Software la cuenta en el transcurso de los años presenta valores constantes por $ 1.187,36 lo cual refleja que no presenta tendencia alguna. En la cuenta Pasivo por el contrario se observa un aumento del 18,79% por una cantidad de $ 11.999,89 con una tendencia creciente y se estima a cuatro años una disminución del 13,38% siempre y cuando normativas de la compañía se mantengan y la cuenta Patrimonio presenta una disminución de 12,52% por una cantidad de $23.190,38.

En el año 2016 la cuenta principal dentro de Propiedad Planta y Equipo es Maquinaria y Equipo con el 60,47% del total del Activo por un valor de $ 168.588,686, dentro del Activo Corriente tenemos Efectivo y Equivalentes al Efectivo con el 20.95% del total del activo por un valor de $58.420,31. Las cuentas y documentos por pagar alcanzaron un valor de $8.613,72 que representa el 11,35% del total de Pasivo. La cuenta resultados del ejercicio es Ganancias Netas por un valor de $76.217,85 que representa el 37,56% del total del Patrimonio.

Análisis y Diagnóstico

Dentro de activos en la cuenta Efectivo y Equivalentes al Efectivo al 2016 referente al año 2015 se incrementó el 50,25% valores que permitirán manejar movimientos económicos en el año, además la cuenta activo presenta una tendencia creciente, se puede observar que la empresa no invierte en equipo de cómputo y software debido a que el valor se mantiene constante en todos los años. La cuenta pasivo presenta una tendencia creciente a diferencia del patrimonio que al año 2016 decrece y se estima a cuatro años una disminución de 0,14% si los factores externos políticos, normativos y técnicos se mantienen.

Andes Kinkuna S.A.

Ubicada en la parroquia de Pujilí, barrio Rumipamba, Vía al barrio San Juan, Pujilí Cotopaxi, dedicada a la elaboración de productos alimenticios.

Tabla 134

Pronóstico de las cuentas E. Kinkuna

CUENTA	AÑO 2015-2016
EQUIPO DE COMPUTACIÓN	100,00%
MARCAS, PATENTES, DERECHOS DE LLAVE, CUOTAS PATRIMONIALES Y OTROS SIMILARES	30,15%
ACTIVO NO CORRIENTE	1013,81%
PASIVO	392,56%
PATRIMONIO	-56,51%

Interpretación

Con la información reflejada en los estados de situación financiera se presenta en la Cuenta del Activo para el año 2016 en relación al año 2015 se presenta un incremento de 249,62%, en la cuenta del Activo no Corriente se presenta un incremento del 1013,81%, en la cuenta de Activo Intangible presenta un incremento del 30,15%, en la cuenta del Pasivo se presenta un incremento del 392,56%, en la cuenta del Patrimonio de presenta una disminución del 56,51%.

Análisis y Diagnóstico

En los últimos meses la Industria obtuvo negociaciones el mismo que ayuda y obliga a incrementar la capacidad de producción según el informe del Gerente, al igual se presenta en las cuentas de activos, activo intangible, pasivo, incrementos ya que se registra sus actividades en la Superintendencia de Compañías y en su cuenta del Patrimonio presenta una disminución cuyo montos corresponde a los gastos administrativos, comerciales, legales y financieros.

4.2. Análisis de los resultados

Se realizó el trabajo de campo en las empresas del Sector Industrial reguladas por la Superintendencia de Compañías en los departamentos: administrativo, tecnología de la información, producción y Comercialización, Financiero y además a un empleado de las organizaciones y se logró obtener los siguientes resultados:

Departamento Administrativo

1. **¿Cuáles son las prácticas de Gestión de Sistemas de información que la empresa ha implementado durante el año 2012-2016?**

Tabla 135

Prácticas de Gestión de Sistemas de Información

Gestión de Sistemas	Incluye		No Incluye		Total
	Frecuencia	Porcentaje de Respuesta SI	Frecuencia	Porcentaje de Respuesta NO	
Políticas de seguridad	17	77,3%	5	22,7%	100%
Auditoría Interna, Externa	13	59,1%	9	40,9%	100%
Clasificación de la Información	11	50,0%	11	50,0%	100%
Plan de continuidad del negocio	4	18,2%	18	81,8%	100%
Plan de respuesta a incidentes	6	27,3%	16	72,7%	100%
Acuerdos y/o contratos (El Acuerdo de Confidencialidad, Acuerdo de Nivel de Servicios)	7	31,8%	15	68,2%	100%
Estándar, normativa o marco de trabajo (ISO)	3	13,6%	19	86,4%	100%
Ninguna	2	9,1%	20	90,9%	100%

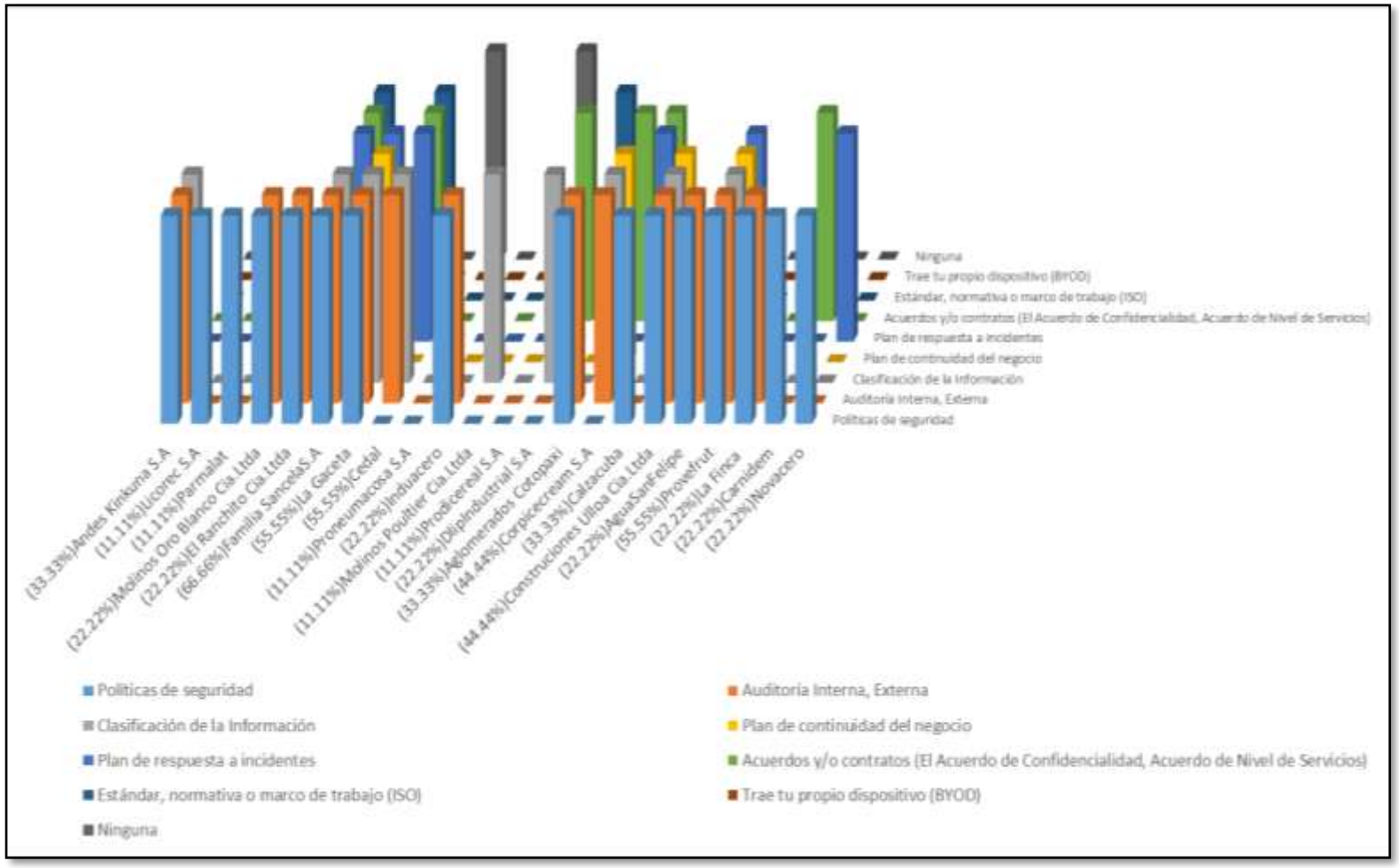

Figura 104. Prácticas de Gestión de Sistemas de Información

Interpretación

Dentro de las prácticas de Gestión de Información las que más se cumplen son las Políticas de Seguridad en las empresas del Sector Industrial representando un porcentaje del 77,3% mientras que el 22,7% no aplican esta política, las prácticas la que menos cumplen las empresas son los Estándares, normativas o marco de Trabajo (ISO) que representa un 13,6%.

2. ¿Cuánto aproximadamente ha invertido la empresa en el período 2012-2016 en herramientas de seguridad y protección de datos?

Tabla 136

Inversión en herramientas de Seguridad y Protección de datos

Inversión	Frecuencia	Porcentaje	Porcentaje acumulado
Ninguno	1	4,5	4,5
$1-$5000	6	27,3	31,8
$5001-$10000	4	18,2	50,0
$10001-$20000	6	27,3	77,3
$20001-$40000	2	9,1	86,4
Mayor a $40001	3	13,6	100,0
Total	22	100,0	

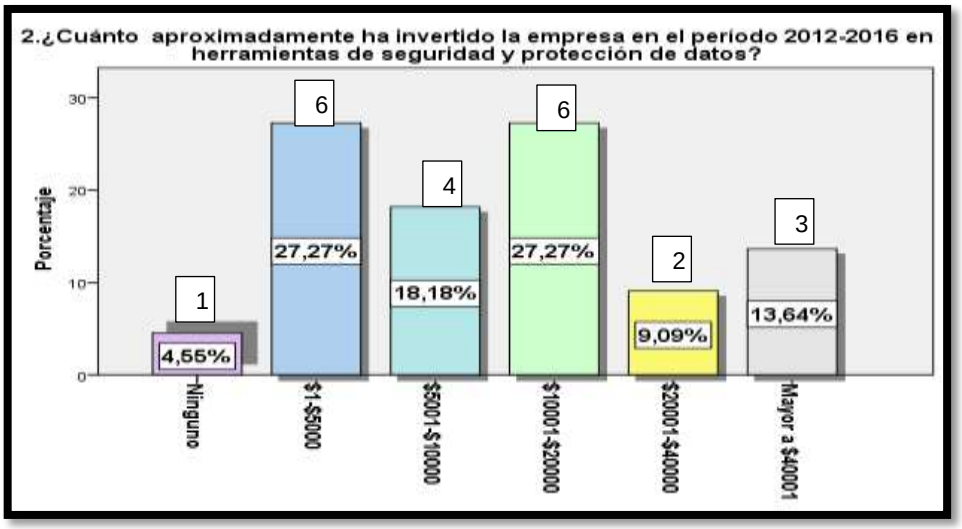

Figura 105. Herramientas de seguridad y protección de datos

Interpretación

Podemos observar que las Industrias tienen mayor inversión entre los valores $1 a $5000 y $10001 a $20000 que representa un porcentaje a cada uno del 27,30% en herramientas de seguridad y protección de datos, a más de ellos se visualiza que el 4.55% no han realizado inversiones del mismo, el 18.18% constatan una inversión entre los valores $5.001 a $1.000, el 9.09% confirman una inversión entre los valores $2.001 a $4.000, y el otro 13.64% dicen haber invertido más de $4.001 en el período 2012-2016.

3. **¿Existe alguna unidad o departamento que se encargue de la seguridad de la Información en la empresa?**

Tabla 137

Área que se encarga de la Seguridad de la Información

Departamento	Incluye		No Incluye		Total
	Frecuencia	Porcentaje de Respuesta SI	Frecuencia	Porcentaje de Respuesta NO	
INTERNA	12	54,50%	10	45,45%	100%
EXTERNA	14	68,20%	8	36,36%	100%

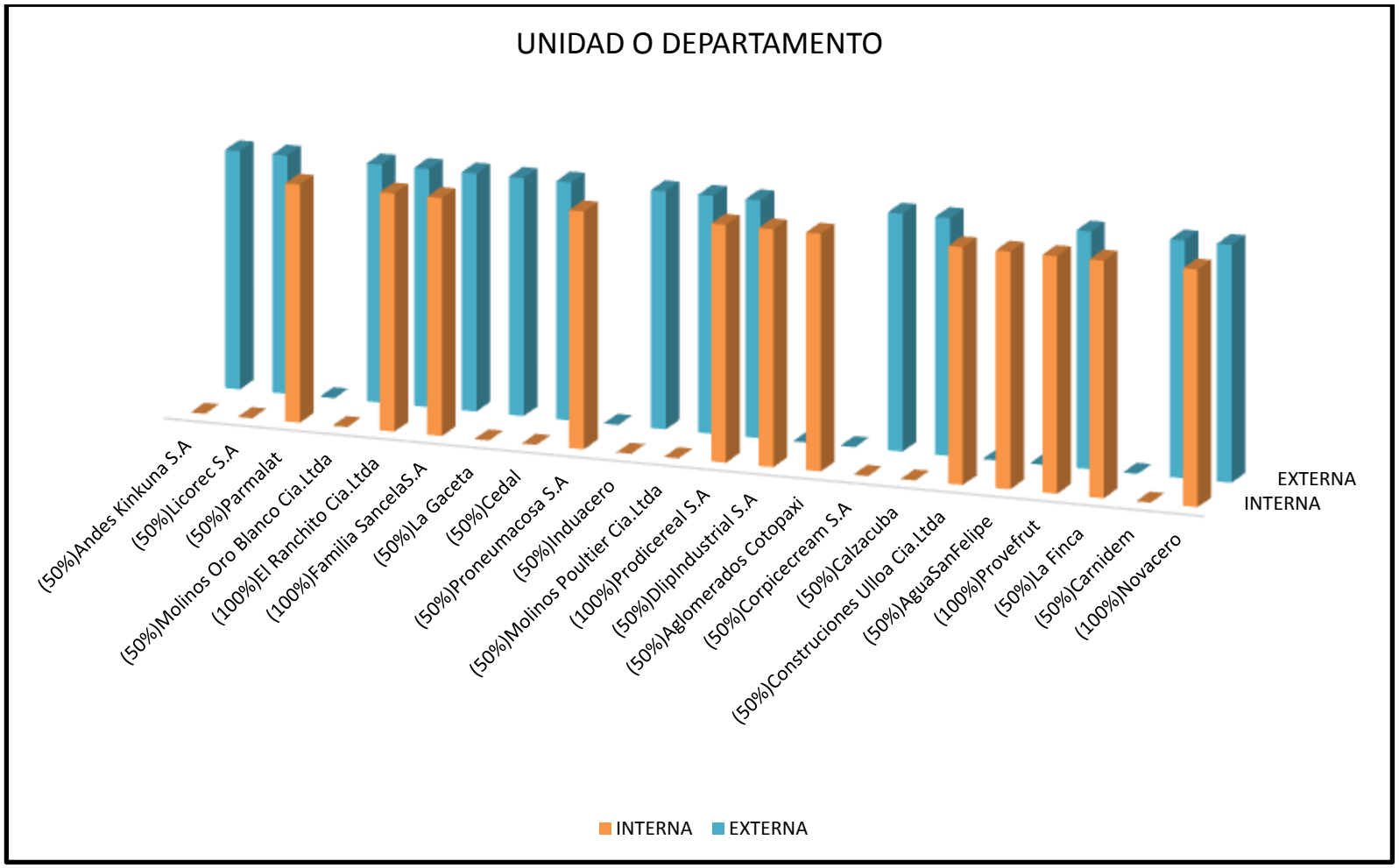

Figura 106. Área que se encarga de la Seguridad de la Información

Interpretación

Las empresas mencionan que el 54.50% tienen una unidad interna de Seguridad de la Información, así mismo constatan que también del 68.20% tienen una unidad Externa, y varias empresas mencionaron que cuentan con los dos departamentos.

4. **Las personas aceptan y firman los términos y condiciones del contrato de empleo y/o confidencialidad antes o después de iniciar sus labores.**

Tabla 138

Contratos y Acuerdos

Términos y Condiciones	INCLUYE		NO INCLUYE		Total
	Frecuencia	Porcentaje de Respuesta SI	Frecuencia	Porcentaje de Respuesta NO	
Contratos Antes	17	77,30%	5	22,7%	100%
Contratos Después	3	13,60%	19	86,4%	100%
Acuerdos Antes	13	59,10%	9	40,9%	100%
Acuerdos Después	3	13,60%	19	86,4%	100%
No Aplica Contrato	2	9,10%	20	90,9%	100%
No Aplica Acuerdo	6	27,30%	16	72,7%	100%

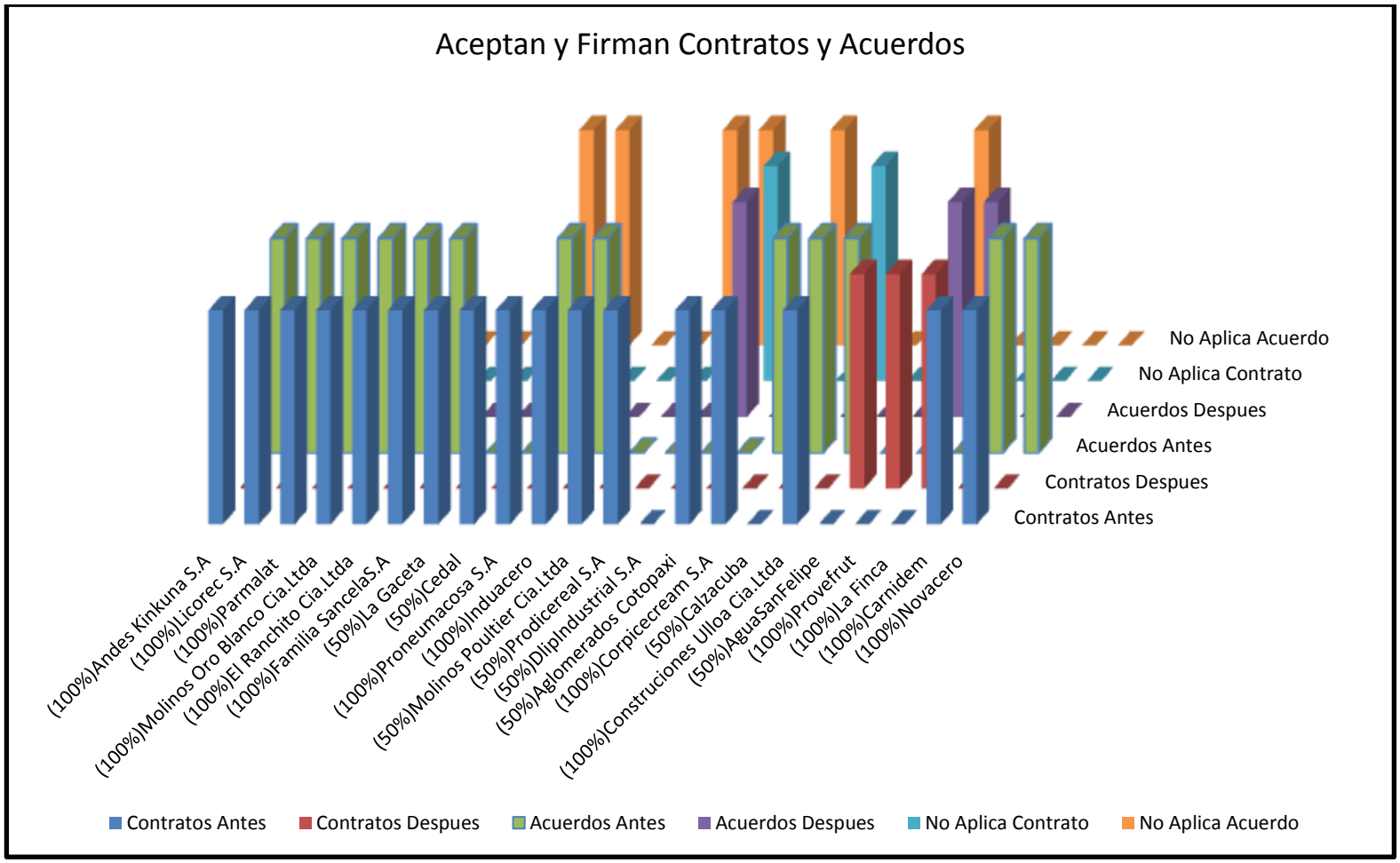

Figura 107. Contratos y Acuerdos

Interpretación

Las empresas mantienen un 77.30% de contratos con los empleados antes de ingresar a la misma y el 13.60% después de ingresar a laborar, el 59.10% las empresas realizan acuerdos de confidencialidad antes del ingreso del personal y 13.60% después, el 9.10% no aplican los contratos para el ingreso y 27.30% no tienen los acuerdos de confidencialidad.

5. **Se realiza un seguimiento del uso del e-mail a las personas antes de salir definitivamente de la empresa.**

Tabla 139

Seguimiento del uso de e-mail

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	10	45,5	45,5
NO	12	54,5	100,0
Total	22	100,0	

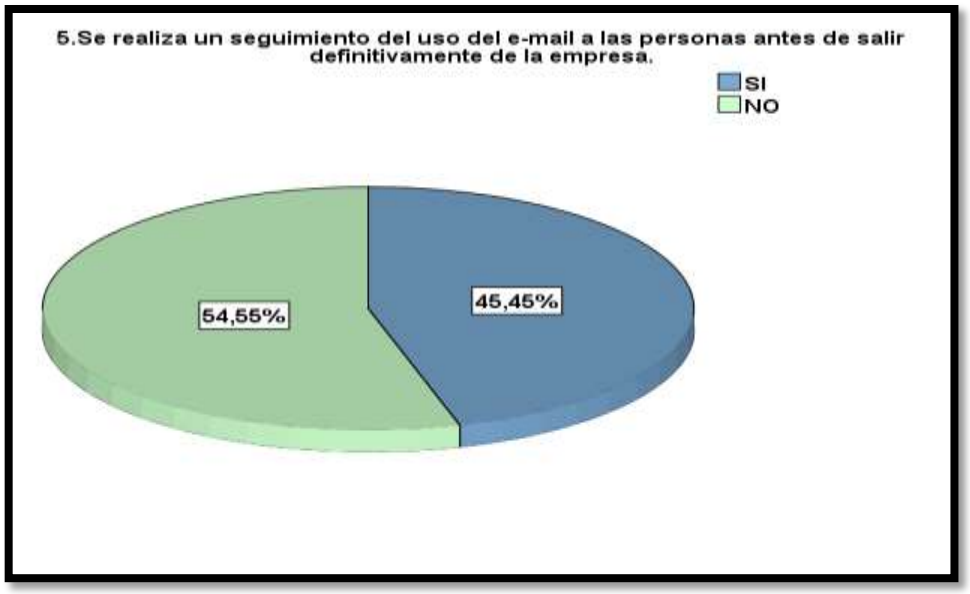

Figura 108. Seguimiento del uso de e-mail

Interpretación

Del total de las empresas encuestadas el 45.45% dicen haber realizado seguimientos de e-mail al personal después de que el empleado abandonara la entidad, además la mayoría de empresas dicen que el 54.55% no han realizado el seguimiento respectivo.

6. **¿Al culminar el contrato de trabajo los empleados dejan de tener acceso a la información?**

Tabla 140

Los empleados dejan de tener acceso

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	21	95,5	95,5
NO	1	4,5	100,0
Total	22	100,0	

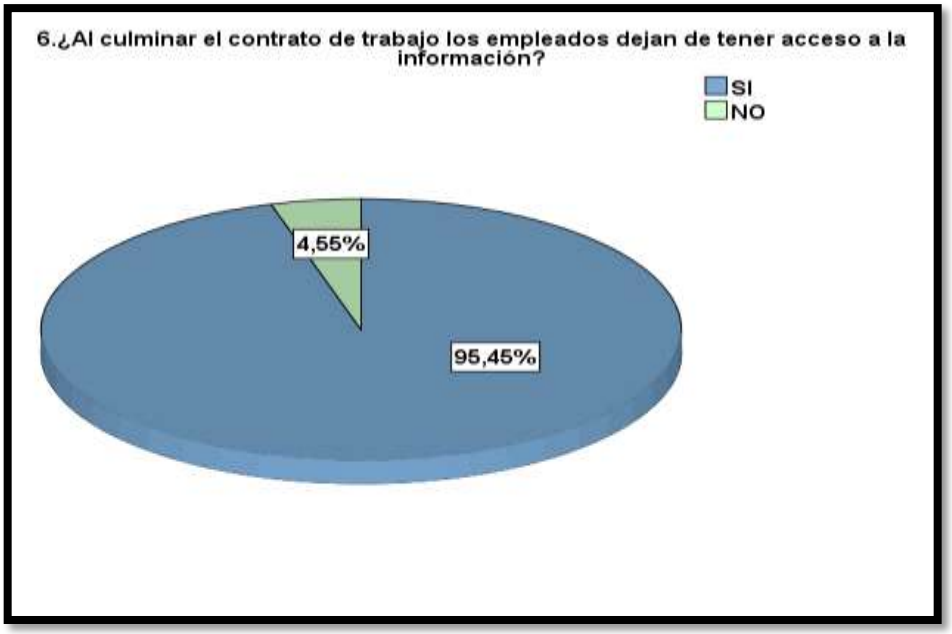

Figura 109. Los empleados dejan de tener acceso

Interpretación

El área Administrativa menciona que el 95.45% del personal dejan de tener accesos a la información de empresa después de haber culminado su contrato laboral y el 4.55% dicen que no dejan de tener el acceso a la información no se realiza un seguimiento respectivo a este control.

7. **¿Los empleados de la organización reciben entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas de seguridad de información y procedimientos para seguridad de la información?**

Tabla 141

Entrenamiento y conocimiento de Políticas

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	13	59,1	59,1
NO	9	40,9	100,0
Total	22	100,0	

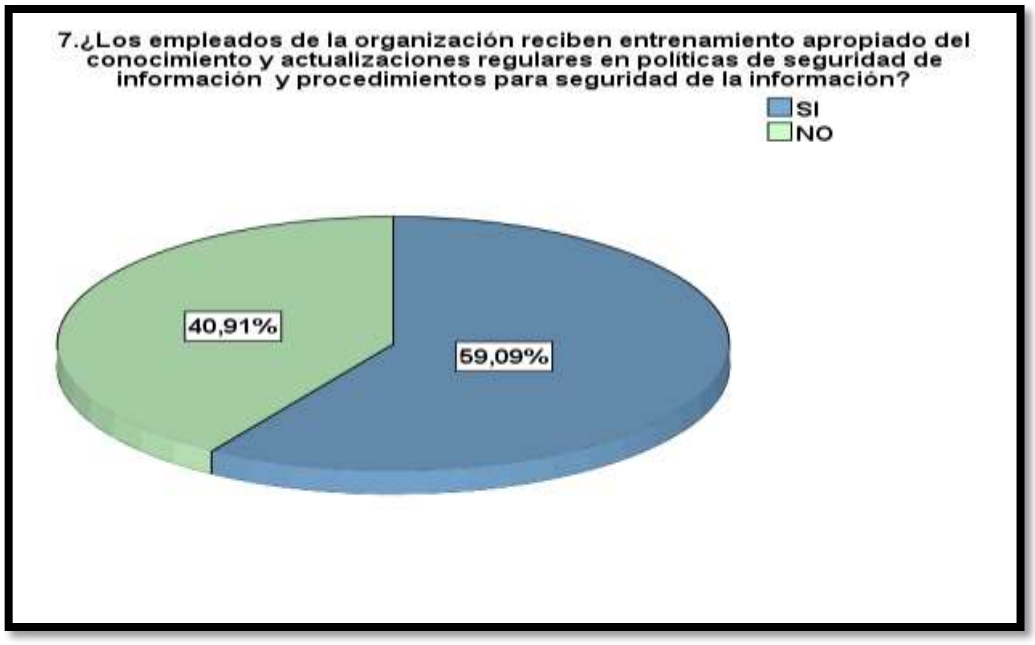

Figura 110. Entrenamiento y conocimiento de Políticas

Interpretación

El 59.09% del Área Administrativa constata que mantiene entrenamiento, conocimiento y actualización de las Políticas de Seguridad de Información con los empleados, mientras tanto el 40.91% dicen que no realiza y es un nivel significante para la investigación.

8. ¿Se resguarda el acceso al cuarto de archivos?

Tabla 142

Acceso al cuarto de archivo

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	17	77,3	77,3
NO	5	22,7	100,0
Total	22	100,0	

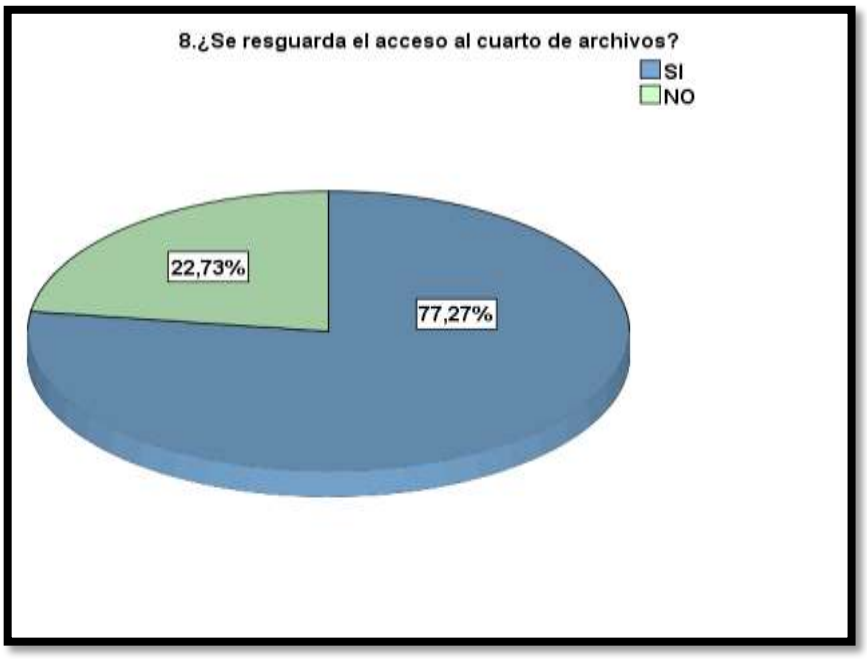

Figura 111. Acceso al cuarto de archivo

Interpretación

El área administrativa de las empresas del sector industrial afirman que el 77.27% si resguardan el acceso a cuartos de archivos y el 22.73% dicen que no realizan dicho resguardo.

9. ¿La empresa ha sufrido pérdidas de Equipos Informáticos?

Tabla 143

Pérdidas de Equipos Informáticos

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
NO	22	100,0	100,0

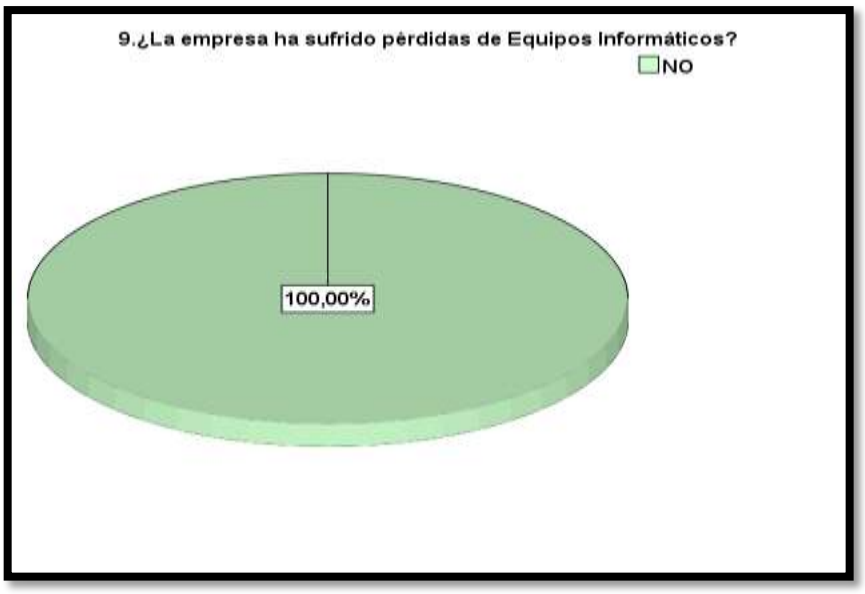

Figura 112. Pérdidas de Equipos Informáticos

Interpretación

El 100% de las Empresas señalan que no han sufrido de pérdidas de equipos informáticos la cual es bueno para las organizaciones tener un cuidado del mismo y control de los equipos.

Departamento de Tecnología de la Información

10. ¿Se lleva un control de la manipulación de información y el responsable del mismo (logs)?

Tabla 144

Manipulación de información y el responsable

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	18	81,8	81,8
NO	4	18,2	100,0
Total	22	100,0	

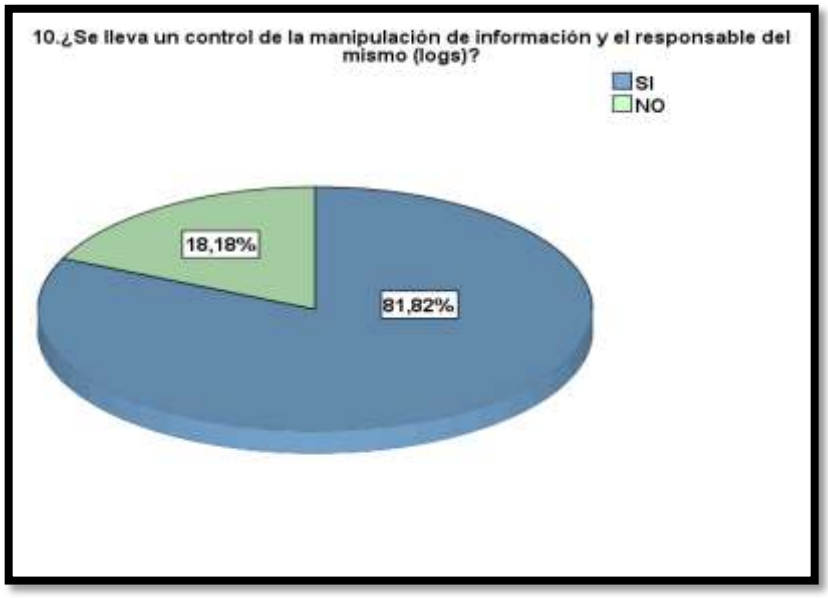

Figura 113. Manipulación de información y el responsable

Interpretación

Mediante la encuesta realizada podemos observar que el 81.82% si llevan un control de manipulación y responsable de la información la cual es bueno dentro de las organizaciones y el 18.18% el área afirma que no lleva un control y las

mismas tendrán que realizar un seguimiento respectivo a este control ya que no es tan común que comentan la falta de control del mismo.

11. ¿La empresa está certificada por la Norma ISO 27001?

Tabla 145

Norma ISO 27001

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	3	13,6	13,6
NO	19	86,4	100,0
Total	22	100,0	

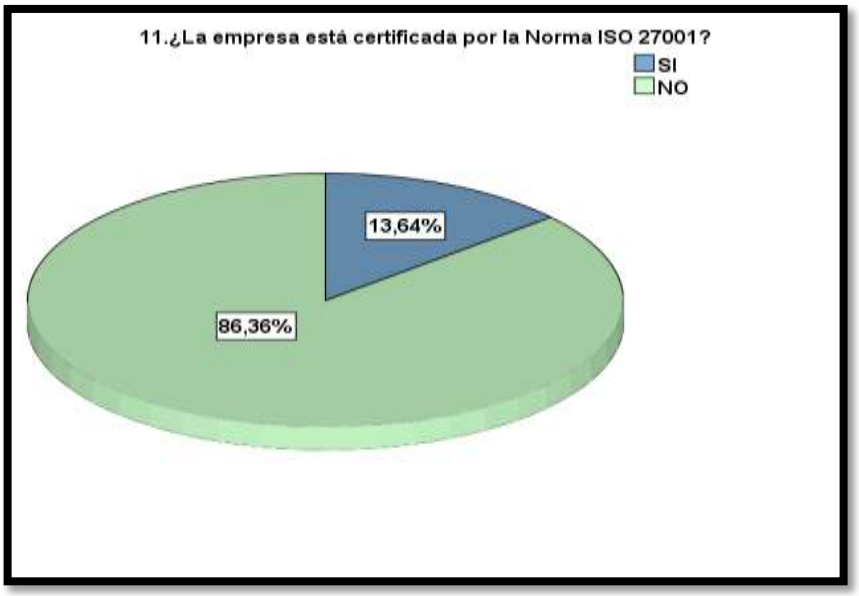

Figura 114. Norma ISO 27001

Interpretación

Las áreas mencionan que el 13,64% las empresas si cuentan con la Certificación de la Normativa ISO 27001 es decir que solo 3 empresas cuentan con esta certificación y el 86.36% no tienen la certificación y es muy importante tener la certificación para un mayor control de las herramientas de seguridad y protección de datos.

12. **¿Los usuarios autorizados a utilizar los accesos a redes y los servicios de red cuentan con políticas de control de Accesos a la información?**

Tabla 146

Políticas de control de Accesos a la información

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	12	54,5	54,5
NO	10	45,5	100,0
Total	22	100,0	

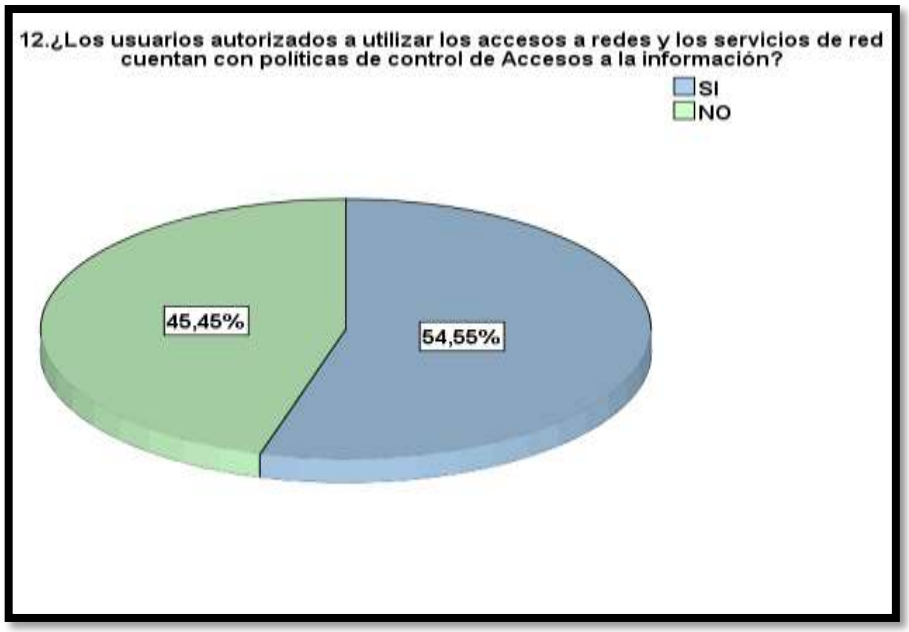

Figura 115. Norma ISO 27001

Interpretación

El 54.38% expresan que si cuentan con políticas de control de acceso a la información dentro del área y la empresa y el 45.45% dice que no cuentan con las políticas y es necesario que las empresas tengan dichas políticas para mejor manipulación y acceso a las redes y los servicios de red en la empresas.

13. ¿Qué tipo de empleados tienen acceso al código fuente de las aplicaciones de software?

Tabla 147

Acceso al código fuente

Personal	INCLUYE		NO INCLUYE		Total
	Frecuencia	Porcentaje de Respuesta SI	Frecuencia	Porcentaje de Respuesta NO	
Programadores	10	45,50%	12	54,5%	100%
Jefe de Sistemas	11	50,00%	11	50,0%	100%
Personal Gerencia	5	22,70%	17	77,3%	100%

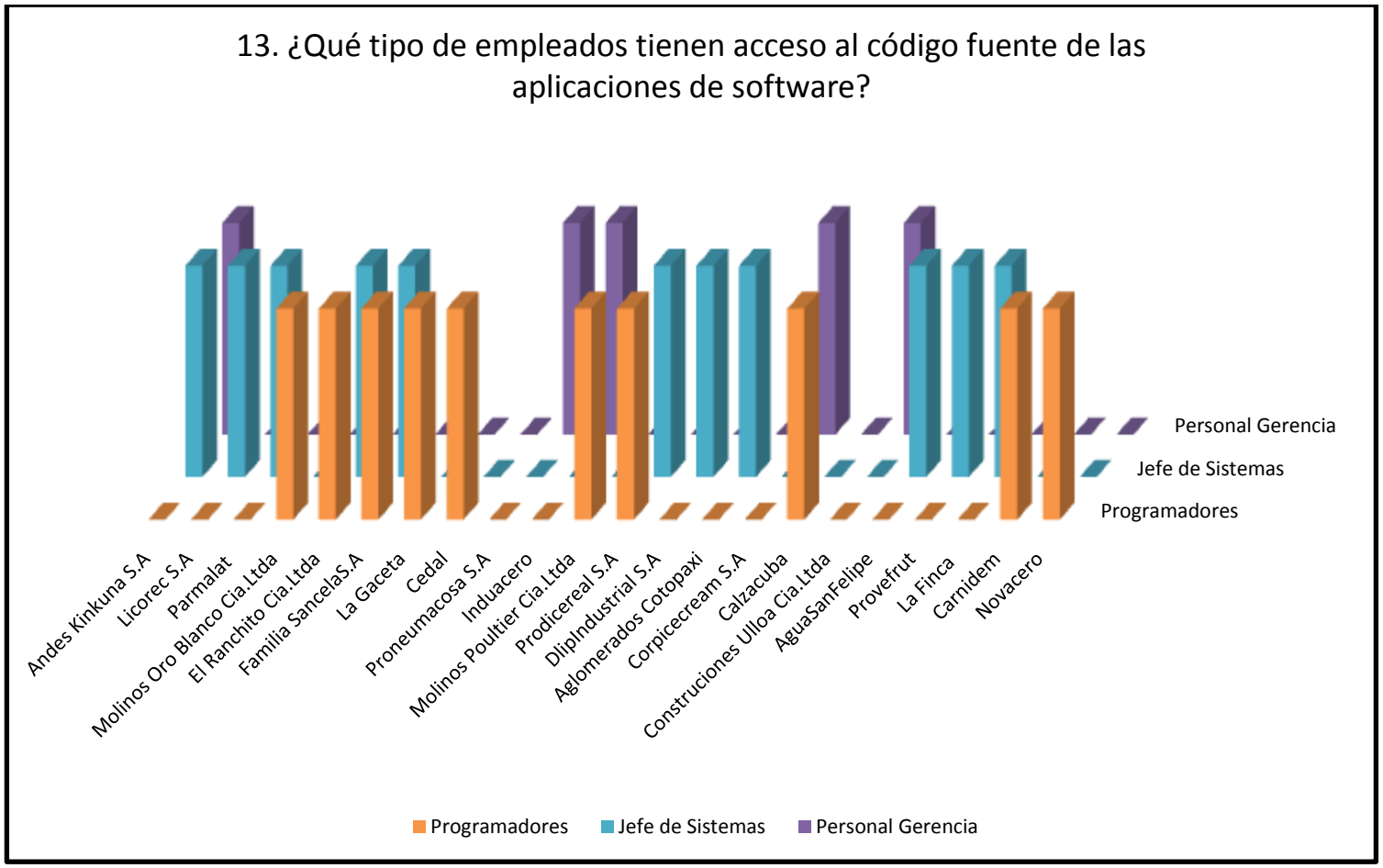

Figura 116. Acceso al código fuente

Interpretación

Del total de las empresas encuestadas se obtuvo como resultados que el 45,45% de las empresas los Programadores tienen acceso al código fuentes de las aplicaciones de software instaladas en los distintos equipos mientras que el 54.5% acceden otro personal de empresa. El 50% los Jefes de Sistemas de las empresas tienen accesos al código fuente y el otro 50% es otro personal quien accede. El 22,23% el personal de Gerencia accede al código fuente y el 77,77% accede otro personal. Podemos mencionar que los empleados que tienen mayor acceso al código fuente de las aplicaciones son los Jefes de Sistemas.

14. ¿Los sistemas de la empresa poseen procedimientos de re-autenticación?

Tabla 148

Re-autenticación

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	15	68,2	68,2
NO	7	31,8	100,0
Total	22	100,0	

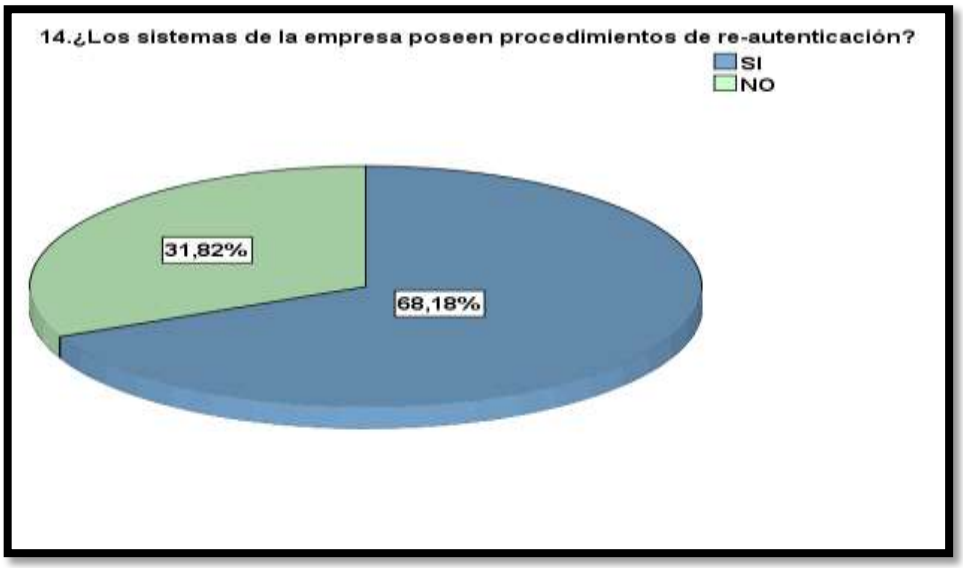

Figura 117. Re-autenticación

Interpretación

El 68.18% expresan que las empresas si tienen procedimientos de re-autenticación y el 31.82% señalan que no poseen y es necesario tenerla para evitar la intromisión de personal no autorizadas a los sistemas.

15. ¿Las actualizaciones de software y/o sistema operativo son sometidas a revisión antes de ser implementadas?

Tabla 149

Actualizaciones de software y/o sistema operativo

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	19	86,4	86,4
NO	3	13,6	100,0
Total	22	100,0	

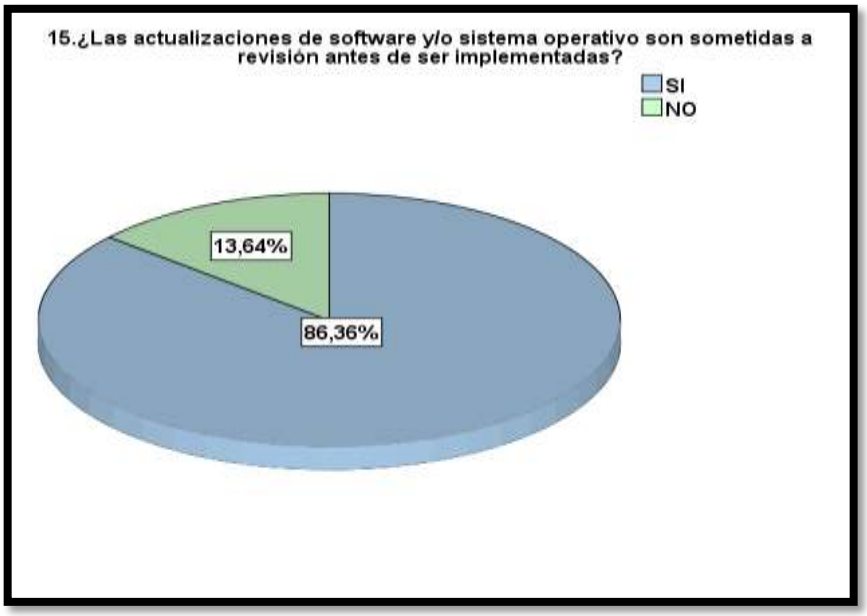

Figura 118. Actualizaciones de software y/o sistema operativo

Interpretación

Es muy necesario que las empresas realicen controles y revisiones de los nuevos software y sistemas operativos para evitar configuraciones no deseadas en los mismos, y en las encuestas realizadas a las empresas del Sector Industrial mencionan los siguiente que el 85.71% expresa las revisiones y actualizaciones del software antes de ser implementadas y el 14.29% manifiesta que no lo realizan.

16. ¿Existe un sitio de recepción que filtre la entrada de personal autorizado a la empresa?

Tabla 150

Existe un sitio de recepción que filtre la entrada

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	18	81,8	81,8
NO	4	18,2	100,0
Total	22	100,0	

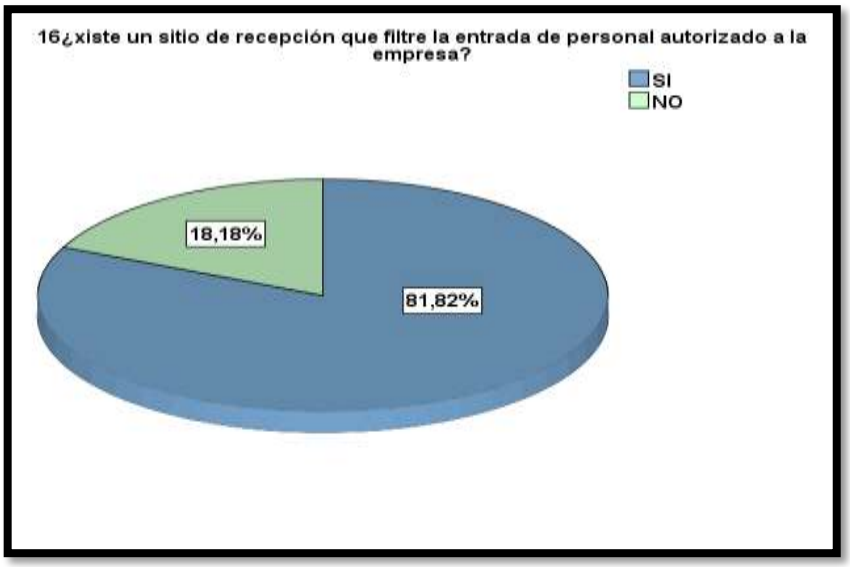

Figura 119. Recepción que filtre la entrada

Interpretación

Hacia mayor seguridad es importante tener una recepción de entrada y salida en la empresa para que el mismo pueda realizar el control respectivo de las personas que ingresan y su respectiva identificación, en las encuestas realizadas las empresas expresan que el 81.82% tienen una recepción donde se filtra la entrada del personal, mientras que 18.18% dicen que no tienen la recepción del filtro de entrada.

17. El sitio en donde se ubican los recursos informáticos están protegidos de accesos no autorizados.

Tabla 151

Recursos informáticos están protegidos

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	21	95,5	95,5
NO	1	4,5	100,0
Total	22	100,0	

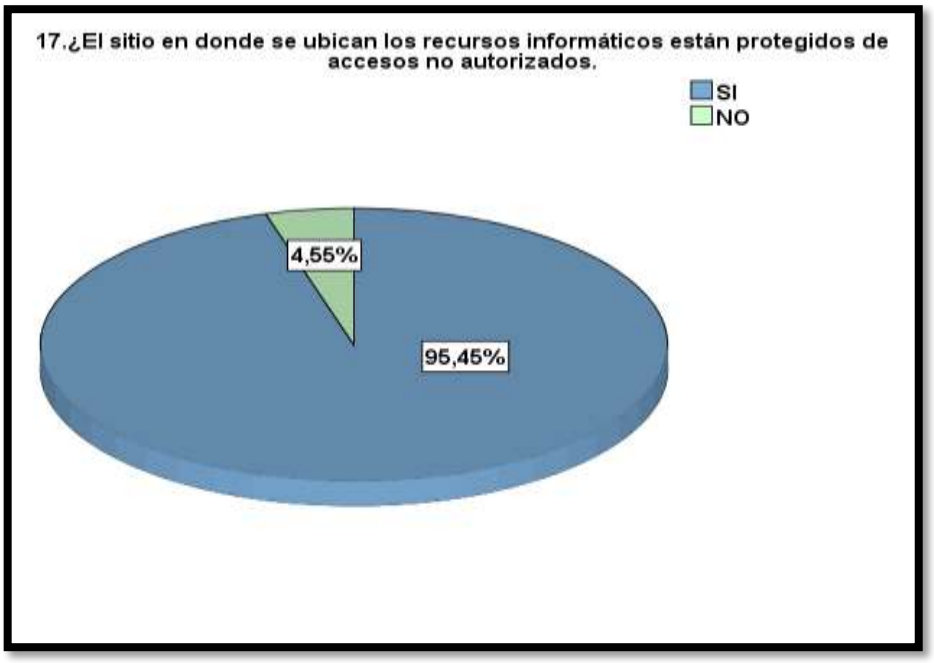

Figura 120. Recursos informáticos están protegidos

Interpretación

El 95.45% de las área del total de las encuestas realizadas mencionan que si se encuentran protegidos los recursos informáticos y existe una mínima parte del 4.55% de las empresas del sector Industrial de Cotopaxi dicen que no se encuentran protegidos.

18. ¿El mantenimiento de Equipos lo realiza el personal autorizado?

Tabla 152

Mantenimiento de Equipos lo realiza el personal autorizado

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	22	100,0	100,0

Figura 121. Mantenimiento de Equipos lo realiza el personal autorizado

Interpretación

El 100% del total de las encuestas realizadas a las empresas del Sector Industrial mencionan que el mantenimiento a los equipos lo realiza el personal

autorizado la cual es ideal para su buen funcionamiento y se evite daños o perjuicios de las entidades.

19. **Se permite la salida de equipos de procesamiento de la información (computadoras personales, agendas electrónicas) pertenecientes a la empresa.**

Tabla 153

Se permite la salida de equipos

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	2	9,1	9,1
NO	20	90,9	100,0
Total	22	100,0	

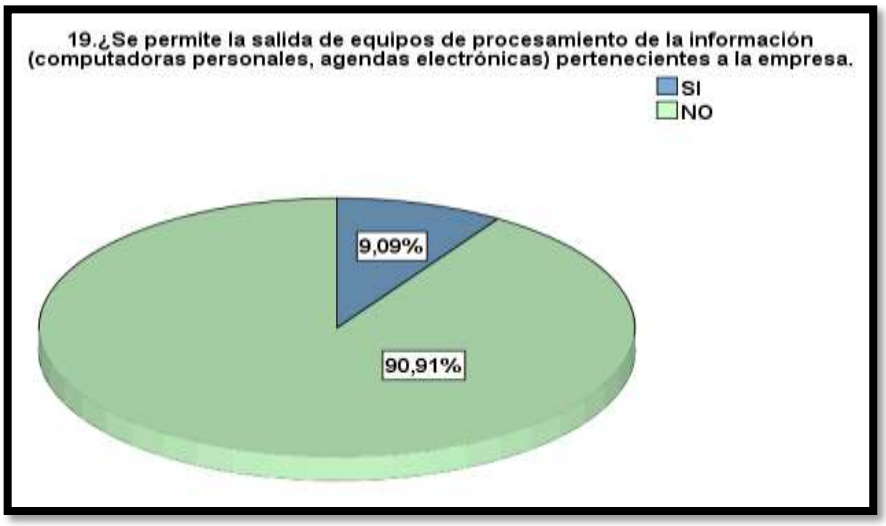

Figura 122. Se permite la salida de equipos

Interpretación

De las encuestas realizadas en el área de Informática de las empresas indica que un 9.09% se les permite la salida de los equipos de la empresa lo cual no es adecuado para la seguridad de los equipos y el 90.91% no se les permite la salida de los equipos eso es muy importante que la empresa cuide los equipos y que se los utilice sólo dentro del mismo.

20. ¿Se administra y controla las redes para acceso solo de equipos autorizados?

Tabla 154

Se administra y controla las redes

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	18	81,8	81,8
NO	4	18,2	100,0
Total	22	100,0	

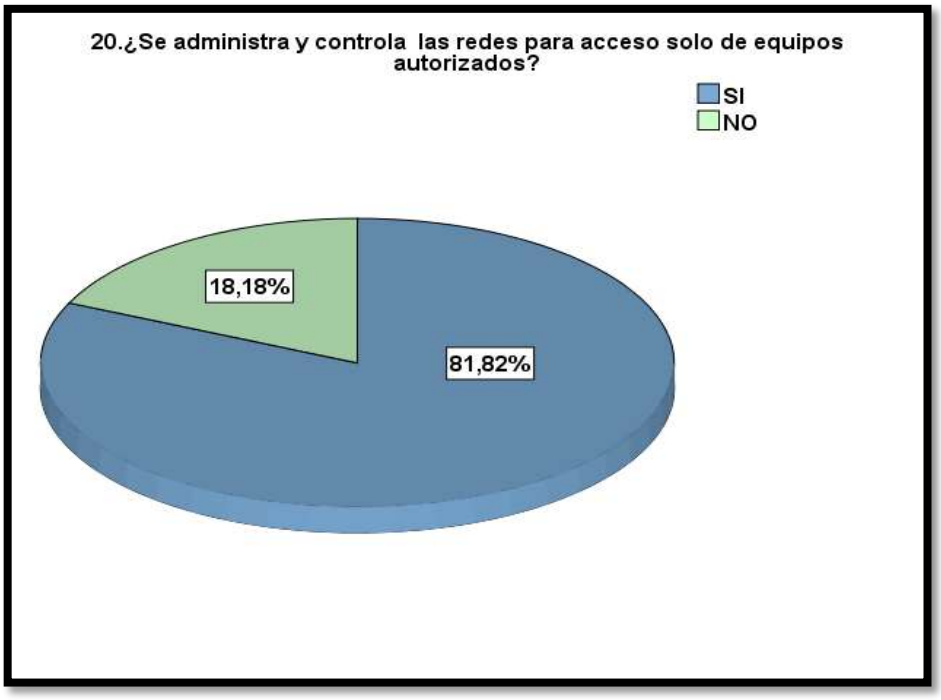

Figura 123. Se administra y controla las redes

Interpretación

El 81.82% de las empresas mencionan que se administra y controla las redes para el acceso a los equipos en la empresa y con un porcentaje de 18.18% dice que no hay control ni administración de las redes.

21. ¿Las redes se encuentran separadas en función de los servicios, usuarios y sistemas de información?

Tabla 155

Las redes se encuentran separadas en función

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	21	95,5	95,5
NO	1	4,5	100,0
Total	22	100,0	

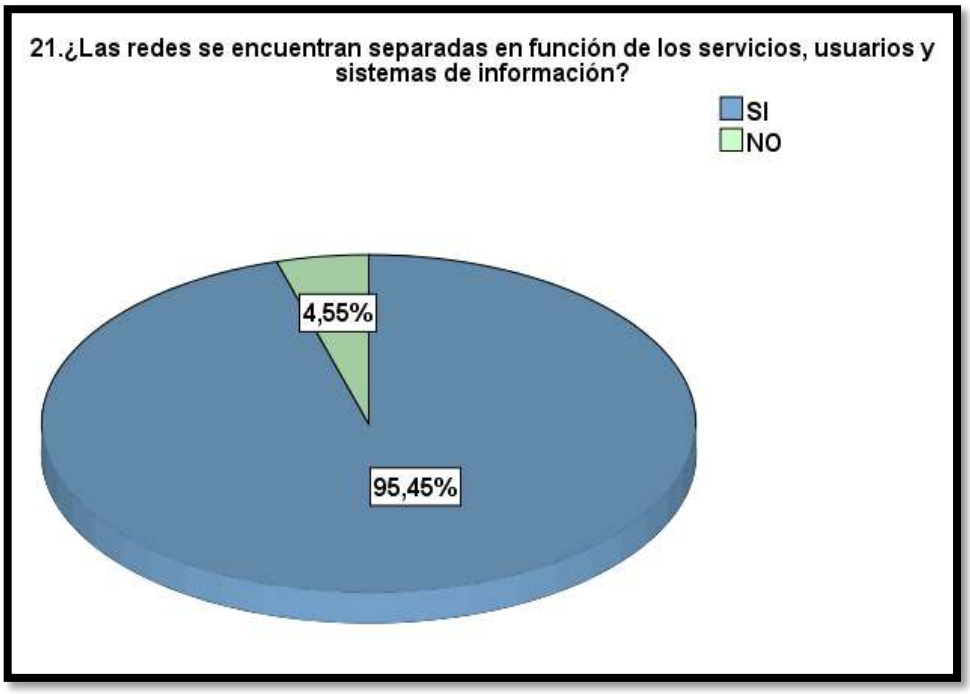

Figura 124.Las redes se encuentran separadas en función

Interpretación

El área pronuncia que el 95.45% las redes se en encuentran separadas a las funciones de cada servicio, usuario y sistema en la empresa mientras que con un porcentaje mínimo del 4.55% dicen que no tienen Funciones clasificadas.

22. ¿Cuáles de los siguientes controles de seguridad se ha implementado en su empresa para protección de información?

Tabla 156

Controles de seguridad

Control	INCLUYE		NO INCLUYE		Total
	Frecuencia	Porcentaje de Respuesta SI	Frecuencia	Porcentaje de Respuesta NO	
Software antivirus	21	95,5%	1	4,5%	100%
Firewall	9	40,9%	13	59,1%	100%
Respaldo de la información (Back up)	13	59,1%	9	40,9%	100%
Anti – spam	9	40,9%	13	59,1%	100%
Usuarios autenticados en Red	11	50,0%	11	50,0%	100%
Herramientas de detección y prevención	8	36,4%	14	63,6%	100%
Tecnología de Cifrado/descifrado	4	18,2%	18	81,8%	100%
Soluciones de seguridad móviles	5	22,7%	17	77,3%	100%
Soluciones de doble autenticación	3	13,6%	19	86,4%	100%

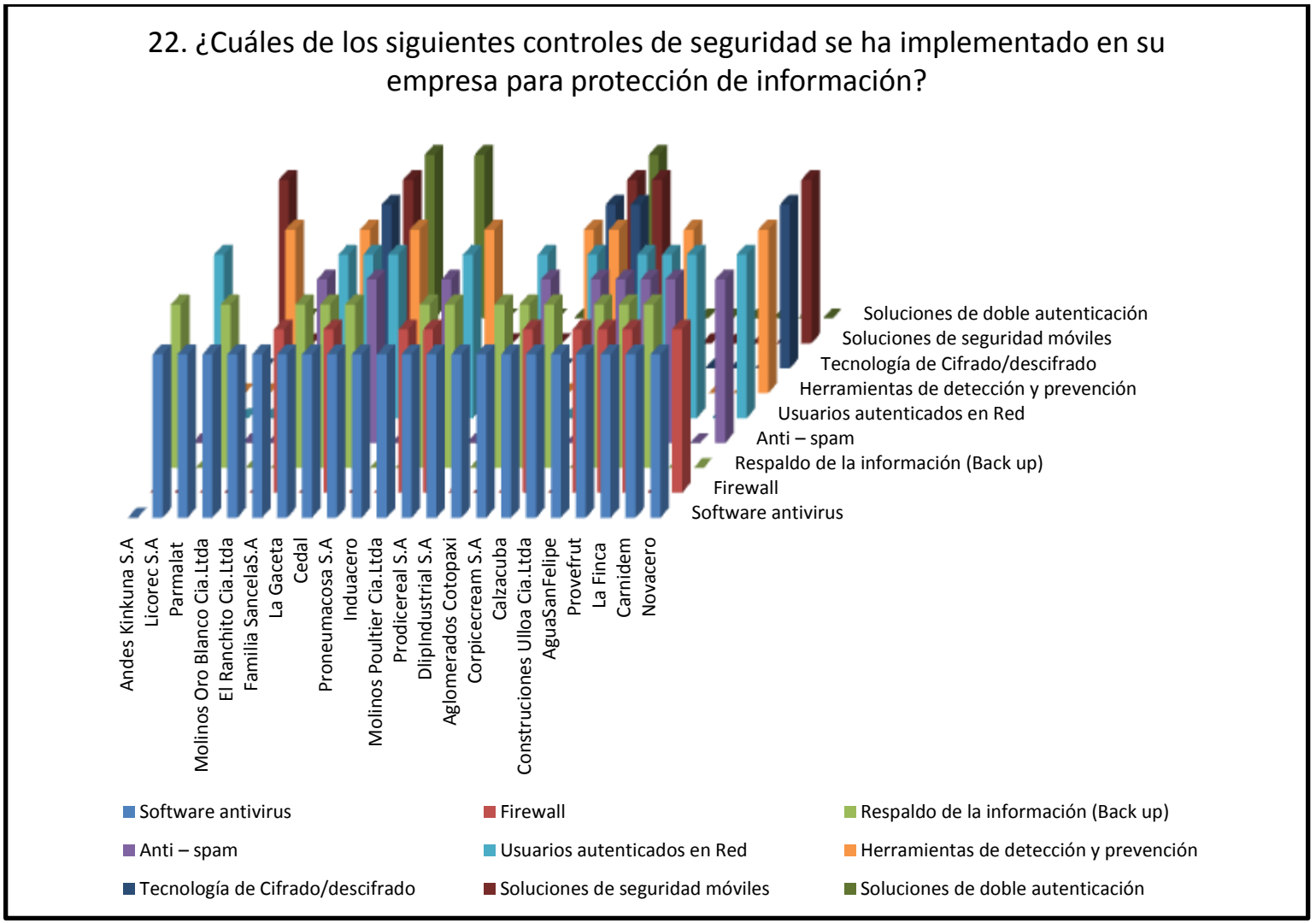

Figura 125. Controles de seguridad

Interpretación

Una vez culminadas las encuestas en las empresas del sector industrial se obtuvo como resultados que del total de empresas el 95,5% de las empresas han implementado software antivirus en sus equipos, el 40,9% han implementado firewall, el 59,1% tienen como controles respaldos de información, el 40,9% han instalado anti spam como control de seguridad, el 50% de las empresas tienen controles de usuarios autenticados en red, el 36,4% han instalado herramientas de detección y prevención para la seguridad de información, el 18,2% cuentan con controles de tecnología de cifrado/ descifrado, el 22,7% cuentan con soluciones para seguridad móvil y el 13,6% de las empresas del sector industrial cuentan con controles de soluciones de doble autenticación.

Se puede observar que el control más utilizado por las empresas es software antivirus dándonos un 95,5%, y el control menos utilizado son las soluciones de doble autenticación con el 13,6%.

23. ¿Cuántos fallos de seguridad (Incidentes) existieron en su empresa durante los años 2012-2016?

Tabla 157

Fallos de seguridad (Incidentes)

Incidentes	Frecuencia	Porcentaje	Porcentaje acumulado
Ninguno	12	54,5	54,5
De 1 a 10	8	36,4	90,9
De 11 a 20	2	9,1	100,0
Total	22	100,0	

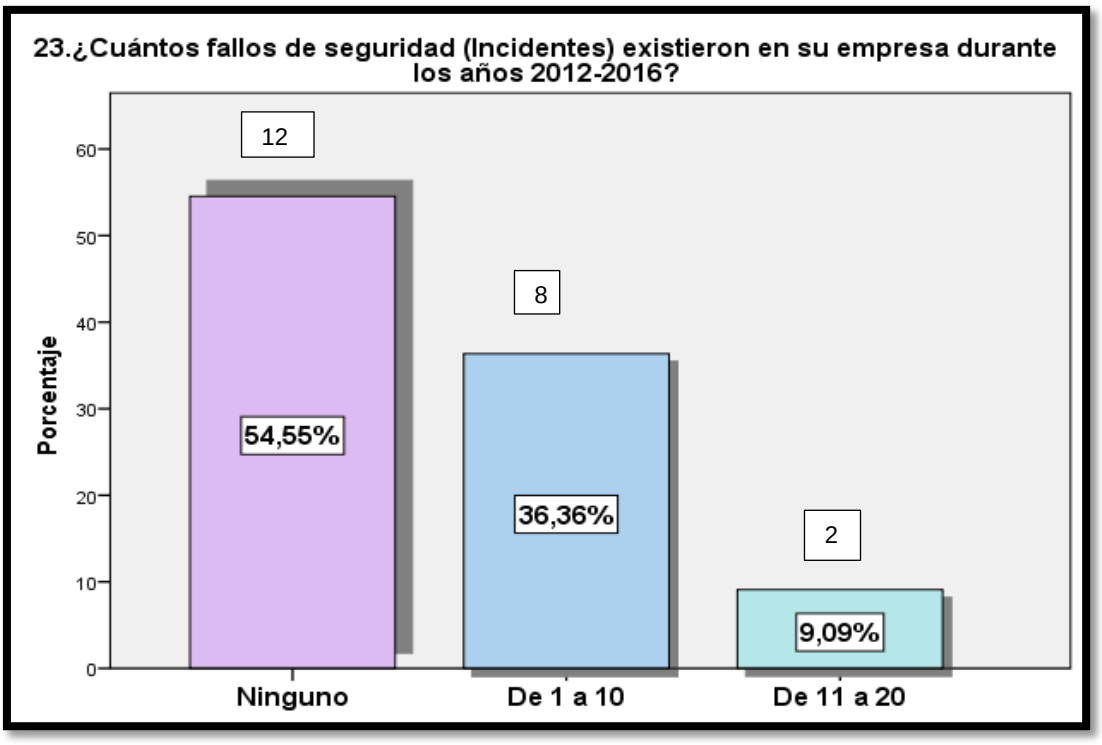

Figura 126. Fallos de seguridad (Incidentes)

Interpretación

El 54.55% no se presentan fallos dentro de las empresas industriales, el 36.36% confirman que existieron fallos entre 1 a 10 en el periodo 2012-2016 y el mismo las empresas deben tener mayor control para evitarlo o eliminar con los incidentes, y el 9.09% corroboran los fallos entre 11 a 20 en las entidades en el que es mínimo este porcentaje pero no se debe de pasar por alto ya que ocurren más incidentes en las empresas.

24. ¿De acuerdo a la pregunta anterior cuánto le costaron esos fallos?

Tabla 158

Costo de fallos

Costos	Frecuencia	Porcentaje	Porcentaje acumulado
Ninguno	13	59,1	59,1
$1 - $10000	7	31,8	90,9
$10001 - $30000	2	9,1	100,0
Total	22	100,0	

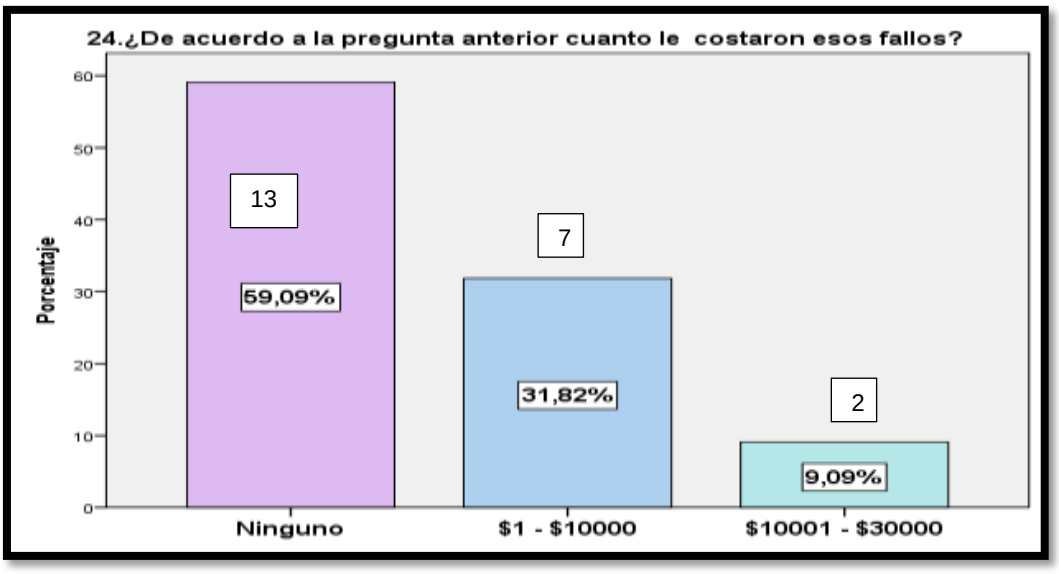

Figura 127. Costo de fallos

Interpretación

El área menciona que un 59.09% no se presentaron costo por los fallos, el 31.82% afirman haber tenido costos entre $1 a $10.000 por los fallos, y el 9.09% constatan los costos entre $10.001 a $30.000 por los fallos habidos, y al poder evitar con los incidente la empresas podrían ahorrar o evitar estos Gastos.

25. ¿La empresa cuenta con controles criptográficos?

Tabla 159

Controles criptográficos

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	10	45,5	45,5
NO	12	54,5	100,0
Total	22	100,0	

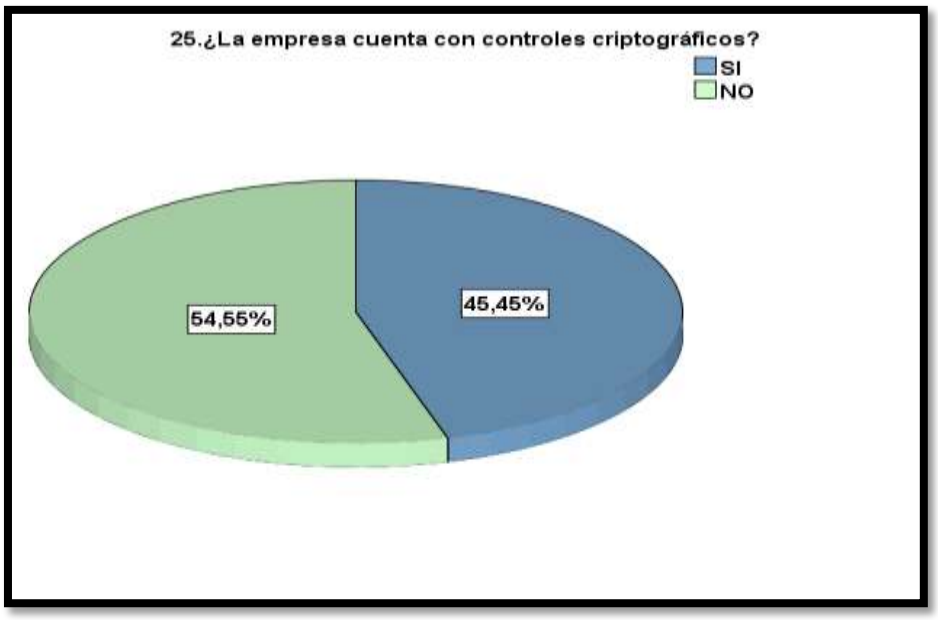

Figura 128. Controles criptográficos

Interpretación

El 45.45% afirman que las empresas si cuentan con controles Criptográficos, mientras que el 54.55% un porcentaje considerable dicen que no mantienen controles criptográficos dentro de la empresa y el mismo está vulnerable al sustracción de información exclusiva de las empresas.

26. ¿En la organización se cuenta con un sistema de gestión de contraseñas interactivos y de calidad?

Tabla 160 Gestión de contraseñas interactivos y de calidad

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	15	68,2	68,2
NO	7	31,8	100,0
Total	22	100,0	

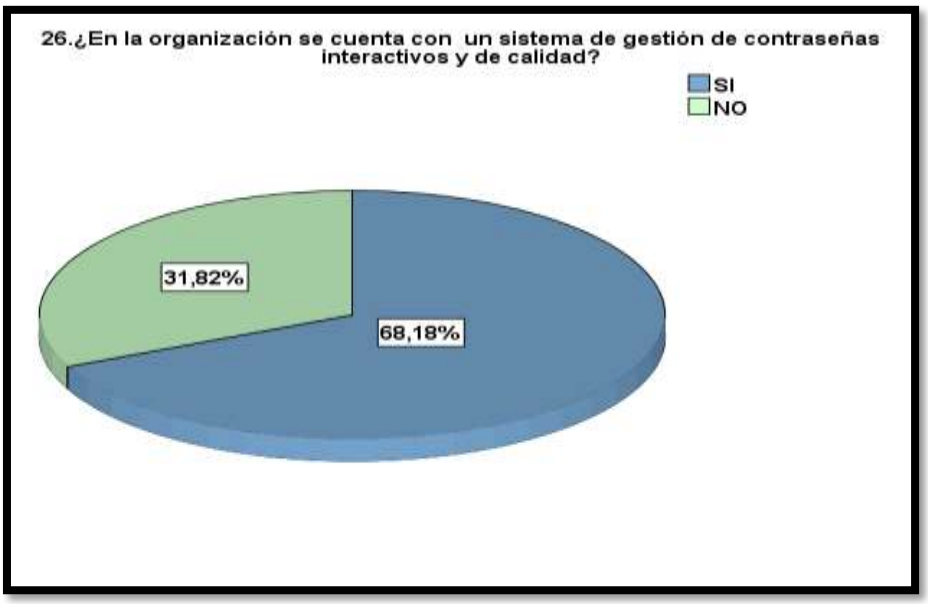

Figura 129. S.G de contraseñas interactivos y de calidad

Interpretación

Del total de las encuestas realizadas las empresas Industriales mencionan que el 68.18% si tienen un sistema de gestión de contraseñas, mientras que el 31.82% manifiestan que no cuentan con el sistema de contraseñas interactivas y de calidad se podría decir que las mismas se encuentran vulnerables a posibles intromisiones de personas no autorizadas a los sistemas.

Departamento de Producción y Comercialización

27. ¿Puede usted ingresar en el sistema de la empresa a otras áreas?

Tabla 161

Ingresar al sistema en otras áreas

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	6	27,3	27,3
NO	16	72,7	100,0
Total	22	100,0	

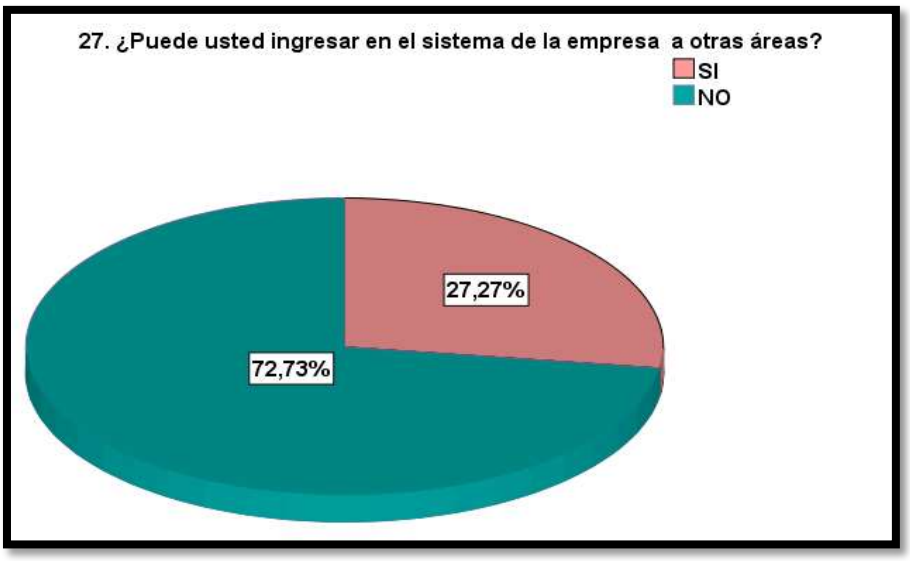

Figura 130. Ingresar al sistema en otras áreas

Interpretación

Según los resultados arrojados de la encuesta se obtuvo que el 72,73% de las empresas los empleados de la parte administrativa pueden ingresar a los sistemas en cualquier área y el 27,27% no tienen acceso.

28. ¿Ha recibido una sociabilización sobre directrices que posee la empresa relativa a seguridad de la información?

Tabla 162

Sociabilización relativa a la Seguridad de la Información

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	10	45,5	45,5
NO	12	54,5	100,0
Total	22	100,0	

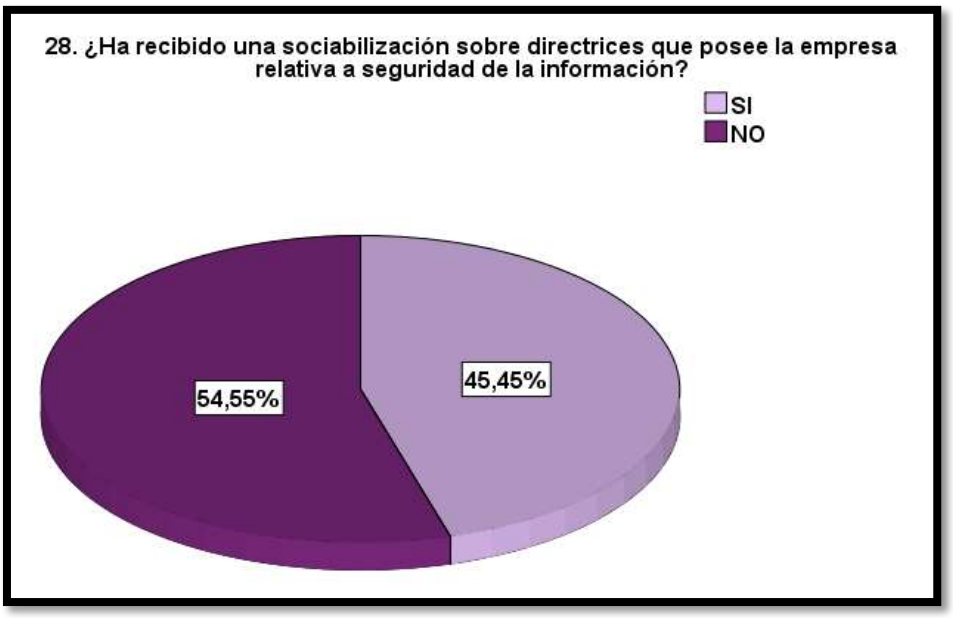

Figura 131. Sociabilización relativa a la Seguridad de la Información

Interpretación.

El 54,55% del total de las empresas del sector Industrial han sociabilizado directrices sobre seguridad de la información a sus empleados en los distintos departamentos, mientras que el 45,45% no sociabilizan directrices.

29. ¿Toda el área del departamento de producción se encuentra filtrado el acceso ante personal no autorizado?

Tabla 163

Acceso al personal no autorizado

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	19	86,4	86,4
NO	3	13,6	100,0
Total	22	100,0	

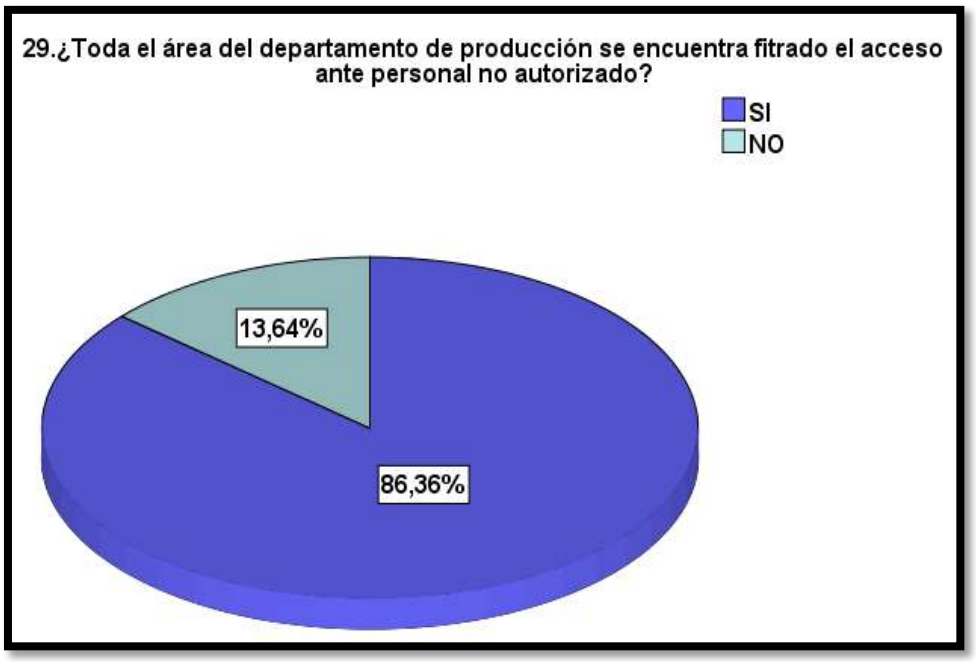

Figura 132. Se filtra el acceso al personal no autorizado

Interpretación

Del total de empresas encuestadas el 86,36% no permiten el acceso de personal no autorizado a los departamentos de producción, y el 13,64% de las empresas del sector industrial no tienen restricciones de ingreso al departamento de producción.

30. Seleccione los tipos de incidentes de seguridad de información que sufrió la empresa durante el período 2012-2016.

Tabla 164

Tipos de Incidentes

Incidentes	**Sufrieron** Respuestas		**No sufrieron** Respuestas		**TOTAL**
	Frecuencia	Porcentaje	Frecuencia	Porcentaje	Porcentaje
Virus	10	45,45%	12	54,54%	100,0%
Phishing	3	13,63%	19	86,36%	100,0%

CONTINÚA

Accesos no autorizados a la web	**1**	**4,54%**	**21**	**95,45%**	**100,0%**
Ataques Ddos	2	9,09%	20	90,90%	100,0%
Ransomware	1	4,54%	21	95,45%	100,0%
Pharming	1	4,54%	21	95,45%	100,0%
Espionaje	2	9,09%	20	90,90%	100,0%
Fuga electrónica de datos	1	4,54%	21	95,45%	100,0%
Otro	1	4,54%	21	95,45%	100,0%
Ninguno	7	31,81%			

Interpretación

Una vez culminadas las encuestas se obtuvo como resultado que del total de empresas encuestadas durante el periodo comprendido del 2012-2016 el 45,45% sufrieron incidentes de virus, el 13,63% phishing, el 4,54% de las empresas del sector industrial sufrieron accesos no autorizados a la web, el 9,09% Ataques Ddos, el 4,54% Ransomware, el 4,54% Pharming, el 9,09% Espionaje, el 4,54% Fuga electrónica de datos 4,54%, el 4,54% sufrieron otro tipo de incidentes y el 31,81% de las empresas del sector industrial no sufrieron ningún tipo de incidente.

Los resultados arrojaron que las empresas del sector industrial sufrieron en el periodo 2012-2014 mayor incidentes por Virus, Phishing, ataques Ddos, Espionaje.

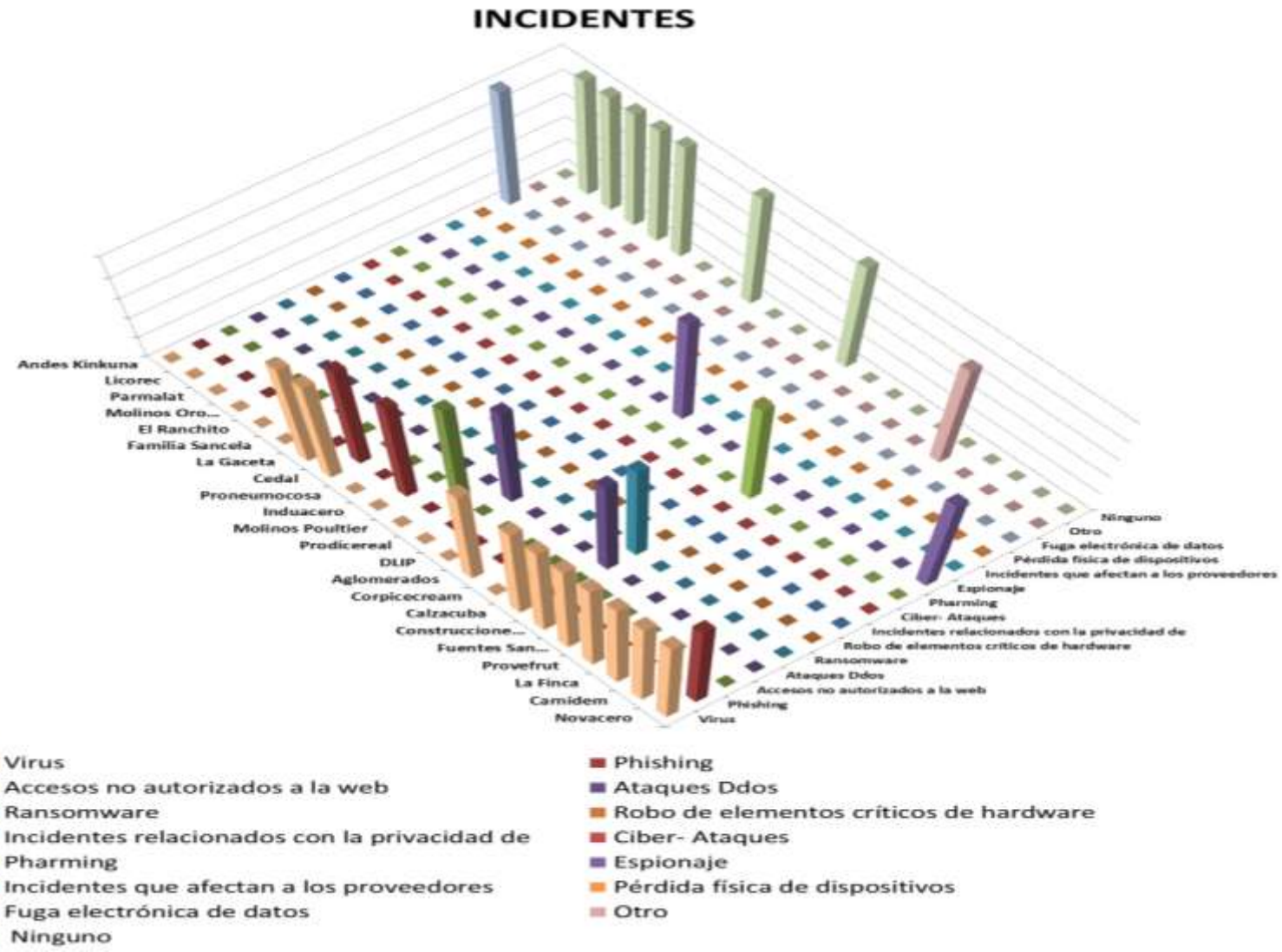

Figura 133. Tipos de Incidentes

31. ¿Se da un seguimiento adecuado cuando el área ha tenido algún incidente en la seguridad de información?

Tabla 165

La empresa da un seguimiento a los incidentes

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	11	50,0	50,0
NO	11	50,0	100,0
Total	22	100,0	

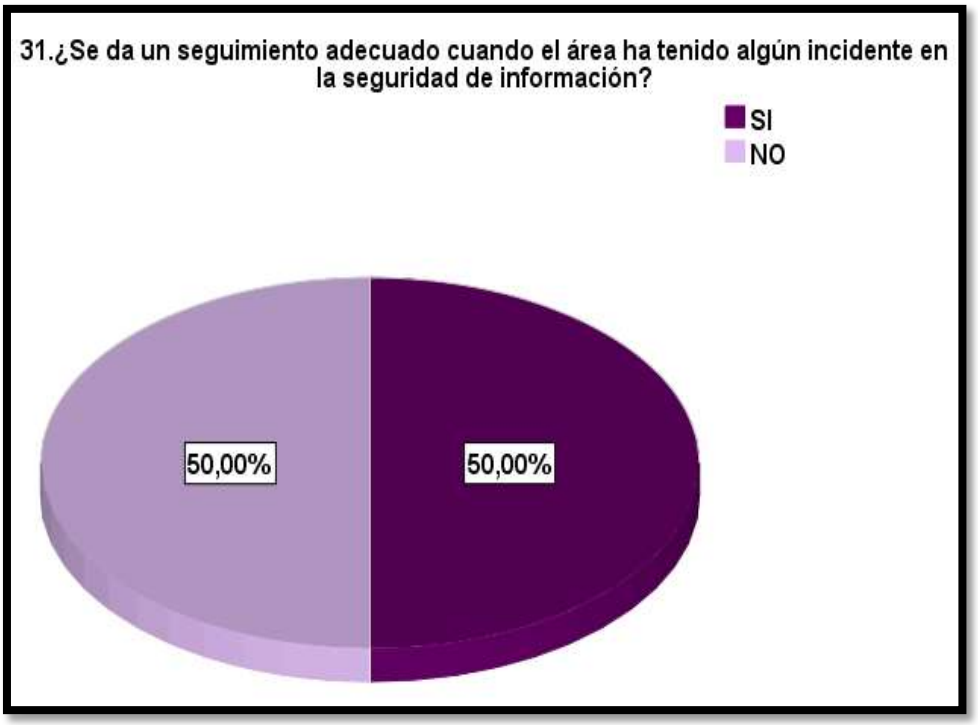

Figura 134. La empresa da un seguimiento a los incidentes

Interpretación

Del total de encuestas realizadas el 50% respondieron que después de haber sufrido algún incidente en seguridad de información se da seguimiento adecuado, y el 50% de los representantes de las empresas respondieron que no dan seguimiento.

32. ¿Tiene métodos de control de integridad para datos y transacciones?

Tabla 166

Métodos de control de integridad

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	21	95,5	95,5
NO	1	4,5	100,0
Total	22	100,0	

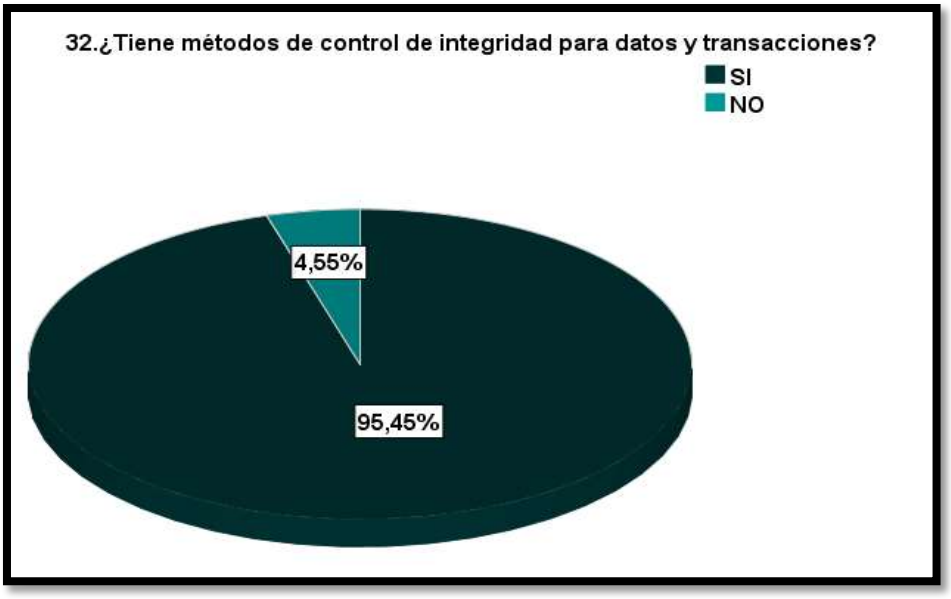

Figura 135. Métodos de control de integridad

Interpretación

Del total de representantes de las empresas Industriales encuestadas el 95,45% respondieron que aplican métodos de control de integridad de datos y transacciones y el 4,55% dijeron que no tienen métodos ni los aplican.

33. ¿Se ha presentado fugas sobre información enviada o recibida por mensajería electrónica?

Tabla 167

Fuga de información

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	7	31,8	31,8
NO	15	68,2	100,0
Total	22	100,0	

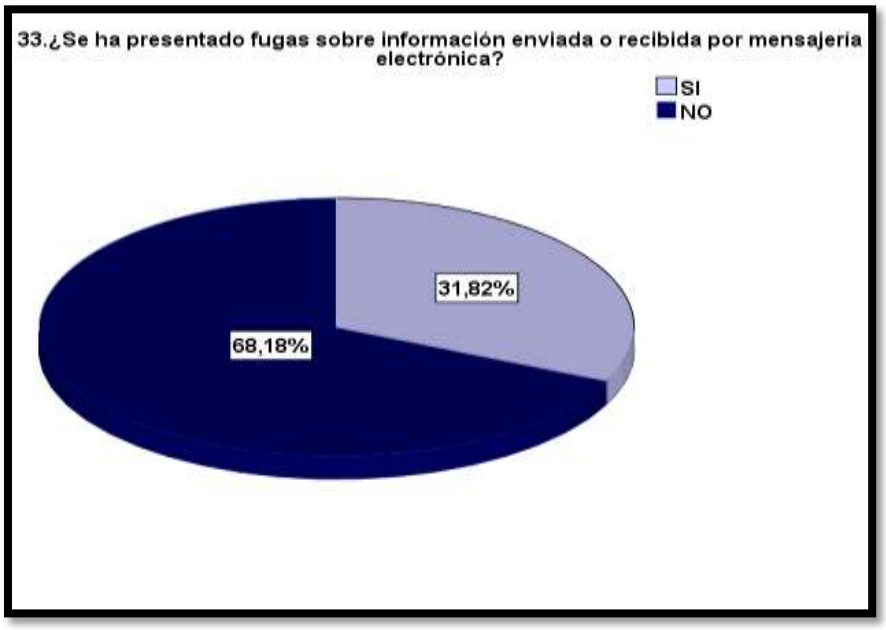

Figura 136. Fuga de información

Interpretación

Del total de empresas encuestadas el 68,18% no han tenido fugas de información enviada o recibida por mensajería electrónica y el 31,82% de las empresas sufrieron fugas de información enviada o recibida por mensajería electrónica.

34. ¿Le exigen cambiar sus contraseñas de forma regular?

Tabla 168

Cambio de contraseñas

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	16	72,7	72,7
NO	6	27,3	100,0
Total	22	100,0	

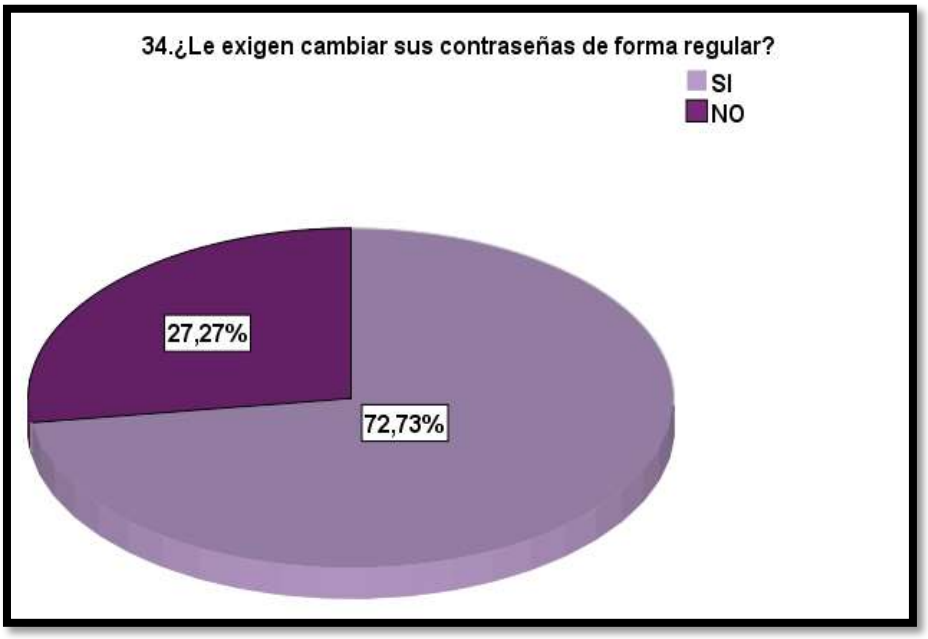

Figura 137. Cambio de contraseñas

Interpretación

Una vez realizadas las encuestas se pudo obtener que el 72,73% de las empresas exigen a sus empleados cambiar de forma regular sus contraseñas y el 27,27% de las empresas no lo realizan y se han mantenido con las mismas contraseñas.

35. ¿Se solicita una identificación por parte del responsable del equipo antes de aceptar el servicio de mantenimiento?

Tabla 169

Solicitud de identificación

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	13	59,1	59,1
NO	9	40,9	100,0
Total	22	100,0	

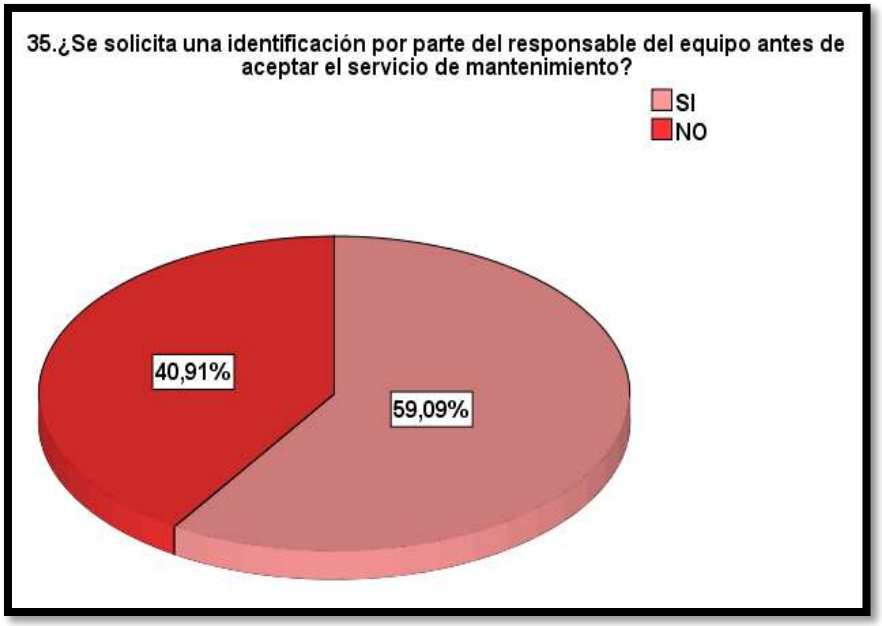

Figura 138 Solicitud de identificación

Interpretación

Al culminar el desarrollo de las encuestas se puede constatar que en el 40,91% del total de empresas los responsables de los equipos no solicitan identificación alguna antes de aceptar un servicio de mantenimiento, por el contrario el 59,09% de las empresas afirman que los responsables de los equipos si solicitan identificaciones antes de aceptar un servicio de mantenimiento.

36. ¿Dentro de la Planificación Estratégica de la empresa se establece un monto de inversión para la Seguridad de Información?

Tabla 170

Montos de inversión en la Planificación estratégica

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	12	54,5	54,5
NO	10	45,5	100,0
Total	22	100,0	

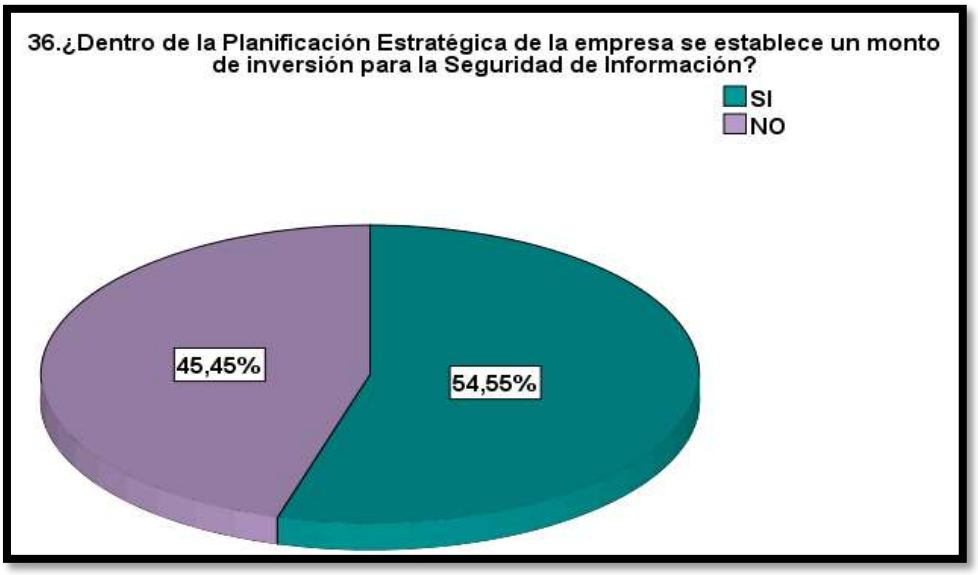

Figura 139. Montos de inversión en la Planificación estratégica

Interpretación

Del total de empresas encuestadas podemos afirmar que el 54,55% establecen montos de inversión para la Seguridad de Información en su planificación estratégica y por el contrario el 45,45% de las empresas sus colaboradores dentro de la planificación estratégica no establecen un monto de inversión para la Seguridad de Información.

37. ¿Tiene herramientas adecuadas para el resguardo de la información?

Tabla 171

Herramientas adecuadas

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	21	95,5	95,5
NO	1	4,5	100,0
Total	22	100,0	

Figura 140. Herramientas adecuadas

Interpretación

Del total de empresas encuestadas el 95,45% presentan herramientas adecuadas para e resguardo de información y por el contrario apenas el 4,55% no tienen herramientas adecuadas que les sirva para resguardar la información.

38. ¿Los colaboradores aplican políticas de pantallas limpias y escritorios limpios de papeles?

Tabla 172

Políticas de pantallas y escritorios limpios

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	14	63,6	63,6
NO	8	36,4	100,0
Total	22	100,0	

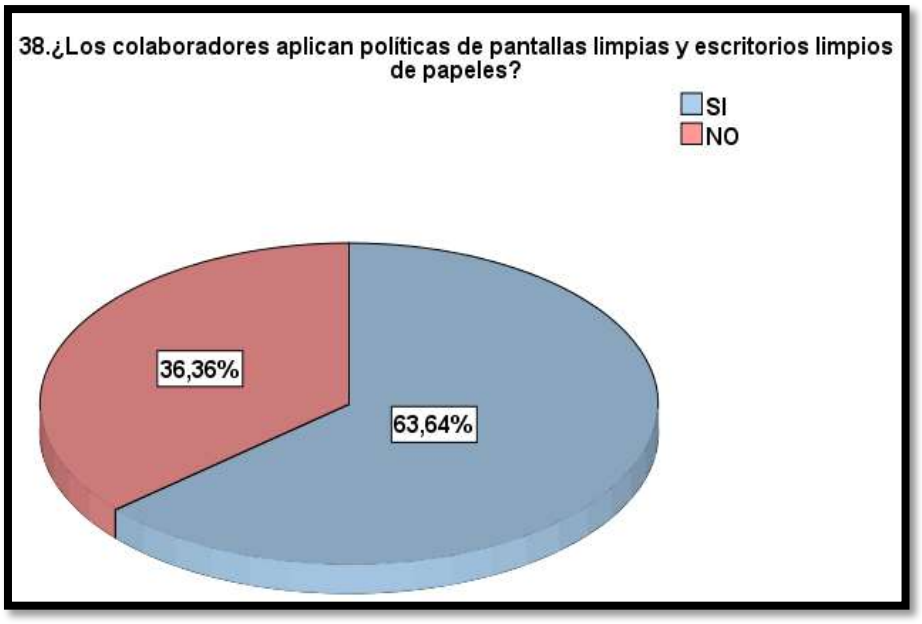

Figura 141. Políticas de pantallas y escritorios limpios

Interpretación

Del total de las encuestas realizadas el 63,64% de las empresas del sector industrial mencionan que sus colaboradores aplican las políticas de pantallas limpias y escritorios limpios de papeles mientras que en el 36,36% de las empresas del sector Industrial sus colaboradores no aplican políticas de pantallas limpias y escritorios limpios de papeles.

39. ¿La empresa cuenta con un presupuesto asignado para las herramientas de seguridad y protección de datos?

Tabla 173

Presupuesto asignado

Presupuesto	Frecuencia	Porcentaje	Porcentaje acumulado
Ninguno	10	45,5	45,5
$1-$5.000	7	31,8	77,3
$5.001-$10.000	3	13,6	90,9
$10.001-$20.000	1	4,5	95,5
Mayor a 40.001	1	4,5	100,0
Total	22	100,0	

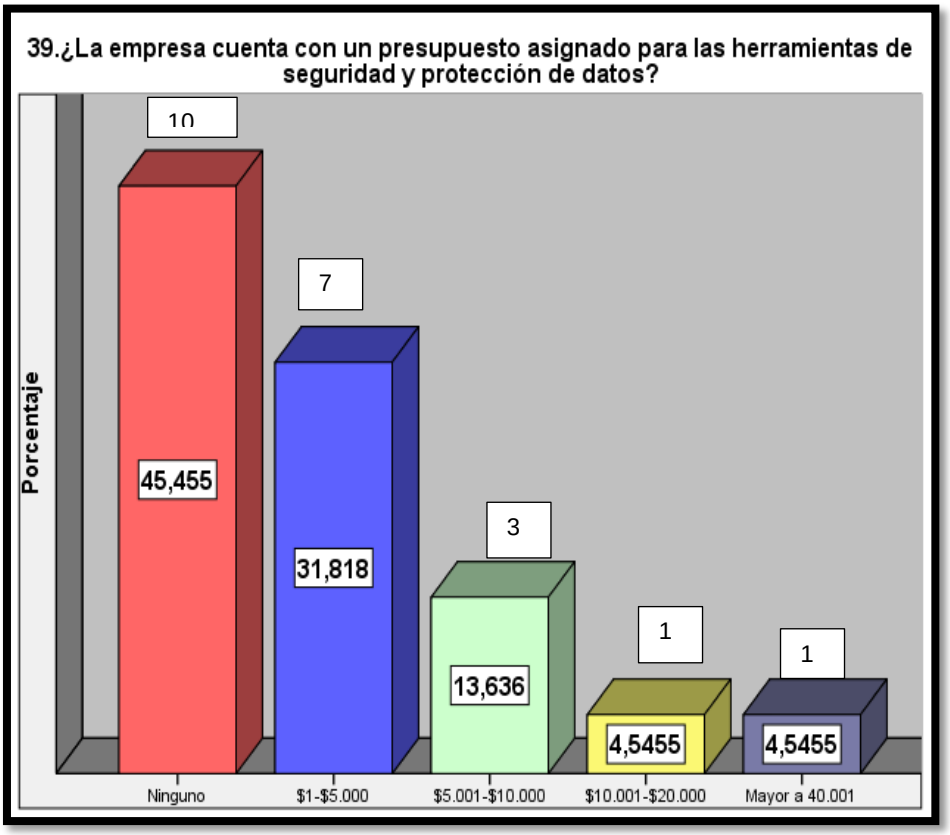

Figura 142. Presupuesto asignado

Interpretación

Una vez culminadas las encuestas se logró obtener como resultados que del total de las empresas encuestadas el 31,81% destinan presupuesto para

herramientas de seguridad y protección de datos entre $1-$5.000, mientras que el 13,6% asignan presupuesto en un rango de $5.001-$10.000, el 4,5% de las empresas Industriales destinan presupuesto en un rango de $10.001-$20.000 y el 4,5% asignan presupuesto mayor a $40.001, además se obtuvo que el 45,45% de las empresas del sector Industrial no asignan presupuesto para las herramientas de seguridad y protección de datos.

40. ¿Qué aspectos, inversiones y gastos están incluidos en su presupuesto para la seguridad de la Información?

Tabla 174

Aspectos que están incluidos en el presupuesto

Aspectos	Incluyen		No Incluyen		Total
	Frecuencia	Porcentaje de casos	Frecuencia	Porcentaje de casos	
Sueldos de personal propio	15	68,18%	7	31,81%	100%
Licencias de Software específico	8	36,36%	14	63,63%	100%
Infraestructura	2	9,09%	20	90,90%	100%
Ninguno	6	18,18%	16	72,72	100%

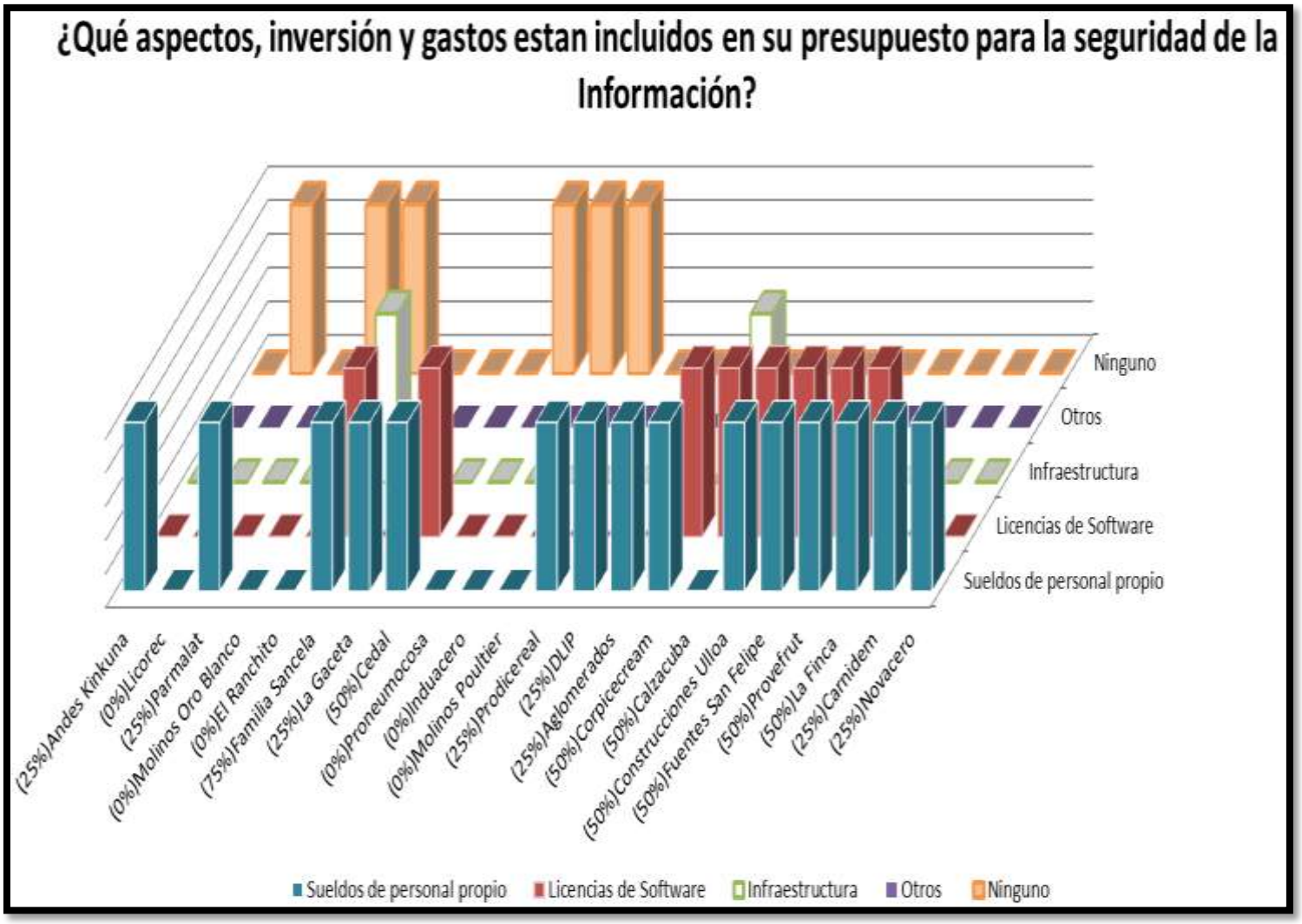

Figura 143. Aspectos que están incluidos en el presupuesto

Interpretación

Una vez realizada la investigación de campo podemos establecer que los Sueldos de personal lo incluyen el 68,18% de las empresas del sector Industrial en su presupuesto para la seguridad de la información, para Licencias de Software lo asignan el 36,36% de las empresas y para infraestructura el 9,09% de las empresas.

Cabe recalcar que el gasto más frecuente que asignan las empresas en su presupuesto es para cubrir sueldos del personal e infraestructura es el que menos consideran las empresas para establecer montos en el presupuesto para la seguridad de la información.

Personal de la Empresa

41. ¿Tiene conocimiento de las políticas de seguridad de la información de la empresa?

Tabla 175

Conoce de políticas de seguridad de la información

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	14	63,6	63,6
NO	8	36,4	100,0
Total	22	100,0	

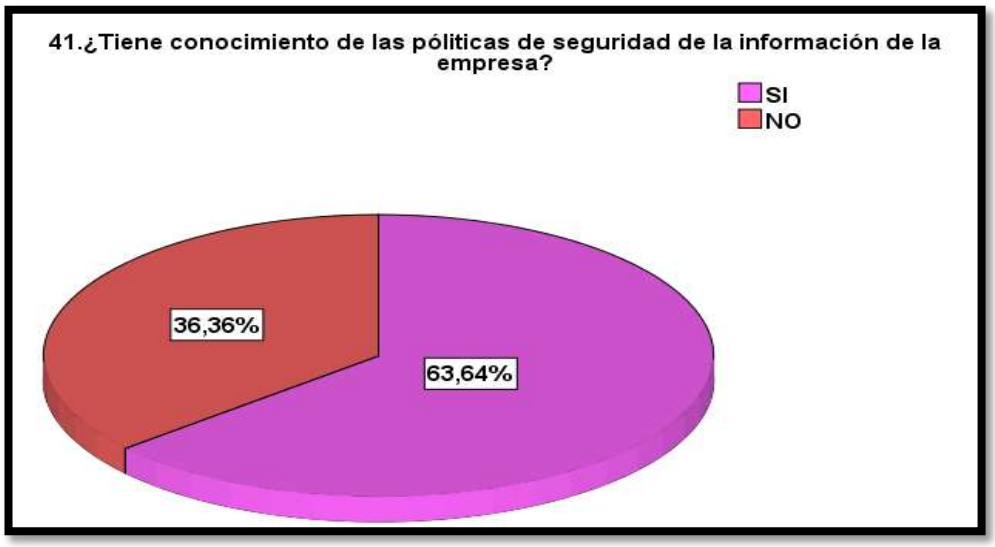

Figura 144. Conoce de políticas de seguridad de la información

Interpretación

Una vez realizada la encuesta se obtuvo que en el 63,64% de las empresas del sector industrial su personal tiene conocimiento de las políticas de seguridad de la información de la empresa y en el 36,36% de las empresas su personal no conoce de las políticas de seguridad de la información que se aplica en la Industria.

42. Al traer dispositivos (Smartphone, portátiles). ¿Puede usted conectarse a la red de la empresa tanto por cable o red de la empresa tanto por cable o red inalámbrica?

Tabla 176

Conectarse a la red de la empresa

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	8	36,4	36,4
NO	14	63,6	100,0
Total	22	100,0	

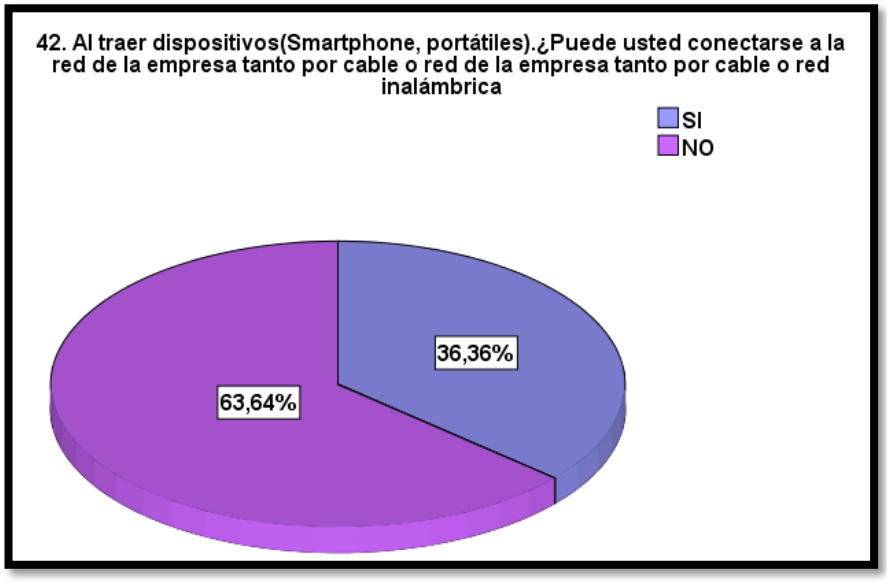

Figura 145. Conectarse a la red de la empresa

Interpretación

Del total de empresas encuestadas podemos decir que en el 36,36% se permite que los empleados puedan conectarse a las redes de la empresa en

sus Smartphone, portátiles ya sea mediante un cable o directamente a través de la red inalámbrica de la empresa, además que en el 63,64% de las empresas no les permiten a sus empleados conectarse a las redes a través de ningún medio.

43. ¿Firmó usted un acuerdo de confidencialidad al ingresar a su puesto de trabajo?

Tabla 177

Acuerdos de confidencialidad

Opciones	Frecuencia	Porcentaje	Porcentaje acumulado
Acuerdo de confidencialidad Antes	14	63,6	63,6
Acuerdo de Confidencialidad después	1	4,5	68,2
Ninguno	7	31,8	100,0
Total	22	100,0	

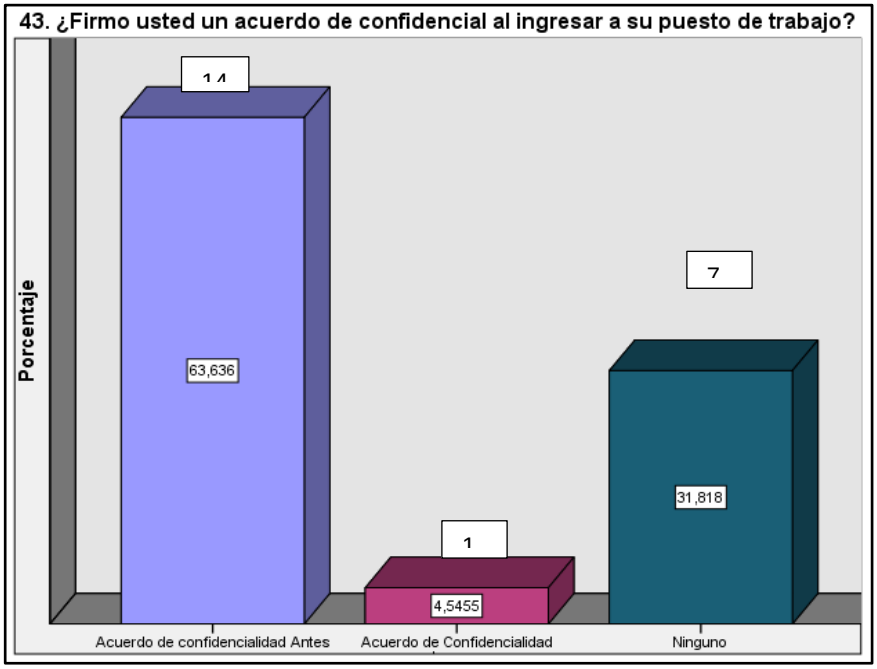

Figura 146. Acuerdos de confidencialidad

Interpretación

Una vez encuestado al personal de las empresas industriales se obtuvo como resultado que en el 63,63% de las empresas los empleados han

firmados acuerdos de confidencialidad antes de ingresar a trabajar, en el 4,54% de las empresas lo firman después y el 31,81% de las empresas no poseen acuerdos de confidencialidad y por ende sus empleados no los han firmado.

44. ¿Al Ingresar a la empresa es requerido su autenticación para el ingreso?

Tabla 178

Se requiere autenticación para el ingreso

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	17	77,3	77,3
NO	5	22,7	100,0
Total	22	100,0	

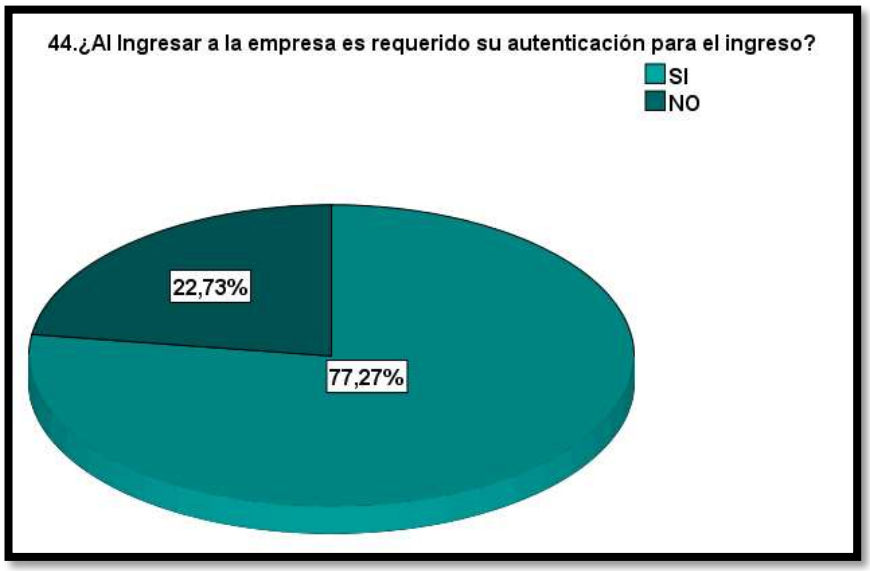

Figura 147. Se requiere autenticación para el ingreso

Interpretación

Del total de empresas del sector industrial encuestadas se obtuvo que en el 23,73% no se requiere ni solicitan ningún tipo de identificación para el ingreso a la empresa y el 77,27% de las empresas si solicitan a cualquier persona que desee ingresar a la industria su autenticación y pasan a través de un filtro en el cual se anuncia el motivo de su visita e identificación.

45. ¿Al utilizar los recursos de red (Internet, Sistemas) tiene algún tipo de autenticación o limitación en el servicio?

Tabla 179

Existe limitación con los recursos de red

Respuesta	Frecuencia	Porcentaje	Porcentaje acumulado
SI	18	81,8	81,8
NO	4	18,2	100,0
Total	22	100,0	

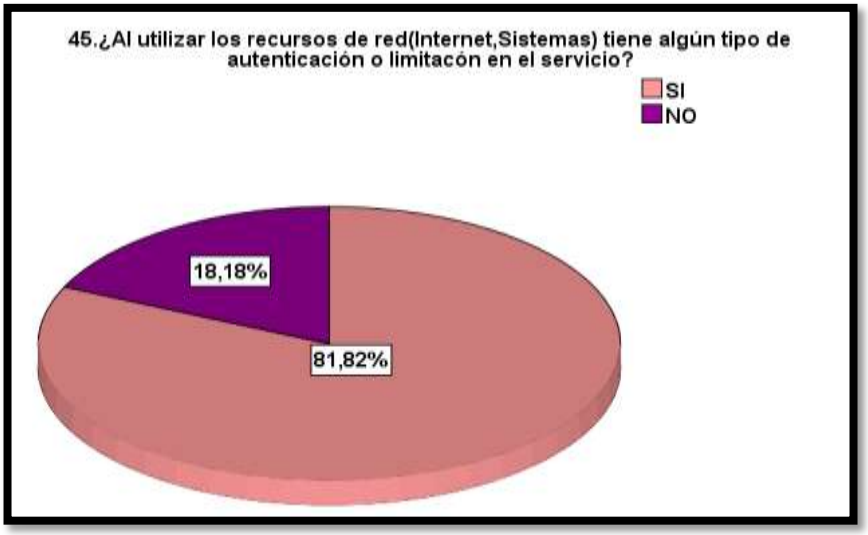

Figura 148. Existe limitación con los recursos de red

Interpretación

Del total de empresas encuestadas se puede observar que en el 81,82% limitan el servicio de internet para sus usuarios restringiendo distintas páginas para evitar entretenimiento y protegen sus sistemas con autenticación por el contrario en el 18,18% de empresas industriales no se limita el servicio de internet y los empleados pueden ingresar a cualquier página

4.2. Comprobación de Hipótesis

a) Hipótesis

(H1)= La inversión en herramientas de seguridad y protección de datos genera un beneficio a las organizaciones del sector industrial reguladas por la Superintendencia de Compañías.

(H0)= La inversión en herramientas de seguridad y protección de datos no genera un beneficio a las organizaciones del sector industrial reguladas por la Superintendencia de Compañías.

b) Señalamiento de Variables

Variable Dependiente (VD): Incremento del beneficio dentro de las organizaciones del sector industrial reguladas por la Superintendencia de Compañías en Seguridad y Protección de datos.

Variable Independiente (VI): Inversión en la aplicación de Herramientas de Seguridad de Información en las organizaciones del sector industrial reguladas por la Superintendencia de Compañías.

c) Comprobación de Hipótesis

En la presente investigación se ha realizado la prueba estadística del Chi-cuadrado que permite medir dos variables y observar si se encuentran relacionadas, con el objeto de comprobar la aceptación de la hipótesis nula o alternativa. De la encuesta aplicada a los departamentos de las distintas empresas del Sector Industrial se consideró dos preguntas que tenían relación con las variables:

Pregunta 2: ¿Cuánto aproximadamente ha invertido la empresa en el período 2012-2016 en herramientas de seguridad y protección de datos?

Pregunta 37: ¿Tiene herramientas adecuadas para el resguardo de la información?

Tabla 180

Relación con las variables

37. ¿Tiene herramientas adecuadas para el resguardo de la información?			Respuestas		Total
			SI	NO	
2. ¿Cuánto aproximadamente ha invertido la empresa en el período 2012-2016 en herramientas de seguridad y protección de datos?	Ninguno	Recuento	0	1	1
		Frecuencia esperada	,9	,1	1,0
	$1-$5000	Recuento	5	1	6
		Frecuencia esperada	5,5	,5	6,0
	$5001-$10000	Recuento	4	0	4
		Frecuencia esperada	3,6	,4	4,0
	$10001-$20000	Recuento	6	0	6
		Frecuencia esperada	5,5	,5	6,0
	$20001-$40000	Recuento	2	0	2
		Frecuencia esperada	1,8	,2	2,0
	Mayor a $40001	Recuento	3	0	3
		Frecuencia esperada	2,7	,3	3,0
Total		Recuento	20	2	22
		Frecuencia esperada	20,0	2,0	22,0

Tabla 181 Pruebas de Chi-cuadrado

Pruebas de Chi-cuadrado			
	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	11,917a	5	,036
Razón de verosimilitudes	7,997	5	,156
Asociación lineal por lineal	4,062	1	,044
N de casos válidos	22		
a. 10 casillas (83,3%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es ,09.			

Resultado

Se eligió un nivel de significancia (α) del 5% (0,05), con 5 grados de libertad se consigue el valor crítico de la tabla de Distribución Chi-Cuadrado x^2 igual a 11,0705 siendo esta menor al valor crítico calculado en el programa Spss con el 11,917 dándonos un valor superior crítico de la tabla donde se encuentra en la zona de aceptación, consecuentemente se rechaza la Hipótesis nula Ho y se acepta la hipótesis Alternativa H1, así podemos concluir que la inversión en herramientas de seguridad y protección de datos genera un beneficio a las organizaciones del sector industrial reguladas por la Superintendencia de Compañías.

CAPÍTULO V

5. ANÁLISIS COSTO BENEFICIO

5.1. Costos de la implementación de herramientas

EMPRESA 1

La empresa cuenta con Políticas de seguridad, a más de ello cuenta con una unidad de externa e Interna de seguridad de la información, además cuenta con contratos y acuerdos de confidencialidad.

Controles necesarios para la empresa:

- Conocimiento y actualización de políticas de seguridad de información y procedimientos de seguridad de la información , salida de equipos de procesamiento de la información a los jefes de personal
- Fallos entre 11 a 20, directrices a la seguridad de la información
- Incidentes (Virus/ Caballos de Troya (Software malicioso), Accesos no autorizados a la web (acceder de manera indebida, descifrando contraseñas), Espionaje (obtener de manera ilícita, información)

Implementaciones necesarias para la empresa:

Políticas

Los activos tangibles no deben tener autorizaciones de salida de las industrias.

Tabla 182

Seguimiento a los controles empresa 1

Controles necesarios	Solución	Costo
Procedimientos de seguridad de la información	Capacitación	$800
Directrices a la seguridad de la información	Capacitación un día	$600
Controles Criptográficos	Instalación y Configuraciones	$135
Presupuesto corrección de fallas		$1.400

Tabla 183

Presupuesto en Herramientas empresa 1

Las empresas que necesitan respaldo de información (BACKUP)	**$400 Anuales**
Licencias Antivirus 30 máquinas	$1.200 Anuales
Capacitaciones	$600
Total Presupuesto de Inversión	$2.200 Anuales

EMPRESA 2

La empresa conserva con Auditoría Interna, Externa, Políticas de seguridad, Estándar, normativa o marco de trabajo (ISO), también cuenta con un departamento Interno que se encargue de la seguridad informática de la empresa, mantiene contratos con los empleados.

La empresa presenta ausencia de:

- Acuerdos de confidencialidad
- Seguimiento de uso de e-mail
- Fallos entre 11 a 20
- Virus/ Caballos de Troya (Software malicioso)
- Fugas sobre información enviada o recibida por mensajería electrónica

Controles necesarios para la empresa:

Políticas

Mantener la confidencialidad con todos los procesos internos de la empresa desde el punto de inicio de labores hasta el cese del mismo.

- Los empleados deberán firmar un acuerdo de confidencialidad/contrato de trabajo antes de iniciar sus labores para así se evitará la divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, precios, manuales.

Uso adecuado de correo electrónico

- Solo el personal autorizado por el jefe directo pueden hacer uso del sistema de correo electrónico empresarial, el acceso del uso del correo empresarial será automáticamente deshabilitado con el cese de actividades.

Tabla 184

Seguimiento a los controles empresa 2

Controles necesarios	**Solución**	**Costo**
Fugas sobre información	Capacitaciones	$ 300
Controles Criptográficos	Instalación y Configuraciones	$135
Presupuesto corrección de fallas		$ 435

Tabla 185

Presupuesto de las Herramientas- empresa 2

	Licencias Antivirus 30 máquinas	**$1.200 Anuales**
	Capacitaciones	$600
Total Presupuesto de Inversión		$1.800 Anuales

EMPRESA 3

La empresa cuenta Auditoría Interna, Externa, Clasificación de la Información, Plan de respuesta a incidentes, Acuerdos y/o contratos (El Acuerdo de Confidencialidad, Acuerdo de Nivel de Servicios), Estándar, normativa o marco de trabajo (ISO).

La empresa presenta ausencia de:

- Fallos entre 1 a 10 p.23
- Virus/ Caballos de Troya (Software malicioso)
- Phishing (Suplantación de identidad)
- Inversión en seguridad de información
- Acuerdos de confidencialidad

Controles necesarios para la empresa:

Políticas:

Mantener la confidencialidad con todos los procesos internos de la empresa desde el punto de inicio de labores hasta el cese del mismo.

- Los empleados deberán firmar un acuerdo de confidencialidad/contrato de trabajo antes de iniciar sus labores para así se evitará la divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, precios, manuales.

Tabla 186

Presupuesto Anual empresa 3

	Las empresas que necesitan respaldo de información (BACKUP)	**$400 Anuales**
	Licencias Antivirus 30 máquinas	$1.200 Anuales
	Capacitaciones	$600
Total Presupuesto de Inversión		$2.200 Anuales

EMPRESA 4

La empresa mantiene Clasificación de la Información, con una unidad de seguridad de información Externa, además presenta contratos con los empleados.

La empresa presenta ausencia de:

- Seguimiento de e-mail
- Acuerdos de confidencialidad
- Conocimiento y actualización de políticas de seguridad de información y procedimientos de seguridad de la información
- Políticas de accesos a la información
- Procesos de re autenticación
- Controles criptográficos
- Contraseñas interactivas
- Directrices a la seguridad de la información

- Filtro de ingreso en el área de producción
- Accesos no autorizados a la web (acceder de manera indebida, descifrando contraseñas)
- Fugas sobre información enviada o recibida por mensajería electrónica
- Políticas de pantallas limpias, escritorios limpios
- Presupuesto de inversión

Controles necesarios para la empresa:

Políticas

Mantener la confidencialidad con todos los procesos internos de la empresa desde el punto de inicio de labores hasta el cese del mismo.

- Los empleados deberán firmar un acuerdo de confidencialidad/contrato de trabajo antes de iniciar sus labores para así se evitará la divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, precios, manuales.

Uso adecuado de correo electrónico

- Solo el personal autorizado por el jefe directo pueden hacer uso del sistema de correo electrónico empresarial.

Sistema de gestión de contraseñas interactivas y de calidad para asegurar el control de acceso a la información sensible.

- Las contraseñas dadas a los colaboradores de la Industrias deben ser únicas e intransferibles.
- Se deben utilizar al menos 8 caracteres para crear la clave, teniendo en cuenta que contengan letras mayúsculas y números.

Protección de la información en cualquiera de sus formas que pueden estar contenidas en escritorios, puestos de trabajo, computadores, medios magnéticos, documentos en papel y en general cualquier tipo de información que utilicen los colaboradores de la empresa.

- Escritorios Limpios: Cuando un trabajador abandona el lugar de trabajo, debe bloquear su ordenador y guardar en lugares seguros

sus documentos, medio magnético u óptico removible que contenga información confidencial.

- Pantallas limpias: Los colaboradores de la empresa deben tener los ordenadores libres de notas tanto en papeles como el protector de pantallas

Tabla 187

Seguimiento a los controles empresa 4

Controles necesarios	Solución	Costo
Procedimientos de seguridad de la información	Capacitación	$400
Políticas de accesos a la información	Solución Uno	Montos
	Equipo servidor/Configuración proxy ACL	$2.000/$700
	Segunda solución	
	Equipo Firewall/Licencia	$2.000/$5.000 anuales
Nota: Pequeñas no tienen muchos usuarios Solución uno.		
Procesos de re autenticación	Configuraciones: Procedimientos de Re autenticación	$150
Controles criptográficos	Instalación y Configuraciones	$235
Directrices a la seguridad de la información	Capacitación	$300
Filtro de ingreso en el área de producción	Lector biométrico + circuito para puertas	$500
Total presupuesto de Inversión Anual		$4.285

Tabla 188

Presupuesto Anual empresa 4

Las empresas que necesitan respaldo de información (BACKUP)	**$200 Anuales**
Licencias Antivirus 15 máquinas	$600 Anuales
Capacitaciones	$300
Total Presupuesto de Inversión	$1.100 Anuales

EMPRESA 5

La empresa necesita:

- Socialización de las directrices de seguridad
- Monto anual destinado a seguridad de la información
- Filtrado el ante personal no autorizado acceso

Tabla 189

Seguimiento a los controles empresa 5

Controles necesarios	Solución	Costo
Socialización de las directrices de seguridad	Capacitación	$300
Filtrado el acceso ante personal no autorizado	Lector biométrico + circuito para puertas	$500
Presupuesto corrección de fallas		$800

Tabla 190

Presupuesto Anual empresa 5

Las empresas que necesitan respaldo de información (BACKUP)	**$200 Anuales**
Licencias Antivirus 15 máquinas	$600 Anuales
Capacitaciones	$300
Total Presupuesto de Inversión	$1.100 Anuales

EMPRESA 6

La empresa cuenta con departamentos Internos y Externos que se encargue de la seguridad informática de la empresa, a más de ello cuenta con contratos hacia los empleados.

La empresa presenta ausencia de:

- Prácticas de Gestión de sistemas
- Acuerdos de confidencialidad
- Seguimiento de uso de e-mail

- Conocimiento y actualización de políticas de seguridad de información y procedimientos de seguridad de la información
- Control de logs
- Políticas de accesos a la información
- Fallos entre 1 a 10
- Controles criptográficos
- Contraseñas interactivas
- Directrices a la seguridad de la información
- Incidentes (Ataques Ddos (A sistema de computadoras o red), Espionaje (obtener de manera ilícita, información)
- Fugas sobre información enviada o recibida por mensajería electrónica
- Políticas de pantallas limpias, escritorios limpios

Controles necesarios para la empresa:

Políticas

Mantener la confidencialidad con todos los procesos internos de la empresa desde el punto de inicio de labores hasta el cese del mismo.

- Los empleados deberán firmar un acuerdo de confidencialidad/contrato de trabajo antes de iniciar sus labores para así se evitará la divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, precios, manuales.

Uso adecuado de correo electrónico

- Solo el personal autorizado por el jefe directo pueden hacer uso del sistema de correo electrónico empresarial.

Sistema de gestión de contraseñas interactivas y de calidad para asegurar el control de acceso a la información sensible.

- Las contraseñas dadas a los colaboradores de la Industrias deben ser únicas e intransferibles.
- Se deben utilizar al menos 8 caracteres para crear la clave, teniendo en cuenta que contengan letras mayúsculas y números.

Protección de la información en cualquiera de sus formas que pueden estar contenidas en escritorios, puestos de trabajo, computadores, medios magnéticos, documentos en papel y en general cualquier tipo de información que utilicen los colaboradores de la empresa.

- Escritorios Limpios: Cuando un trabajador abandona el lugar de trabajo, debe bloquear su ordenador y guardar en lugares seguros sus documentos, medio magnético u óptico removible que contenga información confidencial.
- Pantallas limpias: Los colaboradores de la empresa deben tener los ordenadores libres de notas tanto en papeles como el protector de pantallas.

Tabla 191

Seguimiento a los controles empresa 6

Controles necesarios	Solución	Costo
Procedimientos de seguridad de la información	Capacitación	$400
Fugas sobre información	Capacitaciones	$ 300
Control de logs	Servidor de dominios	$2.500
	Configuraciones de dominios	$1.500
Políticas de accesos a la información	Solución Uno	Montos
	Equipo servidor/Configuración proxy ACL	$2.000/$700
Controles criptográficos	Instalación y Configuraciones	$235
Directrices a la seguridad de la información	Capacitación	$300
Presupuesto corrección de fallas		**$7.935**

EMPRESA 7

La empresa cuenta con, Auditoría Interna, Externa, Clasificación de la Información, Plan de continuidad del negocio, Acuerdos y/o contratos (El Acuerdo de Confidencialidad, Acuerdo de Nivel de Servicios), además

mantiene una unidad de seguridad de información Externa, también cuenta con contratos y acuerdos de confidencialidad con los empleados.

La empresa presenta ausencia de:

- Seguimiento de e-mail
- Acceso de al código fuente el personal de gerencia
- Identificación por parte del responsable del equipo antes de aceptar el servicio de mantenimiento
- Requerido su autenticación para el ingreso

Controles necesarios para la empresa:

Políticas:

Uso adecuado de correo electrónico

- Solo el personal autorizado por el jefe directo pueden hacer uso del sistema de correo electrónico empresarial.

Vigilancia y resguardo a las instalaciones de la industria, a través de un registro de entrada y salida del personal que labora en la empresa, sus clientes, proveedores y visitantes.

- Para el ingreso a la industria todas las personas deberán presentar su identificación.

Personal autorizado al código fuente, resguardo y protección de la información a las aplicaciones de software

Tabla 192

Seguimiento a los controles empresa 7

Controles necesarios	Solución	Costo
Controles criptográficos	Instalación y Configuraciones	$235
Identificación del personal de mantenimiento	Capacitación	$300
Sitio de recepción que filtre la entrada a la empresas	Lector biométrico	$ 400
Controles criptográficos	Instalación y Configuraciones	$235
Presupuesto corrección de fallas		$1.170

EMPRESA 8

La empresa cuenta con las prácticas de gestión: Políticas de seguridad, Auditoría Interna, Externa, Clasificación de la Información, Plan de continuidad del negocio, Plan de respuesta a incidentes, a más de ello cuenta con una unidad de externa e Interna de seguridad de la información, además cuenta con contratos y acuerdos de confidencialidad.

La empresa presenta ausencia de:

- Controles criptográficos
- Virus/ Caballos de Troya (Software malicioso)
- Identificación por parte del responsable del equipo antes de aceptar el servicio de mantenimiento

Tabla 193

Seguimiento a los controles empresa 8

Controles necesarios	Solución	Costo
Controles criptográficos	Instalación y Configuraciones	$235
Identificación del personal de mantenimiento	Capacitación	$300
Control de Virus	Licencias Antivirus 15 máquinas	$600 Anuales
Presupuesto corrección de fallas		$1.135

EMPRESA 9

La empresa ha invertido unos $1000 anuales, cuenta con políticas de seguridad, la seguridad de la información es tercearizada, sus empleados firman tanto el contrato con el acuerdo antes de iniciar sus labores.

Mediante los resultados de la encuesta se obtuvo que la empresa no cuenta con:

- Políticas de control de acceso a la información
- Socialización de las directrices de seguridad
- Monto anual destinado a seguridad de la información

Necesitan:

- Charla de sociabilización sobre las directrices de seguridad
- Políticas de control de acceso a la información (por equipo o software)

Tabla 194

Seguimiento a los controles empresa 9

Controles necesarios	Solución	Costo
Políticas de control de acceso a la información	Solución Uno	Montos
	Equipo servidor/Configuración proxy ACL	$2000/$700
	Segunda solución	
	Equipo Firewall/Licencia	$2000/$5000 anuales
	Nota: Pequeñas no tienen muchos usuarios Solución uno.	
Socialización de las directrices de seguridad	Capacitación un día	$300
Presupuesto corrección de fallas		$3.000

Tabla 195 Presupuesto en Herramientas empresa 9

Las empresas que necesitan respaldo de información (BACKUP)	**$200 Anuales**
Licencias Antivirus 15 máquinas	$600 Anuales
Capacitaciones	$300
Total Presupuesto de Inversión	$1.100 Anuales

EMPRESA 10

La empresa ha invertido aproximadamente $3.000 anuales en herramientas de seguridad y protección de datos, cuenta con clasificación de la información, acuerdos y/o contratos (acuerdos de confidencialidad, acuerdos de nivel de servicios), además mantiene un departamento interno que se encargue de la seguridad informática de la empresa.

Presenta ausencia de:

- Políticas de control de acceso a la información
- Procedimientos de re-autenticación
- Administración y control de las redes
- Presenta fallos de seguridad entre 1 a 10
- Controles criptográficos

Necesitan:

- Charla de sociabilización sobre las directrices de seguridad
- Políticas de control de acceso a la información (por equipo o software)

Tabla 196

Controles necesarios para la empresa 10

Controles necesarios	Solución	Costo
Políticas de control de acceso a la información	Solución Uno	
	Equipo servidor/Configuración proxy ACL	$2.000/$700
Re autenticación	Configuraciones: Procedimientos de Re autenticación	$150
Administración y control de las redes	Un rack	$400
	Router	$500
	Switch	$150
	Pach Panel	$70
	Configuraciones	$300
Controles criptográficos	Instalación y Configuraciones	$235
Presupuesto corrección de fallas		$4.505

EMPRESA 11

La empresa conserva con Auditoría Interna, Externa, Políticas de seguridad, también cuenta con un departamento que se encargue de la seguridad informática de la empresa, y mantiene contratos y acuerdos de confidencialidad con los empleados.

La empresa presenta ausencia de:

- Seguimiento de uso de e-mail
- Conocimiento y actualización de políticas de seguridad de información y procedimientos de seguridad de la información

- Procesos de re autenticación, fallos entre 1 a 10
- Controles criptográficos, ingresos al sistema de otras áreas
- Phishing (Suplantación de identidad)
- Fugas sobre información enviada o recibida por mensajería electrónica
- Políticas de pantallas limpias, escritorios limpios
- Requerido su autenticación para el ingreso

Controles necesarios para la empresa:

Políticas:

Uso adecuado de correo electrónico

- Solo el personal autorizado por el jefe directo pueden hacer uso del sistema de correo electrónico empresarial.

Protección de la información en cualquiera de sus formas que pueden estar contenidas en escritorios, puestos de trabajo, computadores, medios magnéticos, documentos en papel y en general cualquier tipo de información que utilicen los colaboradores de la empresa.

- Escritorios Limpios: Cuando un trabajador abandona el lugar de trabajo, debe bloquear su ordenador y guardar en lugares seguros sus documentos, medio magnético u óptico removible que contenga información confidencial.
- Pantallas limpias: Los colaboradores de la empresa deben tener los ordenadores libres de notas tanto en papeles como el protector de pantallas.

Tabla 197

Seguimiento a los controles empresa 11

Controles necesarios	Solución	Costo
Procedimientos de seguridad de la información	Capacitación	$400

CONTINÚA

Control de incidente	**Capacitaciones**	**$200**
Capacitación sobre fugas de información	Capacitaciones	$100
Procesos de re autenticación	Configuraciones: Procedimientos de Re autenticación	$150
Controles criptográficos	Instalación y Configuraciones	$235
Fugas sobre información	Capacitaciones	$ 300
Ingresos al sistema de otras áreas	Un rack	$400
	Router	$500
	Switch	$150
	Pach Panel	$70
	Opcional Cableado estructurado	$70*maquina
	Instalación y Configuraciones	$1.000
Presupuesto corrección de fallas		**$3.575**

EMPRESA 12

La empresa mantiene Políticas de seguridad, Auditoría Interna, Externa, Clasificación de la Información, con un departamento de seguridad de la información interna, a más de ello cuenta con contratos hacia los empleados

La empresa presenta ausencia de:

- Acuerdos de confidencialidad
- Seguimientos de e-mail
- Conocimiento y actualización de políticas de seguridad de información y procedimientos de seguridad de la información
- Políticas de accesos a la información
- Administración y control de las redes
- Controles criptográficos
- Virus/ Caballos de Troya (Software malicioso), lista negra
- Identificación de responsables de mantenimiento
- Montos de inversión

Controles necesarios para la empresa:

Políticas

Mantener la confidencialidad con todos los procesos internos de la empresa desde el punto de inicio de labores hasta el cese del mismo.

- Los empleados deberán firmar un acuerdo de confidencialidad/contrato de trabajo antes de iniciar sus labores para así se evitará la divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, precios, manuales.

Uso adecuado de correo electrónico

- Solo el personal autorizado por el jefe directo pueden hacer uso del sistema de correo electrónico empresarial.

Sistema de gestión de contraseñas interactivas y de calidad para asegurar el control de acceso a la información sensible.

- Las contraseñas dadas a los colaboradores de la Industrias deben ser únicas e intransferibles.
- Se deben utilizar al menos 8 caracteres para crear la clave, teniendo en cuenta que contengan letras mayúsculas y números.

Tabla 198

Seguimiento a los controles empresa 12

Controles necesarios	Solución	Costo
Procedimientos de seguridad de la información	Capacitación	$400
Políticas de accesos a la información	Solución Uno	
	Equipo servidor/Configuración proxy ACL	$2.000/$700
Administración y control de las redes	Un rack	$400
	Router	$500
	Switch	$150
	Pach Panel	$70
	Configuraciones	$300
Controles criptográficos	Instalación y Configuraciones	$235
Presupuesto corrección de fallas		$4.755

Tabla 199

Presupuesto en herramientas empresa 12

Las empresas que necesitan respaldo de información (BACKUP)	**$200 Anuales**
Licencias Antivirus 15 máquinas	$600 Anuales
Capacitaciones	$300
Total Presupuesto de Inversión	$1.100 Anuales

EMPRESA 13

La empresa presenta ausencia de:

- Seguimientos de e-mail
- Resguardo al cuarto de archivos
- Control de logs
- Personal de gerencia (acceso al código fuente)
- Sitio de recepción que filtre la entrada a la empresas
- Administración y control de las redes
- Las redes se encuentran separadas en función de los servicios, usuarios y sistemas de información
- Fallos entre 1 a 10 p.23
- Contraseñas interactivas
- Virus/ Caballos de Troya (Software malicioso)
- Identificación de responsables de mantenimiento
- Políticas de pantallas limpias, escritorios limpios

Controles necesarios para la empresa:

Políticas:

Uso adecuado de correo electrónico

- Solo el personal autorizado por el jefe directo pueden hacer uso del sistema de correo electrónico empresarial.

Se debe tener acceso controlado y restringido a los cuartos de servidores principales, de archivo y al área de producción debido a que son sitios en el cual resguarda información de la empresa.

- Tener a una persona encargada del cuarto de archivos para el manejo del mismo, su respectivo control, llaves de acceso, registro de los documentos almacenados.

Sistema de gestión de contraseñas interactivas y de calidad para asegurar el control de acceso a la información sensible.

- Las contraseñas dadas a los colaboradores de la Industrias deben ser únicas e intransferibles.
- Se deben utilizar al menos 8 caracteres para crear la clave, teniendo en cuenta que contengan letras mayúsculas y números.

Protección de la información en cualquiera de sus formas que pueden estar contenidas en escritorios, puestos de trabajo, computadores, medios magnéticos, documentos en papel y en general cualquier tipo de información que utilicen los colaboradores de la empresa.

- Escritorios Limpios: Cuando un trabajador abandona el lugar de trabajo, debe bloquear su ordenador y guardar en lugares seguros sus documentos, medio magnético u óptico removible que contenga información confidencial.
- Pantallas limpias: Los colaboradores de la empresa deben tener los ordenadores libres de notas tanto en papeles como el protector de pantallas.

Personal autorizado al código fuente, resguardo y protección de la información a las aplicaciones de software

- Programadores
- Jefes de sistemas

Tabla 200

Seguimiento a los controles empresa 13

Controles necesarios	Solución	Costo
Control de logs	Servidor	$2.500
	Configuraciones de dominios	$1.500
Sitio de recepción que filtre la entrada a la empresas	Lector biométrico	$ 400
Redes se encuentran separadas	Un rack	$400
	Router	$500
	Switch	$150
	Pach Panel	$70
	Opcional Cableado estructurado	$70*maquina
	Instalación y Configuraciones	$1.000
Control de Virus	Licencias Antivirus 15 máquinas	$600 Anuales
Identificación del personal de mantenimiento	Capacitación	$300
Presupuesto corrección de fallas		$7.390

EMPRESA 14

La empresa cuenta con Políticas de seguridad, Clasificación de la Información, Acuerdos y/o contratos (El Acuerdo de Confidencialidad, Acuerdo de Nivel de Servicios), además la empresa cuenta con una unidad de seguridad de información externa, mantiene contratos y acuerdos de confidencialidad con los empleados.

La empresa presenta ausencia de:

- Seguimiento de e-mail
- Conocimiento y actualización de políticas de seguridad de información y procedimientos de seguridad de la información
- Resguardo al cuarto de archivos
- Políticas de accesos a la información
- Procedimientos de re-autenticación
- Actualización de software

- Salida de equipos de procesamiento de la información
- Fallos entre 1 a 10
- Controles criptográficos
- Contraseñas interactivas
- Ingresos al sistema de otras áreas
- Directrices a la seguridad de la información
- Virus/ Caballos de Troya (Software malicioso)
- Políticas de pantallas limpias, escritorios limpios

Controles necesarios para la empresa:

Políticas

Uso adecuado de correo electrónico

- Solo el personal autorizado por el jefe directo pueden hacer uso del sistema de correo electrónico empresarial.

Se debe tener acceso controlado y restringido a los cuartos de servidores principales, de archivo y al área de producción debido a que son sitios en el cual resguarda información de la empresa.

- Tener a una persona encargada del cuarto de archivos para el manejo del mismo, su respectivo control, llaves de acceso, registro de los documentos almacenados.

Sistema de gestión de contraseñas interactivas y de calidad para asegurar el control de acceso a la información sensible.

- Las contraseñas dadas a los colaboradores de la Industrias deben ser únicas e intransferibles.
- Se deben utilizar al menos 8 caracteres para crear la clave, teniendo en cuenta que contengan letras mayúsculas y números.

Protección de la información en cualquiera de sus formas que pueden estar contenidas en escritorios, puestos de trabajo, computadores, medios magnéticos, documentos en papel y en general cualquier tipo de información que utilicen los colaboradores de la empresa.

- Escritorios Limpios: Cuando un trabajador abandona el lugar de trabajo, debe bloquear su ordenador y guardar en lugares seguros sus documentos, medio magnético u óptico removible que contenga información confidencial.
- Pantallas limpias: Los colaboradores de la empresa deben tener los ordenadores libres de notas tanto en papeles como el protector de pantallas.

Los activos tangibles no deben tener autorizaciones de salida de las industrias.

Tabla 201

Seguimiento a los controles empresa 14

Controles necesarios	Solución	Costo
Procedimientos de seguridad de la información	Capacitación	$400
Políticas de accesos a la información	Solución Uno	
	Equipo servidor/Configuración proxy ACL	$2.000/$700
Procedimientos de re-autenticación	Configuraciones: Procedimientos de Re autenticación	$150
Actualización de software	Configuraciones: Deshabilitación de configuraciones automáticas y un seguimiento de actualizaciones	$150
Controles criptográficos	Instalación y Configuraciones	$235
Control de Virus	Licencias Antivirus 15 máquinas	$600 Anuales
Ingresos al sistema de otras áreas	Un rack	$400
	Router	$500
	Switch	$150
	Pach Panel	$70
	Opcional Cableado estructurado	$70*maquina
	Instalación y Configuraciones	$1000
Directrices a la seguridad de la información	Capacitación	$300
Presupuesto corrección de fallas		**$6.725**

EMPRESA 15

La empresa cuenta con Políticas de seguridad, Auditoría Interna, Externa, Clasificación de la Información, además la empresa cuenta con una unidad de seguridad de información Interna, también la empresa mantiene contratos y acuerdos de confidencialidad con los empleados.

La empresa presenta ausencia de:

- Seguimiento de e-mail
- Conocimiento y actualización de políticas de seguridad de información y procedimientos de seguridad de la información
- Políticas de accesos a la información
- Administración y control de las redes
- Controles criptográficos
- Ingresos al sistema de otras áreas
- Directrices a la seguridad de la información
- Virus/ Caballos de Troya (Software malicioso)
- Identificación por parte del responsable del equipo antes de aceptar el servicio de mantenimiento
- Montos de inversión

Controles necesarios para la empresa:

Políticas:

Uso adecuado de correo electrónico

- Solo el personal autorizado por el jefe directo pueden hacer uso del sistema de correo electrónico empresarial.

Tabla 202

Seguimiento a los controles empresa 15

Controles necesarios	Solución	Costo
Procedimientos de seguridad de la información	Capacitación	$400

CONTINÚA

Políticas de accesos a la información	**Solución Uno**	**Montos**
	Equipo servidor/Configuración proxy ACL	$2.000/$700
	Segunda solución	
	Equipo Firewall/Licencia	$2.000/$5.000 anuales
	Nota: Pequeñas no tienen muchos usuarios Solución uno.	
Controles criptográficos	Instalación y Configuraciones	$235
Administración y control de las redes	Un rack	$400
	Router	$500
	Switch	$150
	Pach Panel	$70
	Opcional Cableado estructurado	$70*maquina
	Instalación y Configuraciones	$235
Directrices a la seguridad de la información	Capacitación	$300
Identificación del personal de mantenimiento	Capacitación	$300
Presupuesto corrección de fallas		$5.290

Tabla 203

Presupuesto en herramientas empresa 15

Las empresas que necesitan respaldo de información (BACKUP)	**$200 Anuales**
Licencias Antivirus 15 máquinas	$600 Anuales
Capacitaciones	$300
Total Presupuesto de Inversión	$1.100 Anuales

EMPRESA 16

La empresa cuenta Políticas de seguridad, Plan de respuesta a incidentes, Acuerdos y/o contratos (El Acuerdo de Confidencialidad, Acuerdo de Nivel de Servicios)

La empresa presenta ausencia de:

- Contrato de trabajo
- Seguimiento de uso de e-mail

- Resguardo al cuarto de archivos
- Procesos de re autenticación
- Sitio de recepción que filtre la entrada a la empresa
- Protección donde se ubican los recursos informáticos
- Fallos entre 1 a 10
- Controles criptográficos
- Filtro de ingreso en el área de producción
- Virus/ Caballos de Troya (Software malicioso), Ataques Ddos (A sistema de computadoras o red), Ransomware (Restringe el acceso a su sistema y exige un pago de rescate), Pharming (fraude en línea)
- Políticas de pantallas limpias, escritorios limpios

Controles necesarios para la empresa:

Políticas

Mantener la confidencialidad con todos los procesos internos de la empresa desde el punto de inicio de labores hasta el cese del mismo.

- Los empleados deberán firmar un acuerdo de confidencialidad/contrato de trabajo antes de iniciar sus labores para así se evitará la divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, precios, manuales.

Uso adecuado de correo electrónico

- Solo el personal autorizado por el jefe directo pueden hacer uso del sistema de correo electrónico empresarial

Se debe tener acceso controlado y restringido a los cuartos de servidores principales, de archivo y al área de producción debido a que son sitios en el cual resguarda información de la empresa.

- Tener a una persona encargada del cuarto de archivos para el manejo del mismo, su respectivo control, llaves de acceso, registro de los documentos almacenados.

Protección de la información en cualquiera de sus formas que pueden estar contenidas en escritorios, puestos de trabajo, computadores, medios

magnéticos, documentos en papel y en general cualquier tipo de información que utilicen los colaboradores de la empresa.

- Escritorios Limpios: Cuando un trabajador abandona el lugar de trabajo, debe bloquear su ordenador y guardar en lugares seguros sus documentos, medio magnético u óptico removible que contenga información confidencial.
- Pantallas limpias: Los colaboradores de la empresa deben tener los ordenadores libres de notas tanto en papeles como el protector de pantallas.

Tabla 204

Seguimiento a los controles empresa 16

Controles necesarios	Solución	Costo
Procesos de re autenticación	Configuraciones: Procedimientos de Re autenticación	$150
Filtre la entrada a la empresa	Lector biométrico	$ 400
Protección donde se ubican los recursos Informáticos	Capacitación	$300
Controles criptográficos	Instalación y Configuraciones	$235
Filtro de ingreso en el área de producción	Lector biométrico + circuito para puertas	$500
Políticas de pantallas limpias, escritorios limpios	Capacitación	$200
Presupuesto corrección de fallas		$1.785

Tabla 205 Presupuesto en herramientas empresa 16

Las empresas que necesitan respaldo de información (BACKUP)	**$200 Anuales**
Licencias Antivirus 15 máquinas	$600 Anuales
Capacitaciones	$300
Total Presupuesto de Inversión	$1.100 Anuales

EMPRESA 17

La empresa ha invertido unos $1.000 anuales, cuenta con políticas de seguridad, la seguridad de la información es tercearizada, sus empleados firman tanto el contrato con el acuerdo antes de iniciar sus labores, a más de ello poseen auditorías internas y externas.

Mediante los resultados de la encuesta se obtuvo que la empresa no cuenta con:

- Políticas de seguridad de información
- Procedimientos para la seguridad de la información.
- Políticas de control de acceso a la información
- Redes separadas en función de los servicios, usuarios y sistemas de información.
- Socialización de las directrices de seguridad
- Monto anual destinado a seguridad de la información

Necesitan:

- Charla de sociabilización sobre las directrices de seguridad
- Políticas de control de acceso a la información (por equipo o software)

Tabla 206 Controles necesarios para la empresa 17

Controles necesarios	Solución	Costo
Políticas de seguridad de información	Capacitación	$600
Procedimientos para la seguridad de la información.	Solución Uno	Montos
	Equipo servidor/Configuración proxy ACL	$2.000/$700
	Segunda solución	
	Equipo Firewall/Licencia	$2.000/$5.000 anuales
Redes separadas en función de los servicios, usuarios y sistemas de información.	Un rack	$400
	Router	$500
	Swuich	$150
	Pach Panel	$70
	Opcional Cableado estructurado	$70*maquina
	Instalación y Configuraciones	$235
Filtro de entradas a la empresa	Lector biométrico	$ 400
Presupuesto corrección de fallas		$4.525

Tabla 207 Presupuesto Anual empresa 17

Las empresas que necesitan respaldo de información (BACKUP)	**$200 Anuales**
Licencias Antivirus 15 máquinas	$600 Anuales
Capacitaciones	$300
Total Presupuesto de Inversión	$1.100 Anuales

EMPRESA 18

Mediante los resultados de la encuesta se obtuvo que la empresa no cuenta con**:**

- Prácticas de gestión de sistemas de información
- Monto anual destinado a seguridad de la información
- Políticas de control de acceso a la información
- Socialización de las directrices de seguridad
- Monto anual destinado a seguridad de la información
- Seguimiento de uso de e –mails

Controles necesarios para la empresa:

Políticas

Mantener la confidencialidad con todos los procesos internos de la empresa desde el punto de inicio de labores hasta el cese del mismo.

- Los empleados deberán firmar un acuerdo de confidencialidad/contrato de trabajo antes de iniciar sus labores para así se evitará la divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, precios, manuales.

Uso y manejo adecuado de los servicios de correo electrónico e internet.

- Solo el personal autorizado por el jefe directo pueden hacer uso del sistema de correo electrónico empresarial.

Se debe tener acceso controlado y restringido a los cuartos de servidores principales, de archivo y al área de producción debido a que son sitios en el cual resguarda información de la empresa.

- Tener a una persona encargada del cuarto de archivos para el manejo del mismo, su respectivo control, llaves de acceso, registro de los documentos almacenados.

Vigilancia y resguardo a las instalaciones de la industria, a través de un registro de entrada y salida del personal que labora en la empresa, sus clientes, proveedores y visitantes.

- Para el ingreso a la industria todas las personas deberán presentar su identificación.

Sistema de gestión de contraseñas interactivas y de calidad para asegurar el control de acceso a la información sensible.

- Las contraseñas dadas a los colaboradores de la Industrias deben ser únicas e intransferibles.
- Se deben utilizar al menos 8 caracteres para crear la clave, teniendo en cuenta que contengan letras mayúsculas y números.

Protección de la información en cualquiera de sus formas que pueden estar contenidas en escritorios, puestos de trabajo, computadores, medios magnéticos, documentos en papel y en general cualquier tipo de información que utilicen los colaboradores de la empresa.

- Escritorios Limpios: Cuando un trabajador abandona el lugar de trabajo, debe bloquear su ordenador y guardar en lugares seguros sus documentos, medio magnético u óptico removible que contenga información confidencial.
- Pantallas limpias: Los colaboradores de la empresa deben tener los ordenadores libres de notas tanto en papeles como el protector de pantallas

Tabla 208

Seguimiento a los controles empresa 18

Controles necesarios	Solución	Costo
Prácticas de gestión de sistemas de información	Capacitación	$400
Re autenticación	Configuraciones: Procedimientos de Re autenticación	$150
Actualización de software	Configuraciones: Deshabilitación de configuraciones automáticas y un seguimiento de actualizaciones	$150
Control y separación de redes	Un rack	$400
	Router	$500
	Swich	$150
	Pach Panel	$70
	Opcional Cableado estructurado	$70*maquina
	Instalación y Configuraciones	$235
Directrices de seguridad de la información	Capacitación	$300
Acceso al área de producción	Lector biométrico + circuito para puertas	$500
Acceso a la empresa	Lector biométrico	$ 400
Autenticación al ingreso al internet	Solución Uno	
	Equipo servidor/Configuración proxy ACL	$2.000/$700
Presupuesto corrección de fallas		**$6.025**

EMPRESA 19

La empresa cuenta con, Políticas de seguridad, Auditoría Interna, Externa, Clasificación de la Información, Acuerdos y/o contratos (El Acuerdo de Confidencialidad, Acuerdo de Nivel de Servicios), a más de ello cuenta con una unidad de externa de seguridad de la información.

La empresa presenta ausencia de:

- Acceso a la información de la empresa
- Accesos al cuarto de archivos
- Políticas de control de accesos a la información
- Acceso de al código fuente el personal de gerencia
- Actualización de los software

- Fallos entre 1 a 10
- Controles criptográficos
- Contraseñas interactivas y de calidad
- Socialización de las directrices de seguridad
- Fuga electrónica de datos de los sistemas internos
- Fugas sobre información enviada o recibida por mensajería electrónica
- Identificación por parte del responsable del equipo antes de aceptar el servicio de mantenimiento
- Conocimiento de las políticas de seguridad de la información de la empresa

Implementaciones:

Se debe tener acceso controlado y restringido a los cuartos de servidores principales, de archivo y al área de producción debido a que son sitios en el cual resguarda información de la empresa.

- Tener a una persona encargada del cuarto de archivos para el manejo del mismo, su respectivo control, llaves de acceso, registro de los documentos almacenados.

Sistema de gestión de contraseñas interactivas y de calidad para asegurar el control de acceso a la información sensible.

- Las contraseñas dadas a los colaboradores de la Industrias deben ser únicas e intransferibles.
- Se deben utilizar al menos 8 caracteres para crear la clave, teniendo en cuenta que contengan letras mayúsculas y números.

Personal autorizado al código fuente, resguardo y protección de la información a las aplicaciones de software

- Programadores
- Jefes de sistemas

Tabla 209

Seguimiento a los controles empresa 19

Controles necesarios	Solución	Costo
Políticas de control de acceso a la información	Solución Uno	Montos
	Equipo servidor/Configuración proxy ACL	$2.000/$700
Actualización de software	Configuraciones: Deshabilitación de configuraciones automáticas y un seguimiento de actualizaciones	$150
Controles Criptográficos	Instalación y Configuraciones	$1.000
Socialización de las directrices de seguridad	Capacitación	$300
Presupuesto corrección de fallas		$4.525

5.2. Beneficio Marginal

Cálculo del ROSI (Retorno de la Inversión en Seguridad Informática)

- Fórmula

ROSI= (Exposición del Riesgo, % Riesgo mitigado) – Costo de la Solución

- Datos:
  - Costo promedio de los incidentes (P24)
    - $12500
  - % Riesgo mitigado
    - 90%
  - Costo promedio de los costos de inversión
    - $4100

ROSI= (12500*90%)-4100

ROSI= 11.250-4100

ROSI= 7.150

Relación= 7.150/4100

Relación= 1,74

Relación= 174%

Análisis

En la presente ecuación se trabajó bajo los parámetros del ROI (Retorno de la Inversión) ajustándose a la ecuación del ROSI donde se constata incidentes ocurridos en la empresa la cual se obtuvo mediante encuestas realizadas a las empresas del sector Industrial en la provincia de Cotopaxi Reguladas por la Superintendencia de Compañías, se obtuvo un promedio de 10 incidentes de lo cual se desea mitigar al menos 9 incidentes de los 10, además se consiguió el costo de los incidentes con un promedio del $12.500, se tomó un promedio de los costos calculados que deberían invertir las Industrias siendo este de $4.100, dándonos un retorno de la inversión en seguridad de la información de 174%, es decir que al invertir $4.100 se logra una disminución del nivel del riesgo de $7.150, En otras palabras por cada dólar que se invierte en seguridad se logrará una disminución del riesgo de 1,74 dólares.

CAPÍTULO VI

5. PROPUESTA DE INVESTIGACIÓN

5.1. Objetivos de las Propuesta

Sugerir Herramientas y Políticas de Seguridad de Información y Protección de datos, que las empresas del Sector Industrial puedan implementar en base a las debilidades que se encontraron en cada una de ellas.

5.2. Fundamentación de la Propuesta

1. Políticas de seguridad

Según Pritesh (2012) para realizar el Documento de Políticas se debe considerar los objetivos de la organización, las estrategias planteadas y los distintos procesos adoptados conjuntamente con los requisitos de leyes obligatorias de cumplimiento y políticas procedentes de niveles superiores.

Tabla 210

Políticas de Seguridad

Políticas para la seguridad de la información	Se establecen políticas aprobadas por la dirección y se da a conocer a todos los empleados.
Revisión de las políticas para la seguridad de la información	Las políticas se planifican y revisan frecuentemente garantizando así la efectividad.

Fuente: (ISO 27002, 2013)

2. Aspectos organizativos de la seguridad de la información

Tabla 211

Aspectos organizativos de la seguridad de la información

Segregación de tareas:	Distribuir de manera adecuada cada una de las responsabilidades y tareas en el Departamento.
Seguridad de la información en la gestión de proyectos	Resguardar la información de los proyectos a desarrollarse en las empresas.
Teletrabajo	Una política adecuada para la utilización y autorización del trabajo llevado a lugares diferente de las instalaciones centrales de la empresa.

Fuente: (ISO 27002, 2013)

3. Seguridad ligada a los recursos humanos

Tabla 212

Seguridad ligada a los recursos humanos

Investigación de antecedentes	Verificar antecedentes de candidatos al empleo en concordancia con las leyes y ética.
Términos y condiciones de contratación	Se establecen obligaciones en la organización y los empleados deben aceptar y firmar las condiciones.
Concienciación, educación y capacitación en SI	Los empleados de la organización deben recibir conocimientos y actualizaciones que sean relevantes para sus funciones.

Fuente: (ISO 27002, 2013)

4. Gestión de activos

Tabla 213

Gestión de activos

Propiedad de los activos	Tener enumerados y registro cada de uno de los activos que posee la empresa a más de ello debe estar controlado por un departamento de la empresa.
Devolución de activos	Al abandonar el empleado un puesto de trabajo debe dejar en la empresa todos los activos, cuentas, contraseñas que la empresa le otorgó.
Etiquetado y manipulado de la información	Llevar un control de quienes tiene acceso y autorización de llevar la información privilegiada de la empresa.
Manipulación de activos	De acuerdo con la información especificada a cada empleado se le otorga un activo la cual se le enseña al correcto manejo del mismo.
Soportes físicos en tránsito	Al ser trasladado algún medio que contenga información exclusiva de la empresa se deberá tener cuidado al momento de que salga de la instalación de trabajo por medio de alguna herramienta de seguridad.

Fuente: (ISO 27002, 2013)

5. Control de accesos

Tabla 214

Control de accesos

Política de control de accesos	Se elabora en base a las necesidades de seguridad.
Control de acceso a las redes y servicios asociados	Se debería proveer a los usuarios que han sido expresamente autorizados a utilizarlos.
Gestión de altas/bajas en el registro de usuarios	Registro inicial de nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información.
Gestión de los derechos de acceso asignados a usuarios	Aprovisionamiento de accesos para asignar o revocar derechos de acceso a todos los usuarios para todos los sistemas.
Gestión de los derechos de acceso con privilegios especiales	Restringir los derechos de acceso con privilegios
Gestión de información confidencial de autenticación de usuarios	Control mediante procesos de Gestión para la Información confidencial
Retirada o adaptación de los derechos de acceso	Retirar los derechos de acceso para los empleados y a las instalaciones del procesamiento de información al finalizar su contrato o empleo.
Uso de información confidencial para la autenticación	Implantar policías para mantener mesas de escritorios y monitores libres de cualquier información para reducir el riesgo de acceso no autorizado.
Restricción del acceso a la información	Restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones
Procedimientos seguros de inicio de sesión	Si la política de control de acceso lo establece se controla el acceso a los sistemas mediante un proceso de log-on
Gestión de contraseñas de usuario	Asegurar contraseñas de calidad a través de sistemas de Gestión de contraseñas
Control de acceso al código fuente de los programas	Restringir el acceso al código fuente de las aplicaciones de software instaladas.

Fuente: (ISO 27002, 2013)

6. Cifrado

Tabla 215

Cifrado

Política de uso de los controles criptográficos	La empresa deberá implementar una política donde vigile la protección de los datos mediante controles criptográficos.
Gestión de claves	Dentro de las políticas de seguridad de la información deberá estar el periodo de una clave para el acceso a la información.

Fuente: (ISO 27002, 2013)

7. Seguridad Física y ambiental

Tabla 216

Seguridad Física y ambiental

Perímetro de seguridad física	Utilizar perímetros de seguridad para la protección de las áreas que contienen información sensible o crítica.
Controles físicos de entrada	Establecer controles de entrada adecuados garantizando que solo el personal autorizado dispone de permisos de acceso
Seguridad de oficinas, despachos y recursos	Aplicar un sistema de seguridad física a cada una de los departamentos e instalaciones.
Áreas de acceso público, carga y descarga	Un control en áreas de carga y descarga evitando así el ingreso de personas no autorizadas.
Seguridad del cableado	Se deben proteger contra la intercepción y transferencia los cables electrónicos que transportan datos y apoyan a los servicios de información.
Mantenimiento de los equipos	Un adecuado mantenimiento de los Equipos
Salida de activos fuera de las dependencias de la empresa	Sin autorización la información, equipos y software de la empresa no pueden ser movidos de su sitio.
Reutilización o retirada segura de dispositivos de almacenamiento	Comprobar que los equipos que tengan medios de almacenamiento con datos sensibles y software con licencias se hayan extraído de manera segura antes de eliminarlos o reutilizarlos.
Equipo informático de usuario desatendido	Los equipos que no se utilizan se encuentren protegidos de manera adecuada.
Política de puesto de trabajo despejado y bloqueo de pantalla	Esta política permitirá la documentación en papel y para medios de almacenamiento extraíbles, además una política de monitores que permitirán la instalación de procesamiento de información.

Fuente: (ISO 27002, 2013)

8. Seguridad en la operativa

Tabla 217

Seguridad en la operativa

Controles contra el código malicioso	Tener controles de seguridad contra afectaciones de malware.
Copias de seguridad de la información	Mantener la información en algún sistema de confianza como respaldo de todos los datos de empresa.
Protección de los registros de información	Resguardar la información contra ataques y malversación de los registros de la empresa.
Sincronización de relojes	Tener un control y registro de los horarios de las actividades mediante la sincronización de los relojes.
Instalación del software en sistemas en producción	Guías para el control y aplicación de software.
Restricciones en la instalación de software	Mantener normas de seguridad y de quienes pueden acceder a las instalaciones o áreas restringidas.

Fuente: (ISO 27002, 2013)

9. Seguridad en las telecomunicaciones

Tabla 218

Seguridad en las telecomunicaciones

Controles de red	Control de redes para proteger la información en sistemas y aplicaciones.
Mecanismos de seguridad asociados a servicios en red	Identificar mecanismos de seguridad, lo requisitos de red de administración de todos los servicios de red.
Segregación de redes	De acuerdo a los grupos de servicios, usuarios y sistemas se deben segregar las redes.
Políticas y procedimientos de intercambio de información	Políticas de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación.
Mensajería electrónica	Proteger información referida a la mensajería electrónica.
Acuerdos de confidencialidad y secreto	Se debe identificar, documentar los requisitos para os acuerdos de confidencialidad.

Fuente: (ISO 27002, 2013)

10. Adquisiciones, Desarrollo y mantenimiento de los sistemas de información

Tabla 219

Adquisiciones, Desarrollo y mantenimiento de los sistemas

Seguridad de las comunicaciones en servicios accesibles por redes públicas	Beneficiarse de herramientas para el control de las redes públicas así evitar actividades fraudulentas, malversación de la información, modificaciones mal intencionadas en contra de la empresa.
Protección de las transacciones por redes telemáticas	Proteger con herramientas las redes telemáticas para evitar la estafa de las transacciones compartidas entre equipos de computación distantes.
Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Vigilar los sistemas operativos y probar cuando se haya realizado algún cambio.
Restricciones a los cambios en los paquetes de software	Realizar cambios en el software solo cuando sea necesario y no dejar la manipulación a terceros, tener cautela del mismo.
Uso de principios de ingeniería en protección de sistemas	Cumplir con los principios seguridad en ingeniería de sistemas manteniendo herramientas para su protección.
Pruebas de aceptación	Realizar las respectivas pruebas de funcionamiento y adaptación dentro de las áreas necesarias.

Fuente: (ISO 27002, 2013)

11. Relaciones son suministros

Tabla 220

Relaciones son suministros

Política de seguridad de la información para suministradores	Documentar adecuadamente los requisitos de seguridad de la información requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al acceso por parte de terceras personas.
Tratamiento del riesgo dentro de acuerdos de suministradores	Acordar requisitos de seguridad de los proveedores que pueden almacenar, comunicar componentes de TI
Cadena de suministro en tecnologías de la información y comunicaciones	En los acuerdos se incluyen requisitos para abordar los riesgos de seguridad de la información en relación a la cadena de suministros de los servicios y productos de TI

Fuente: (ISO 27002, 2013)

12. Gestión de incidentes en la seguridad de la información

Tabla 221

Gestión de incidentes en la seguridad de la información

Notificación de los eventos de seguridad de la información	Informar inmediatamente los incidentes ocurridos, de manera correcta y con el seguimiento respectivo.
Notificación de puntos débiles de la seguridad	Todo el personal que tenga acceso a los sistemas débiles debe tener anotaciones sobre los impactos maliciosos o cualquier eventualidad de los puntos vulnerables de los sistemas.
Valoración de eventos de seguridad de la información y toma de decisiones	Clasificar y ponderar los puntos importantes de los sistemas para mayor seguridad.
Respuesta a los incidentes de seguridad	Mitigar los casos según su importancia y su respectiva guía de documentación.
Aprendizaje de los incidentes de seguridad de la información	Reconocer los incidentes y así corregirlo o eliminarlo en un futuro.
Recopilación de evidencias	Mantener bitácoras de todos los incidentes ocurridos dentro de las empresas.

Fuente: (ISO 27002, 2013)

13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio

Tabla 222

Aspectos de seguridad de la información en la gestión de la continuidad del negocio

Planificación de la continuidad de la seguridad de la información	Se determinan requisitos de la seguridad y su gestión en situaciones de crisis
Implantación de la continuidad de la seguridad de la información	Mantener niveles necesarios de seguridad
Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Verificar regularmente los controles para poder garantizar su validez y eficacia ante situaciones adversas.
Disponibilidad de instalaciones para el procesamiento de la información	Implementar suficiente redundancia en las instalaciones de procesamiento de información cuando se demuestren arquitecturas insuficientes.

Fuente: (ISO 27002, 2013)

14. Cumplimiento

Tabla 223

Cumplimiento

Identificación de la legislación aplicable	Todo proceso y control de los sistema informáticos debe estar constando en normas, políticas, contratos, para su correcto uso.
Derechos de propiedad intelectual (DPI)	Mantener las herramientas de seguridad en informática originales para evitar el mal uso del mismo y control de los sistemas.
Protección de los registros de la organización	De acuerdo con las leyes, normas de seguridad se debe proteger todo registro de la empresa mediante el uso de herramientas apropiadas.
Protección de datos y privacidad de la información personal	Cumplir con el resguardo de los datos personales de los empleados de la empresa.
Revisión independiente de la seguridad de la información	Identificar el enfoque de las empresas así poder implementar herramientas de seguridad y cumplimiento de las actividades de la empresa.
Comprobación del cumplimiento	Inspeccionar periódicamente el cumplimiento de cada actividad con su respectivo seguimiento normativo.

Fuente: (ISO 27002, 2013)

5.2.1. Controles necesarios en cada departamento representativo de las empresas Industriales

- Departamento Administrativo

Tabla 224

Controles

Términos y condiciones de contratación
Cese o cambio de puesto de trabajo
Concienciación, educación y capacitación en SI
Perímetro de seguridad física
Propiedad de los activos

- Departamento Financiero

Tabla 225

Controles

Gestión de contraseñas de usuario
Mantenimiento de los equipos
Protección de las transacciones por redes telemáticas
Mensajería electrónica
Seguridad de oficinas, despachos y recursos

- Departamento Tecnología de la Información

Tabla 226

Controles

Política de control de accesos ACL lista de control de Acceso
Etiquetado y manipulado de la información
Control de acceso al código fuente de los programas
Procedimientos seguros de inicio de sesión
Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
Retirada o adaptación de los derechos de acceso
Gestión de los derechos de acceso asignados a usuarios
Mantenimiento de los equipos
Salida de activos fuera de las dependencias de la empresa
Controles de red
Segregación de redes
Política de uso de los controles criptográficos
Gestión de contraseñas de usuario

- Departamento de Producción

Tabla 227

Controles

Segregación de Redes
Concienciación, educación y capacitación en SI
Seguridad de oficinas, despachos y recursos

- Personal de la empresa

Tabla 228

Controles

Seguridad de la información en la gestión de proyectos
Controles de Red
Retirada o adaptación de los derechos de acceso
Política de control de accesos ACL lista de control de Acceso

CONCLUSIONES

- Las empresas que se analizó del sector industrial reguladas por la Superintendencia de Compañías mediante las encuestas realizadas presentaron, qué mayor parte de las entidades no cuentan con la certificación de la Norma ISO (International Standarization Organization) 27001:2013, de igual manera la perspectiva de Gerencia hacia el cumplimiento de la misma presenta niveles bajos en temas de Gestión en sistemas de información, a más de ello se constató que las empresas tratan de cumplir con varios controles de acuerdo a la ISO 27002:2013 misma que es una ayuda para el cumplimiento de la certificación ISO 27001:2013.
- Dentro de las empresas que se tomó como referencia para la investigación presenta un 45,5% (porcentaje tomado de las encuestas) no tienen presupuesto designado para hardware, software, soporte informático, capacitaciones del conocimiento de las políticas en seguridad informática.
- De acuerdo al estudio de campo realizado a las empresas del sector Industrial se obtuvo que el 27,3% de las industrias poseen planes de respuesta a incidentes como prácticas de sistemas de información durante los periodos 2012-2016 y el 72,7% no cuentan con estos planes.
- Según los resultados obtenidos de las preguntas dirigidas a los gerentes de las empresas del Sector Industrial se obtuvo que en el 40,9% no se da un entrenamiento apropiado del conocimiento y actualizaciones de las políticas de seguridad de información.
- De acuerdo a los resultados obtenidos del ROSI en promedio el retorno de la inversión en seguridad de la información es de 174%, es decir que al invertir $4.100 se logra una disminución del nivel del riesgo de $7.150, para una mejor comprensión las empresas del sector Industrial por cada dólar que inviertan en seguridad de la información lograrán una disminución del riesgo de 1,74 dólares.

RECOMENDACIONES

- Se recomienda a las empresas del Sector Industrial implementar un manual de políticas en seguridad información y protección de datos, basadas en los controles de la norma ISO 27002:2013, pues es uno de los parámetros para llevar a cabo la certificación ISO 27001:2013, ya que la misma es un beneficio al seguimiento y resguardo de la seguridad de la información en las empresas, así mismo es necesario que se realicen mejoras continuas en el transcurso de los años.
- Se recomienda tomar como referencia y conocimiento de los costos aproximados para implementar los controles de acuerdo a la ISO 27002:2013, la misma que ayuda en la implementación de un buen Sistema en Seguridad, con la asistencia de hardware, sistemas de software, soporte informático, llevando a cabo una inversión inicial, un seguimiento continuo, ajustes necesarios en el transcurso de tiempo, que se puedan realizar y de esta forma las empresas puedan generar mejoras continuas en la Seguridad informática.
- Se recomienda a la administración de las empresas del Sector Industrial implementar planes de respuestas a incidentes, y de este modo estar preparados ante cualquier amenaza que pueda ocurrir y altere el buen transcurso del negocio.
- A los Jefes de Sistemas de las empresas del Sector Industrial programar capacitaciones referentes a las políticas corporativas de seguridad de información para el personal, además actualice sus conocimientos sobre la gestión de los sistemas de Información.
- Se recomienda a la administración de las empresas del sector industrial realizar un análisis en cuestión de sistemas de seguridad de información y protección de datos, para que de esta manera se pueda tomar medidas apropiadas para evitar nuevas amenazas que puedan ir surgiendo en el transcurso del negocio.

REFERENCIAS BIBLIOGRÁFICAS

Superintendencia de Compañias Valores y Seguros del Ecuador. (31 de Diciembre de 2017). Recuperado el 12 de Septiembre de 2017, de www.supercias.gob.ec

Andrango, H. (2012). *Superintendencia de Compañias y Valores.* Recuperado el 2017, de Sector Societario Documentos: http://appscvs.supercias.gob.ec/consultaImagen/VisualizaDocumetos.zul?tipoDocumento=economica&expediente=62018&idDocumento=3.1.5%20%20&fecha=2012-12-31%2000:00:00.0

Areitio, J. (2008). *Seguridad de la información, redes, informática y sistemas de información.* Madrid: Paraninfo.

Areito Bertolín, J. (2008). *Seguridad de la información.* España: Paraninfo.

Arteta, P. J. (2016). *Superintendencia de Compañias y Valores.* Obtenido de Sector Societario/Documentos: http://appscvs.supercias.gob.ec/consultaImagen/VisualizaDocumetos.zul?tipoDocumento=economica&expediente=7210&idDocumento=3.1.5%20%20&fecha=2016-12-31%2016:27:38.0

Asamblea Nacional. (2 de Diciembre de 2013). *Ley de Sistema Nacional de Resgistro de Datos Públicos.* Recuperado el 10 de Septiembre de 2017, de Ley de Sistema Nacional de Resgistro de Datos Públicos: https://www.registrocivil.gob.ec/wp-content/uploads/downloads/2014/01/este-es-11-LEY-DEL-SISTEMA-NACIONAL-DE-REGISTRO-DE-DATOS-P%C3%9ABLICOS-leyes-conexas1.pdf

Asamblea Nacional. (12 de Julio de 2016). *Ley orgánica de protección de los derechos a la intimidad y privacidad sobre los datos personales.* Recuperado el 5 de Octubre de 2017, de http://www.fundamedios.org/wp-content/uploads/2016/09/proyecto-ley-de-datos.pdf

Avast. (s.f.). *Avast*. Recuperado el Julio de 2017, de Ransomware: https://www.avast.com/es-es/c-ransomware

BBC Mundo. (2017). Virus WannaCry: ¿corre peligro mi computadora? *BBC MUNDO*.

Chávez, R. (2015). *Introducción a la Metodología de la Investigación.* Machala: Universidad Técnica de Machala.

Congreso Nacional. (2 de Diciembre de 2004). *LEY ORGANICA DE TRANSPARENCIA Y ACCESO Y A LA INFORMACIÓN PÚBLICA.* Obtenido de LEY ORGANICA DE TRANSPARENCIA Y ACCESO Y A LA INFORMACIÓN PÚBLICA: http://www.seguridad.gob.ec/wp-content/uploads/downloads/2015/04/ley_organica_de_transparencia_y_acceso_a_la_informacion_publica.pdf

Consejo Nacional de Planificación. (2013). *Plan Nacional del Buen Vivir.* Obtenido de https://www.unicef.org/ecuador/Plan_Nacional_Buen_Vivir_2013-2017.pdf

ECUADOR, C. D. (2008). *ELEMENTOS CONSTITUTIVOS DEL ESTADO.* Obtenido de http://www.inocar.mil.ec/web/images/lotaip/2015/literal_a/base_legal/A._Constitucion_republica_ecuador_2008constitucion.pdf

EL TELEGRAFO. (16 de AGOSTO de 2016). *Justicia*. Recuperado el 1 de Julio de 2017, de En Ecuador, el 85% de los delitos informáticos ocurre por descuido del usuario: http://www.eltelegrafo.com.ec/noticias/judicial/13/en-ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario

ESET. (1 de Diciembre de 2016). *Secutity Report Latinoamerica.* Recuperado el 1 de Julio de 2017, de Latinoamerica 2016: https://www.welivesecurity.com/wp-content/uploads/2016/04/eset-security-report-latam-2016.pdf

Estallo, M. d., & Fuente, F. G. (6 de Octubre de 2007). *Cómo crear y hacer funcionar una empresa.* Recuperado el 1 de Agosto de 2017, de Libros profesionales de empresa: https://books.google.com.ec/books?id=4O2e7DjTQL4C&printsec=frontcover#v=onepage&q&f=false

Excelsior. (13 de Enero de 2011). *Excelsior.com*. Recuperado el 11 de Junio de 2017, de Renault presenta una demanda por el caso de espionaje: http://www.excelsior.com.mx/node/703851

Garcia, J., & Casanueva, C. (10 de Enero de 2014). *Prácticas de la Gestión empresarial.* Recuperado el 8 de Octubre de 2017, de Definición de empresa: http://webquest.carm.es/majwq/public/files/files_user/gerardobernabe/definicion_de_empresa.pdf

GESCONSULTOR. (1 de Enero de 2017). *GOBIERNO T.* Recuperado el 5 de Junio de 2017, de RIESGO - CUMPLIMIENTO: http://www.gesconsultor.com/iso-27001.html

Gonzalez, M. V., & Quintana, N. C. (2004). *Ciencias Penales: Temas Actuales.* CAracas: Universidad Católica Adrés Bello.

Guato, J. (1-31 de Enero-Diciembre de 2016). *Sector Societario/ Documentos.* Recuperado el 12 de Octubre de 2017, de PASTEURIZADORA EL RANCHITO: http://appscvs.supercias.gob.ec/consultaImagen/VisualizaDocumetos.zul?tipoDocumento=economica&expediente=94642&idDocumento=3.1.5%20%20&fecha=2016-12-31%2000:00:00.0

Guerrero, D. (2012). *Fraude en la red, Aprenda a protegerse contra el fraude en internet.* Bogotá, Colombia: Ra-ma(España).

Heredero, C. d., & López, J. J. (2011). *Organización y Transfromación de los Sistemas de la Infromación en los sistemas.* Madrir: ESIC.

Hernández, M. (14 de Julio de 2017). *Forbes*. Recuperado el 20 de Julio de 2017, de Forbes: https://www.forbes.com.mx/el-robo-de-informacion-aun-es-un-problema-para-las-empresas-en-latam/

Hernández, M. A. (Diciembre de 2013). *Procedimientos y técnicas.* Recuperado el 7 de Febrero de 2018, de Estudio de Encuestas: https://www.uam.es/personal_pdi/stmaria/jmurillo/InvestigacionEE/Presentaciones/Curso_10/ENCUESTA_Trabajo.pdf

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la Investigación.* México, Bogotá: Mc Graw Hill.

Hurtado León, I., & Toro Garrido, J. (2017). *Paradigmas y métodos de investigación en tiempos de cambio.* Venezuela: CEC.SA.

INEC. (8 de Enero de 2014). *Directorio de Empresas y Establecimientos*. Recuperado el 16 de Julio de 2016, de Empresas: http://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Economicas/DirectorioEmpresas/Empresas_2014/Principales_Resultados_DIEE_2014.pdf

INEN. (22 de Mayo de 2009). *INSTITUTO ECUATORIANO DE NORMALIZACIÓN.* Recuperado el 12 de Julio de 2017, de Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27002:2009: http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2014/EXTRACTO_2014/GAN/nte_inen_iso_iec_27002extracto.pdf

ISO 27002. (2013). *ISO 27002.es*. Obtenido de Portal de soluciones técnicas y organizativas de referencia a los CONTROLES DE ISO/IEC 27002: http://iso27000.es/iso27002.html

ISO27000. (5 de Diciembre de 2005). *Sistema de Gestión de la Seguridad de la Información.* Recuperado el 2 de Julio de 2017, de ISO: http://www.iso27000.es/download/doc_sgsi_all.pdf

ISOTools. (17 de Octubre de 2016). *La Norma ISO 27001.* Recuperado el 13 de Septiembre de 2017, de Aspectos claves de su diseño e implantación: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

Kerlinger. (2017). *Métodos de Investigación.* Obtenido de http://www.psicol.unam.mx/Investigacion2/pdf/METO2F.pdf

Molina, V. H., & Cruz, E. P. (1 de Mayo de 2012). *Repositorios Digitales y Bibliotecas Ecuador.* Recuperado el 12 de Junio de 2017, de Pontificia Universidad Catolica del Ecuador: http://repositorio.puce.edu.ec/bitstream/handle/22000/12436/TESIS%20MAESTRÍA%20-%20Gerencia%20de%20TI.pdf?sequence=1&isAllowed=y

Moscoso, B. P. (Diciembre de 2016). *Superintendencia de Compañias y Valores.* Obtenido de Sector Societario/ Documentos/ Notas explicativas a los Estados Financieros separados por el año terminado: http://appscvs.supercias.gob.ec/consultaImagen/VisualizaDocumetos.zul?tipoDocumento=economica&expediente=7210&idDocumento=3.1.L%20%20&fecha=2016-12-31%2016:27:38.0

Otzen, T., & Manterola, C. (19 de Diciembre de 2016). *Técnicas de muestreo sobre una población a Estudio.* Recuperado el 10 de Enero de 2018, de Introducción a la Metodología de la Investigación: https://scielo.conicyt.cl/pdf/ijmorphol/v35n1/art37.pdf

Pareja, I. V. (2014). Inversiones. En I. P. Valéz, *Inversiones* (pág. 1). Bogotá: Pearson.

Pilco, E. H. (17 de Julio de 2014). *Repositorios Digitales y Bibliotecas Ecuador.* Recuperado el 8 de Junio de 2017, de ESTUDIO, ANÁLISIS Y COMPARACIÓN DE TRES HERRAMIENTAS : http://repositorio.utn.edu.ec/bitstream/123456789/1722/3/04%20ISC%20244%20ART%C3%8DCULO%20CIENT%C3%8DFICO.pdf

Portaltic Europa Press. (17 de febrero de 2017). *Portaltic europapress*. Recuperado el 10 de Junio de 2018, de Espionaje industrial: robo de información en el sector tecnológico y los casos más sonados: http://www.europapress.es/portaltic/sector/noticia-espionaje-industrial-robo-informacion-sector-tecnologico-casos-mas-sonados-20170217085938.html

Pritesh. (2012). *ISO 27002.ES*. Recuperado el Enero de 2018, de El prtal de ISO 27002 en Español: http://www.iso27000.es/iso27002_5.html

Robles, X. R. (31 de Agosto de 2015). *Repsitorio Digital Universidad De Las Américas.* Recuperado el 10 de Junio de 2017, de Repositorio Digital: http://200.24.220.94/bitstream/33000/4476/1/UDLA-EC-TIERI-2015-02.pdf

Sallenave, J. P. (2012). *La Gerencia Integral.* Bogota: Pearson.

Scharager, J. (2016). *Metodologia de la Investigacón.* Chile.

Smith, L. V. (31 de Marzo de 2017). *Superintendencia de Compañias.* Obtenido de Portal de Documentos: Acta de la Junta General Ordinaria Universal De Accionistas de "NOVACERO S.A.": http://appscvs.supercias.gob.ec/consultaImagen/VisualizaDocumetos.zul?tipoDocumento=economica&expediente=8360&idDocumento=3.1.N%20%20&fecha=2016-12-31%2000:00:00.0

Tamayo, M. (1997). *El proceso de la Investigacion Cientifica.* México: Limusa S.A.

Velásquez, A. (04 de Septiembre de 2017). *Mattica*. Recuperado el 03 de Enero de 2018, de Retorno de la inversión en seguridad informatica: https://mattica.com/retorno-de-inversion-en-seguridad-informatica/

Velásquez, R. (14 de Diciembre de 2016). *PROVEFRUT S.A.* Obtenido de Class International Rating: http://www.provefrut.com/uploads/content/2017/01/file_1485456180_1485456193.pdf

Villavicencio, C. J. (01 de Abril de 2016). *Superintendencia de Compañías.* Recuperado el 10 de Octubre de 2017, de Portal de Documentos: http://appscvs.supercias.gob.ec/consultaImagen/VisualizaDocumetos.zul?tipoDocumento=economica&expediente=87599&idDocumento=3.1.5%20%20&fecha=2016-12-31%2000:00:00.0

Zapata, F. X. (11 de Junio de 2014). *Repositorios Digitales Y Bibliotecas Ecuador.* Recuperado el 2017 de Junio de 8, de Universidad Central del Ecuador: http://www.dspace.uce.edu.ec/bitstream/25000/4244/1/T-UCE-0011-55.pdf

ANEXOS

DEPARTAMENTO DE CIENCIAS ECONÓMICAS ADMINISTRATIVAS Y DEL COMERCIO

CARRERA DE INGENIEÍA EN FINANZAS Y AUDITORÍA

CERTIFICACIÓN

Se certifica que el presente trabajo fue desarrollado por las Señoritas: **FERNANDA GISSELA GÁLVEZ ESCOBAR Y JOSELINE MARIELA SÁNCHEZ CAJAMARCA**

En la ciudad de Latacunga. A los 7 días del mes de Marzo del 2018

Eco. Francisco Caicedo A.
DIRECTOR DEL PROYECTO

Aprobado por:

Eco. Alisva Cárdenas P.
DIRECTORA DE CARRERA (E.)

Dr. Juan Carlos Díaz Álvarez
SECRETARIO ACADÉMICO