ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

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: FRAUDE INFORMÁTICO, ANÁLISIS DE VULNERABILIDAD EN LAS EMPRESAS DEL SECTOR INDUSTRIAL DE LA PROVINCIA DE COTOPAXI.

AUTORES:

DIEGO FERNANDO PINSHA DEFAZ

KLEBER GONZALO QUEVEDO ZAMBONINO

DIRECTOR: ING. LUIS ALFONSO LEMA CERDA

LATACUNGA

2017

DEPARTAMENTO DE CIENCIAS ECONÓMICAS, ADMINISTRATIVAS Y DEL COMERCIO

CARRERA DE INGENIERÍA EN FINANZAS Y AUDITORÍA

CERTIFICADO TUTOR

Certifico que el trabajo de titulación, "**FRAUDE INFORMÁTICO, ANÁLISIS DE VULNERABILIDAD EN LAS EMPRESAS DEL SECTOR INDUSTRIAL DE LA PROVINCIA DE COTOPAXI",** realizado por los señores **DIEGO FERNANDO PINSHA DEFAZ** y **KLEBER GONZALO QUEVEDO ZAMBONINO,** ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo que cumple con todos los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar a los señores **DIEGO FERNANDO PINSHA DEFAZ** y **KLEBER GONZALO QUEVEDO ZAMBONINO** para que lo sustenten públicamente.

Latacunga, Diciembre del 2017

Ing. Luis Alfonso Lema Cerda

DIRECTOR

DEPARTAMENTO DE CIENCIAS ECONÓMICAS, ADMINISTRATIVAS Y DEL COMERCIO

CARRERA DE INGENIERÍA EN FINANZAS Y AUDITORÍA

AUTORÍA DE RESPONSABILIDAD

Nosotros, **DIEGO FERNANDO PINSHA DEFAZ**, con cédula de identidad N° 050305003-1 y **KLEBER GONZALO QUEVEDO ZAMBONINO**, con cédula de identidad 050398732-3 declaramos que el presente trabajo de investigación titulado "**FRAUDE INFORMÁTICO, ANÁLISIS DE VULNERABILIDAD EN LAS EMPRESAS DEL SECTOR INDUSTRIAL DE LA PROVINCIA DE COTOPAXI",** ha sido desarrollado de acuerdo a 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 ellos nos declaramos responsables del contenido, veracidad y alcance de investigación mencionada.

Latacunga, Diciembre del 2017

DIEGO FERNANDO
PINSHA DEFAZ
C.C.: 050305003-1

KLEBER GONZALO
QUEVEDO ZAMBONINO
C.C.: 050398732-3

ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS ECONÓMICAS, ADMINISTRATIVAS Y DEL COMERCIO

CARRERA DE INGENIERÍA EN FINANZAS Y AUDITORÍA

AUTORIZACIÓN

Nosotros **DIEGO FERNANDO PINSHA DEFAZ Y KLEBER GONZALO QUEVEDO ZAMBONINO,** autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca virtual de la institución el presente trabajo de titulación denominado "**FRAUDE INFORMÁTICO, ANÁLISIS DE VULNERABILIDAD EN LAS EMPRESAS DEL SECTOR INDUSTRIAL DE LA PROVINCIA DE COTOPAXI",** cuyo contenido, ideas y criterios son de nuestra autoría y responsabilidad.

DIEGO FERNANDO
PINSHA DEFAZ
C.C.: 050305003-1

KLEBER GONZALO
QUEVEDO ZAMBONINO
C.C.: 050398732-3

Latacunga, Diciembre del 2017

DEDICATORIA

"No hay secretos para el éxito. Este se alcanza, trabajando arduamente y aprendiendo del fracaso."

Colin Powell

A mi Madre

A mi Madre Nelly Eloisa Defaz Vilcacundo por ser la mujer, madre, amiga, consejera, apoyo incondicional, quien desde pequeño con mucho sacrificio y esfuerzo me ha dado el todo el apoyo necesario para mi educación y más aún para mi carrera profesional , quien ha estado en las malos y buenos momentos, brindándome comprensión, cariño y amor, por estar conmigo en todos los éxitos y fracasos que he tenido ayudándome a levantarme, ha sido mi fuente de inspiración y motivación para superarme día a día y así lograr este objetivo tan anhelado, a ella es que le dedico con amor, esfuerzo y dedicación, "MADRE QUERIDA TE AMO"

A mis hermanos

A mi hermana Evelyn y mi hermano Edwin por haberme apoyado en todo momento, por estar pendientes de mí, y de mi realización paso a paso en mi carrera profesional.

A mi familia

A toda mi familia por estar siempre conmigo con palabras de aliento, para seguir en adelante y nunca desmayar en este largo caminar.

Gracias a todos

DEDICATORIA

"Lo único que se interpone entre ti y tu sueño, es la voluntad de intentarlo y la creencia de que en realidad es posible".

Joel Brown

Con profundo amor y respeto dedico este trabajo:

A mis padres Elvia Inés Zambonino y Luis Gonzalo Quevedo quienes han sido mi fortaleza y respaldo moral, económico para el logro de esta meta, con sus sabios consejos me enseñaron a ser un hombre de bien y a superar las adversidades que se presentaron en mi vida siendo un hoy un profesional.

A mis hermanos y hermanas (Polivio, Fabián, Roció, Mercedes, Mirian, Margoth, Diana, Carmen y Magali), y toda mi familia por las palabras de apoyo que siempre me brindaron día a día en el transcurso de mi carrera, en especial a Dianita y Mirian quienes han sido mis segundas madres, mis consejeras y confidentes de mis éxitos y derrotas.

A mis sobrinos y sobrinas (Anthony, Edwin, Fabricio Sandro, Denis, Elvin, Xavier Ismael, Jampier, Nicolás, Markel, Gilmar, Erika, Melania, Aymar, y Tania) quienes son mi razón de vivir, mi fuerza de superación personal y profesional.

A mi mejor amiga, compañera y enamorada Cecilia quien compartió conmigo los momentos difíciles, felices y trascendentales durante este arduo caminar, brindándome su amor incondicional……

AGRADECIMIENTO

Comenzar agradeciendo a Dios y a la Santísima Virgen del Quinche, por darme esta oportunidad de vida, quienes iluminan mi sendero enfocándome por el camino del bien, gracias a Dios por la privilegiada familia que tengo que ayudaron alcanzar esta meta tan añorada.

Agradezco a mi compañero y amigo de investigación Kleber Quevedo, por haber compartido 5 años de carrera universitaria, tiempo que hemos compartido tantas cosas hasta la realización del trabajo de titulación, formando un equipo excelente de trabajo compartiendo conocimientos y valores como la amistad, la perseverancia, constancia y la humildad.

Agradezco al estimado Ing. Luis Alfonso Lema Cerda, Director de Tesis, por ser una gran persona excepcional, un apoyo fundamental en la realización del presente trabajo, brindándonos su amistad, paciencia, conocimientos, experiencias, valores, guiándome de una manera íntegra y profesional en la ejecución y finalización del proyecto, gracias querido director.

Al director de Carrera el Ing. Julio César Tapia León, docente, amigo y una gran persona por siempre estar pendiente de sus estudiantes a lo largo de la formación profesional, enseñándonos a superar cualquier obstáculo y alcanzar nuestras metas.

Agradezco a todos los docentes que formaron parte de mi formación académica, por la paciencia y todos sus conocimientos mil gracias.

A la Universidad de las Fuerzas Armadas "ESPE", por brindarme la oportunidad de pertenecer a tan prestigiosa institución, formándome con valores éticos y morales para el desenvolvimiento en mi vida profesional.

AGRADECIMIENTO

Al terminar el presente trabajo, quiero agradecer a Dios por haberme concedido la salud y la vida, por ser la luz que guía mi camino por el sendero del bien, la paz y la tranquilidad, por la familia extraordinaria que tengo a mi lado, quienes me apoyan día a día.

También agradezco a mi compañero y amigo de investigación Diego Fernando, por haber compartido este tiempo en la realización del trabajo con quien forme un verdadero equipo de trabajo donde prevaleció el respeto, la amistad, la perseverancia y constancia.

A mi Director de Tesis Ing. Luis Lema Cerda, por su amistad, paciencia, quien me guió y me brindó sus conocimientos y experiencias para la ejecución de la tesis.

Al Ing. Julio Tapia, amigo, docente y gran ser humano, quien con su experiencia y don de gente me enseño que una caída no es una derrota, es un aprendizaje más en el camino de la vida que hay que superarlo para lograr nuestros sueños anhelados y alcanzar el éxito en nuestra vida.

A la prestigiosa Universidad de las Fuerzas Armadas "ESPE", quien me abrió sus puertas para lograr este objetivo, que me permitirá realizarme como profesional competitivo en el mercado laboral, imponiendo mis valores positivos cultivados durante mi vida.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente proyecto de investigación está orientado a realizar un análisis de fraude informático y la vulnerabilidad de las empresas del sector industrial de la provincia de Cotopaxi durante el periodo 2012-2016, ya que por muchos años estas empresas han sido el pilar fundamental para el desarrollo de su comunidad, aportando al bienestar de las familias que la conforman y es importante investigar la tendencia de fraudes en las organizaciones del sector. La investigación consta de cinco capítulos en lo que se estudiarán distintos tópicos relacionándose a una investigación exploratoria de datos de las empresas manufactureras de la provincia, iniciando con la problemática de la investigación y su evaluación de los sistemas de información y vulnerabilidad que estos pueden sufrir, contextualizando las variables de estudio, definiendo las bases teóricas con respecto al tema planteado y que servirán de apoyo al desarrollo del estudio, también nos referimos a un diagnostico financiero previo, a la utilización de la metodología a emplear en la ejecución del proyecto, donde la investigación es netamente de campo, descriptiva y exploratoria, dando a conocer los resultados del análisis de control interno, encuestas, auditoría informática, examen especial y análisis forense digital, para dar solución a los fraudes informáticos y nuestra opinión de como contrarrestarlos. Se describe el análisis y evaluación de los resultados de la investigación realizando la comprobación de la hipótesis y estableciendo una tendencia de los fraudes informáticos en la Provincia, además se realizó un diagnóstico de los fraudes informáticos, una guía de buenas prácticas para la protección y seguridad de la información en las empresas, por último se finaliza con las conclusiones y recomendaciones orientadas a todo el proceso de la investigación.

PALABRAS CLAVE:

- **COTOPAXI – EMPRESAS INDUSTRIALES**
- **FRAUDE INFORMÁTICO**
- **SISTEMAS DE INFORMACIÓN - VULNERABILIDAD**
- **CONTROL INTERNO**
- **SEGURIDAD INFORMÁTICA**

ABSTRACT

This research project is aimed at conducting an analysis of computer fraud and the vulnerability of companies in the industrial sector in the province of Cotopaxi during the period 2012-2016, since for many years these companies have been the fundamental pillar for the development of their community, contributing to the welfare of the families that comprise it and it is important to investigate the trend of fraud in organizations in the sector. The research consists of five chapters in what will be studied different topics related to an exploratory research of data from manufacturing companies in the province, starting with the problem of research and its evaluation of the information systems and vulnerability they may suffer, contextualizing the variables of study, defining the theoretical bases with respect to the topic raised and that will serve to support the development of the study, we also refer to a previous financial diagnosis,. The analysis and evaluation of the results of the investigation is described by checking the hypothesis and establishing a trend of computer fraud in the Province, in addition, a diagnosis of computer fraud was made, a guide to good practices for the protection and security of information in companies, and finally, conclusions and recommendations aimed at the entire investigation process are finalized.

KEYWORDS:

- **COTOPAXI – ENTERPRISE INDUSTRIAL**
- **COMPUTER FRAUD.**
- **INFORMATION SYSTEMS - VULNERABILITY.**
- **INTERNAL CONTROL.**
- **INFORMATIC SECURITY**

CAPÍTULO I

1. PROBLEMA DE LA INVESTIGACIÓN

1.1. Tema de investigación

Fraude Informático, Análisis de Vulnerabilidad en las empresas del Sector Industrial de la Provincia de Cotopaxi.

1.2. Área de Influencia

1.2.1. Área de Intervención

Empresas de la Provincia de Cotopaxi

1.2.2. Área de Influencia Directa

Las empresas del Sector Industrial de la Provincia de Cotopaxi.

1.2.3. Área de Influencia Indirecta

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

1.3. Problemática de la Investigación

1.3.1. Contextualización

a) Macro Contextualización

Las actividades informáticas delictivas en la actualidad presentan un constante crecimiento a nivel global, incluyendo a América Latina. El incremento de la delincuencia informática encuentra algunas de sus respuestas en una gran variedad de factores tecnológicos y cuyo desarrollo ya ha sido trabajado ampliamente con la finalidad de contrarrestar las vulnerabilidades de los sistemas informáticos.

Según Pilmayquen (2013) en su estudio realizado sobre “Delitos informáticos en Latinoamérica” menciona que:

> Los países de Latinoamérica en la década de los 90 se empezaron a promulgar leyes sobre la Confidencialidad e Integridad de la Información de las Empresas, Propiedad Intelectual, Software, Protección de Datos Personales, Falsedades Documentales, Documentos Electrónicos y Firma Digital hasta llegar a leyes sobre Delitos Informáticos”. (pág. 10).

El incremento de la tecnología disponible, tanto para el delincuente como para las víctimas, combina con el escaso conocimiento o información sobre cómo protegerse de los posibles delitos informáticos que se pueden sufrir a través de las nuevas tecnologías ya que esto otorga a los delincuentes un amplio campo fértil de potenciales víctimas de ataques.

Por otro lado, el crecimiento sostenido del mercado negro y de la evolución de la tecnología en el mundo funciona como motor que impulsa una importante concentración de delitos cibernéticos, principalmente destinados a obtener bases de datos con información personal privilegiada.

Según Temperini (2013) en una investigación realizada sobre Delitos Informáticos en Latinoamérica manifiesta que “De acuerdo a un estudio realizado se calculó que los costos directos asociados con los delitos informáticos que afectan a los consumidores en el mundo ascendieron a US$ 110.000 billones en doce meses” (pág. 1)

> El mismo estudio revela que por cada segundo 18 adultos son víctimas de un delito informático, lo que da como resultado más de un millón y medio de víctimas de delitos informáticos cada día, a nivel mundial. Entre los desafíos citados anteriormente, uno de los más importantes es el hecho que este tipo de delitos pueden ser cometidos sin respetar barreras geográficas o jurisdiccionales de las personas o empresas. (Temperini, 2013)

En este sentido, cualquier delincuente informático o hacker de sombrero negro puede operar acciones desde un determinado lugar, conectarse a sistemas o equipos en otra parte y finalmente atacar datos o

sistemas ubicados en otro sitio, para de esa manera tener una retribución económica que compense el fraude o delito informático.

ODILA

> Según datos de la Organización de Delitos Informáticos de Latinoamérica (ODILA) en su segundo reporte del 2016 nos presenta datos importantes referentes a los delitos informáticos, ya que todo se generó a partir de 1260 denuncias recibidas entre 16/06/2015 y el 16/06/2016, dando un promedio de 3 y 4 reportes diarios. (pág. 9)

Tipo de Víctimas

De acuerdo a la información que nos proporciona el Observatorio de Delitos Informáticos (ODILA), considera a cinco tipos de víctimas que han sufrido vulneración a sus sistemas de información, datos personales u organizacionales causando un impacto negativo en el desarrollo de las mismas.

> Se destaca que el 83% de los reportes han sido realizados por personas físicas, observándose un aumento en casi un 13% respecto del informe anterior. Este punto ratifica uno de los objetivos principales de ODILA, que es ser una fuente de consulta e información para las personas físicas. (Observatorio de Delitos Informaticos de Latinoamèrica (ODILA), 2016).

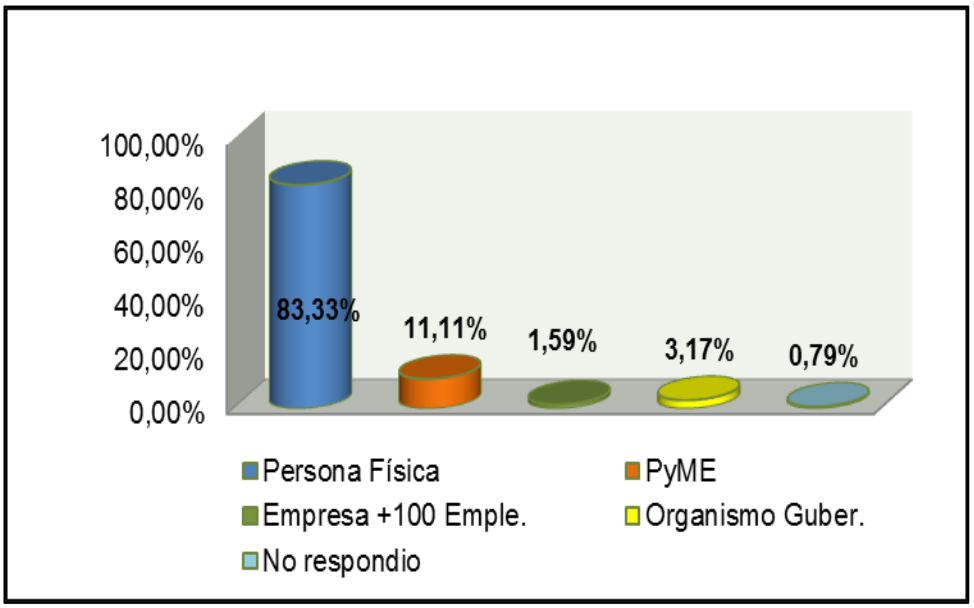


Figura 1 Tipos de Víctimas

De acuerdo a estudios realizados por la Organización de Estados Americanos (OEA) sobre “Tendencias en la seguridad cibernética en América Latina y el Caribe se afirma que:

“Es un desafío contabilizar el número de incidentes que afectan a los ciudadanos individuales ya que existe incluso un porcentaje más alto de ellos que pasan desapercibidos y no se reportan en ninguna fuente de información” (Observatorio de Delitos Informaticos de Latinoamèrica (ODILA), 2016)

En consideración al reporte presentado nos muestra datos relevantes con respecto a los ataques informáticos que han sufrido las personas u entidades, si estas han tomado algún tipo de acción legal o denuncia dentro de cada entidad competente si existiera en el país que se suscite el delito.

> Según este mismo informe que emite la Organización de Delitos Informáticos de Latinoamérica nos proporciona un ratio sobre la lista negra, de los perjudicados que en un 82% no han realizado la denuncia formal sobre los diversos ataque informático que han sufrido sus sistemas, con un incremento del 12% con relación al año anterior”. (pág. 10).

Figura 2 Promedio de denuncias

La no realización de una denuncia sobre el ataque de los intrusos en los sistemas informáticos de las empresas, es quizá por falta de experiencia

en como sobrellevar una vulnerabilidad o fallo informático, o por la no reacción inmediata de la unidad o departamento que fue afectado.

Causas de la falta de denuncias

Mediante el informe se presenta las principales causas por la cuales no se realiza la denuncia al haber sido víctima de un delito informático que se menciona a continuación:

- Primer lugar con un 19% (creció un 9% con respecto al informe anterior) las personas no denuncian porque no saben dónde ir a realizar las denuncias, poniendo en evidencia un gran problema sobre la falta de información, o bien, de la escasez de recursos para poder acceder a la justicia.
- En segundo lugar, compartiendo el índice del 16,19%, simplemente no se cree que la investigación tenga éxito, junto al temor por futuras represalias por parte del autor del delito. Esto demuestra la falta de confianza en la justicia e ilumina el análisis posterior sobre cuáles son los delitos más reportados.
- Tercer lugar, con un 13,33 % (8% más que antes), las personas reconocen que no se consideran víctimas y, en razón de ello, es que deciden no realizar las denuncias. Este dato podría ser analizado también por la falta de información por parte de los usuarios, ya que en general existe una situación de duda sobre si lo que están sufriendo configura o no un delito penal en el país donde se encuentran y como último pero no menos importante se encuentra.
- Cuarto lugar con un 12.38% se encuentran a aquellos que deciden no realizar las denuncias privilegiando la confidencialidad del incidente. (Observatorio de Delitos Informaticos de Latinoamèrica (ODILA), 2016).

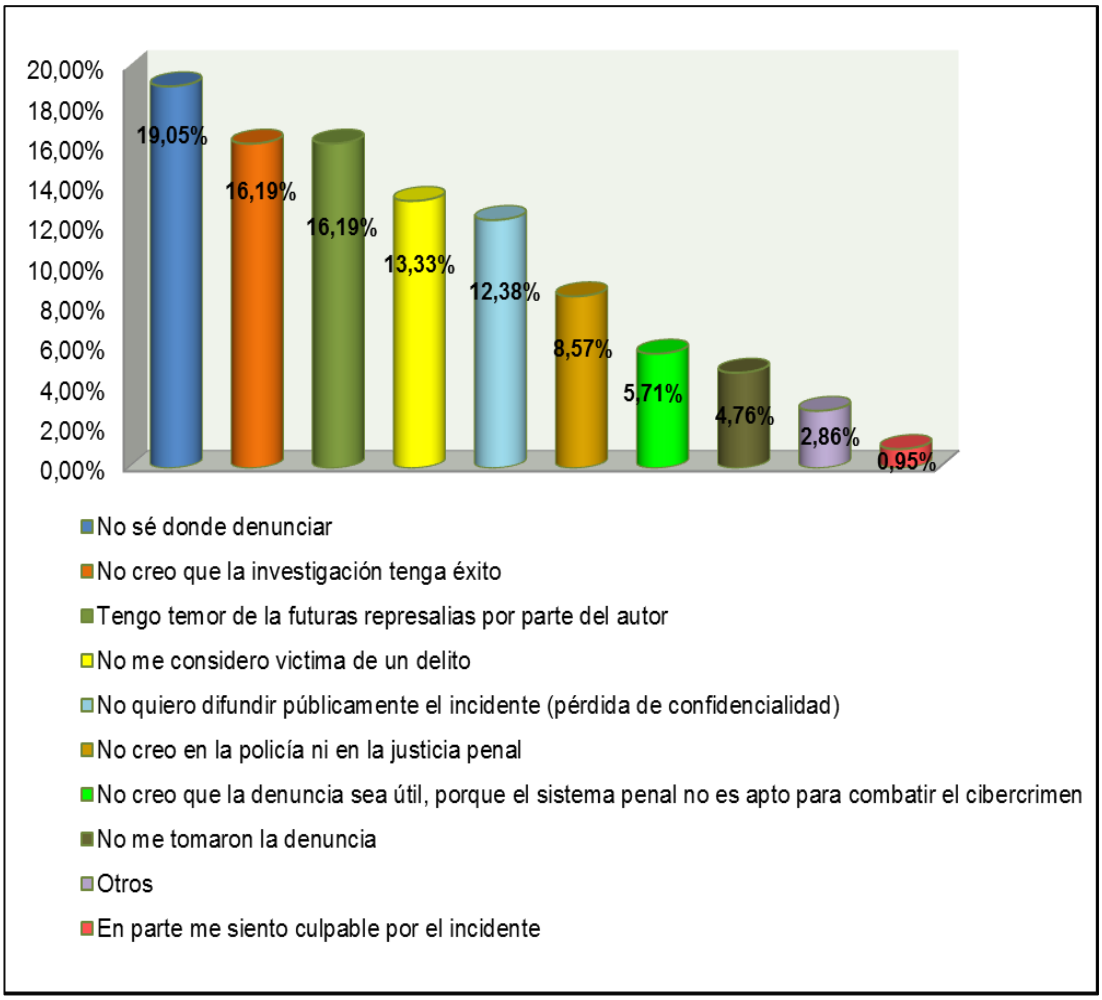


Figura 3 Causas de la falta de denuncias

Una vez mencionado cuales son las principales causas ver Gráfico 3, por las cuales no se realizan las respectivas denuncias podemos decir, que esto no se da quizá por el no convencimiento de que son víctimas directas, de no saber a dónde ir a denunciar a qué lugar en específico y el ultimo por conservarlo de manera reservada, no hacerlo público, serian decisiones que cada uno de los empresarios o quienes dirijan las empresas sepan dirigir de la mejor manera.

A continuación se presenta los tipos de incidentes más representativos denunciados por parte de las personas y organizaciones que han sido estudiados por ODILA de manera minuciosa y clara.

Tipos de incidentes denunciados

Existen una variedad de ataques cibernéticos o delitos informáticos que se van expandiendo a nivel mundial los cuales se nombra a continuación los más identificados en América Latina.

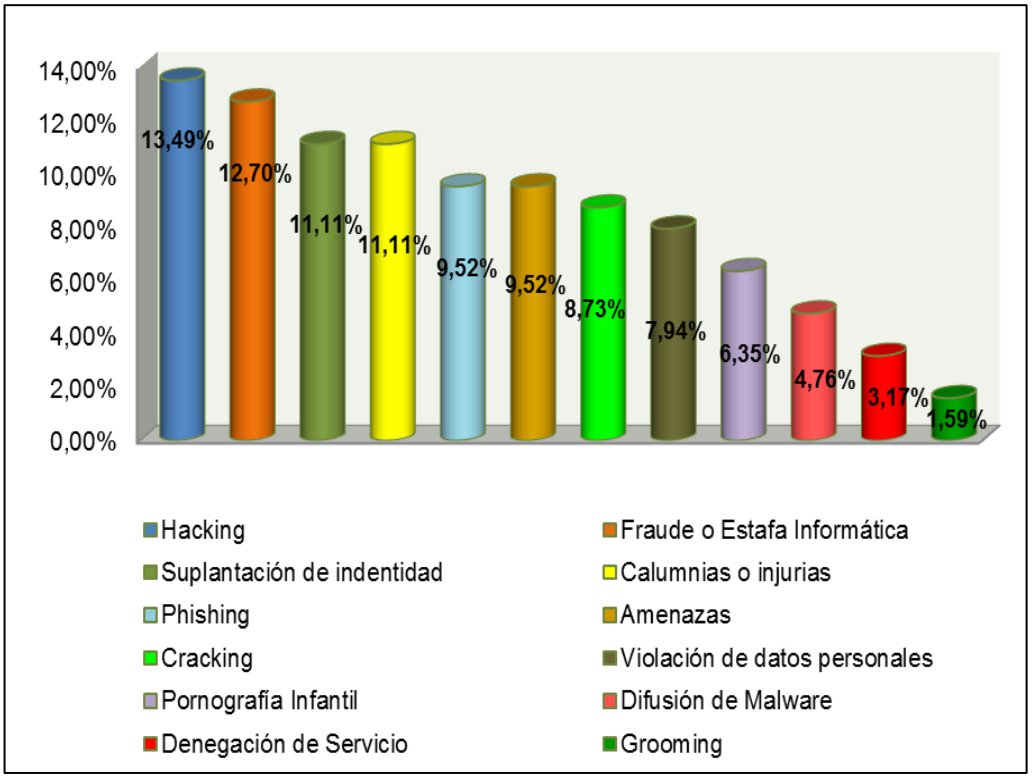


Figura 4 Tipos de incidentes denunciados

Con respecto al primer informe ha disminuido en un 9%, pero el primer lugar de incidentes denunciado es el acceso indebido de datos o sistemas restringidos (hacking) reportado con un 13.5%, en segundo lugar se encuentra los fraudes y estafas informáticas con un 4.2% y como tercer lugar con un 11.11% comparte posición las calumnias e injurias, de la mano con la suplantación de identidad digital en un + 2%. (Observatorio de Delitos Informaticos de Latinoamèrica (ODILA), 2016)

Cantidad de denuncias por país

En Latinoamérica se puede observar que Argentina es el país que ha sufrido la mayor cantidad de ataques generándose un porcentaje de denuncias del 55%, y con relación a los demás países se encuentran en un

rango menor del 10%, donde seguido del primer lugar están Colombia, Honduras, México y Ecuador.

Dentro de esta información tenemos a Ecuador formando parte de las denuncias sobre algún delito informático, con un porcentaje del 4.76%, algo que no es tan significativo con respecto a los ataques identificados.

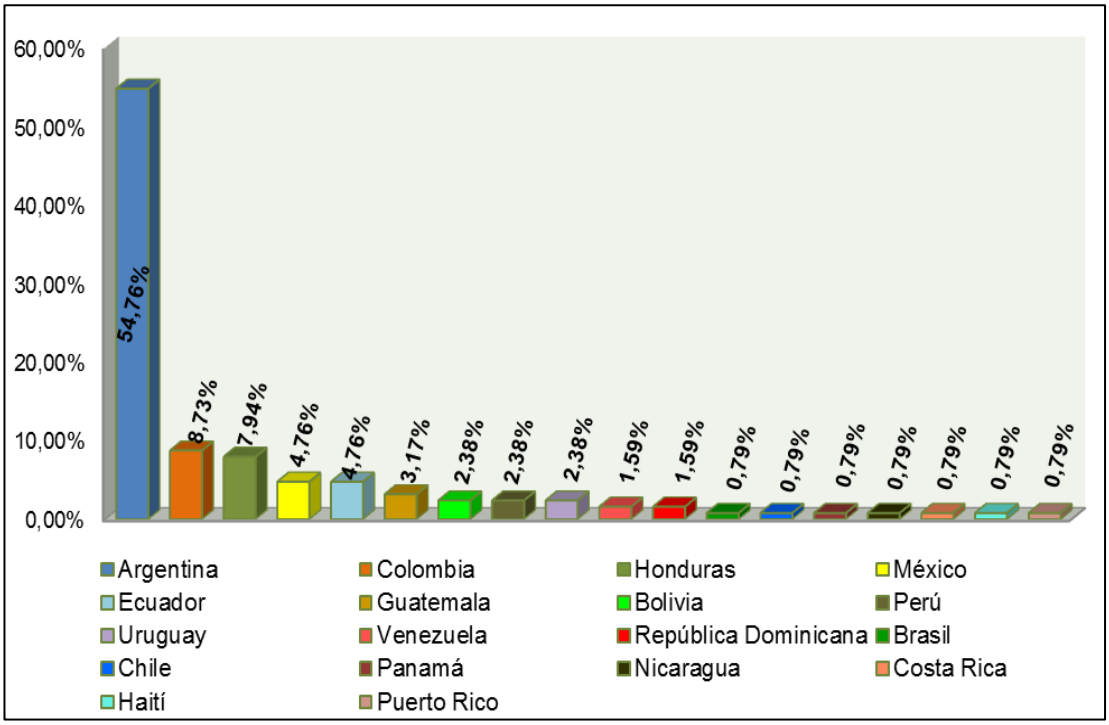


Figura 5 Denuncias por País

b) Meso Contextualización

Ecuador es el país que en la década de los 90 tiene el acceso a la conexión de Internet, ya que no se identificaron iniciativas de TIC para el desarrollo en los diferentes campos laborales, es decir en las organizaciones, las actividades estaban orientadas al uso interno de las mismas, donde a partir de la segunda mitad de los 90 se empiezan a efectuar algunas iniciativas todavía incipientes, es así que países hermanos se enlazaron más tarde que el Ecuador logrando niveles de cobertura, conectividad y velocidad más extensos y rápidos que en estos país.

Según el Ministerio de Telecomunicaciones y Sociedad de la Información menciona que “Ecuador es reconocido como un país que implementa políticas públicas para universalizar el acceso a las Tecnologías de la Información y Comunicación (TIC), ejecutadas por el Ministerio de Telecomunicaciones y de la Sociedad de la Información. (MINTEL, sf).

> El MINTEL, en cooperación con el Instituto Nacional de Pre inversión (INP), desarrolló el Plan Estratégico de Investigación, Desarrollo e Innovación para las TIC en el Ecuador, para el período 2014-2018, con el objetivo de determinar el direccionamiento estratégico más conveniente para el desarrollo de las TIC en el país, en concordancia con el Plan Nacional del Buen Vivir. Diversos estudios confirman el desarrollo de la industria de las Tecnologías de la Información y Comunicación y los beneficios sociales y económicos que generan la masificación del uso de internet, por lo que ejecuta un plan estratégico de las TIC, en el ámbito de la Sociedad de la Información y Gobierno Electrónico. (Ministerio de Telecomunicaciones y Sociedad de la Informacion, sf).

En el Ecuador el ministerio de telecomunicaciones conjuntamente con el Plan Nacional del Buen Vivir (2013 – 2017), informa que todas las organizaciones ya sean públicas o privadas deben estar inmersas a la inclusión en tecnologías de información y comunicación, con la finalidad de crear un ambiente de conocimiento en las últimas tendencias tecnológicas.

Dentro de un contexto nacional, Ecuador cuenta con datos importantes que pueden ayudar de manera relevante conocer la perspectiva de crecimiento de fraudes informáticos o ciberataques que sufren las personas y empresas, datos que han sido recogido por lo diferentes medios de prensa escrita, páginas web, o por los mismos portales de cada una de las instituciones del Estado Ecuatoriano como la Fiscalía General de Estado, Agencia de Regulación y Control de las Telecomunicaciones

Diario el Telégrafo

> La Fiscalía General del Estado registró 530 delitos informáticos en los primeros cinco meses de 2016, en el mismo período del año anterior se presentaron 635 denuncias. Las cifras evidencian una disminución. En Guayas hubo 18 casos; 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”. (Diario El Telégrafo, 2016)

En relación a la información anterior se puede evidenciar que en los datos existe una disminución en las cifras, en relación al año anterior dentro del mismo periodo investigado, y nos da una connotación de como la tecnología se vuelven cada vez más vulnerable tanto para las empresas y la personas, siendo los mismos blancos fáciles de ataques informáticos directos mediante lo cual los intrusos pueden apropiarse la información y utilizarlo de manera maliciosa con la finalidad de obtener un rédito económico financiero.

Según un estudio elaborado por la Policía Nacional, de manera conjunta con la Interpol y el Centro de respuestas a Incidentes informáticos de Ecuador (Ecucert) y con el apoyo importantes organismos similares de América Latina que coadyuvan a la protección de la información y de ciberataques nos indican que:

- El 85% de los ataques cibernéticos sobre los sistemas informáticos son causados por errores de los consumidores, quienes no toman precauciones al acceder a las redes sociales, utilizar el correo electrónico.
- El 58% de personas permiten que sus teléfonos móviles contengan información sensible, con respecto a sus cuentas bancarias o información de negocios.
- El 60% utiliza el mismo Password en dispositivos laborales y personales.
- Finalmente el 80% de amenazas en las redes sociales juega con la curiosidad de los usuarios que quieren saber quién o quiénes ven su perfil, anota el capitán Edgar Toapanta, Oficial de Seguridad de la Información Pública. (Diario El Telégrafo, 2016)

Por lo tanto se puede evidenciar que existe un descuido total en el manejo de la seguridad de los sistemas de información, por parte de las personas y de las organizaciones encontradas en las provincias más grandes del país como son Guayas, Pichincha, Azuay y el Oro.

Según Troops, Trolls and Troublemakers en un estudio realizado sobre las Tropas Cibernéticas menciona que “Ecuador es uno de los 28 países que tienen tropas cibernéticas, destina recursos estatales y contrata empresas privadas con este fin. Estas son las principales conclusiones del estudio” (Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation., 2017).

> Es la primera vez que el país queda registrado en el mapa mundial de las guerras cibernéticas por el control de la opinión. Según los investigadores de Oxford, Samantha Bradshaw y Philip N. Howard, las tropas cibernéticas son equipos gubernamentales, militares o de partidos políticos que buscan manipular la opinión pública en las redes sociales. Las consideran como “un fenómeno omnipresente y global. (Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation., 2017).

Ecuador registra tanto el uso de 'bots' como de humanos en sus tropas cibernéticas. Es uno de los países cuyos gobiernos han creado plataformas para atacar a sus críticos. Es el caso del sitio Somos +.

País	Mensajería y valencia		Estrategia de comunicación		
	Comentarios en los medios sociales	Orientación individual	Cuentas falsas	Sitios web, cuentas o aplicaciones gubernamentales	Creación de contenido
Argentina	+/-	Pruebas encontradas	Automatizado	...	
Brasil	+/n	Pruebas encontradas	Automatizado, Humano, organismo cibernético	...	Pruebas encontradas
Ecuador	**+/-**	**Pruebas encontradas**	**Automatizado, humano**	**Pruebas encontradas**	
México	+/-	Pruebas encontradas	Automatizado, humano, organismo cibernético	...	Pruebas encontradas
Venezuela	+	...	Automatizado, humano	Pruebas encontradas	...

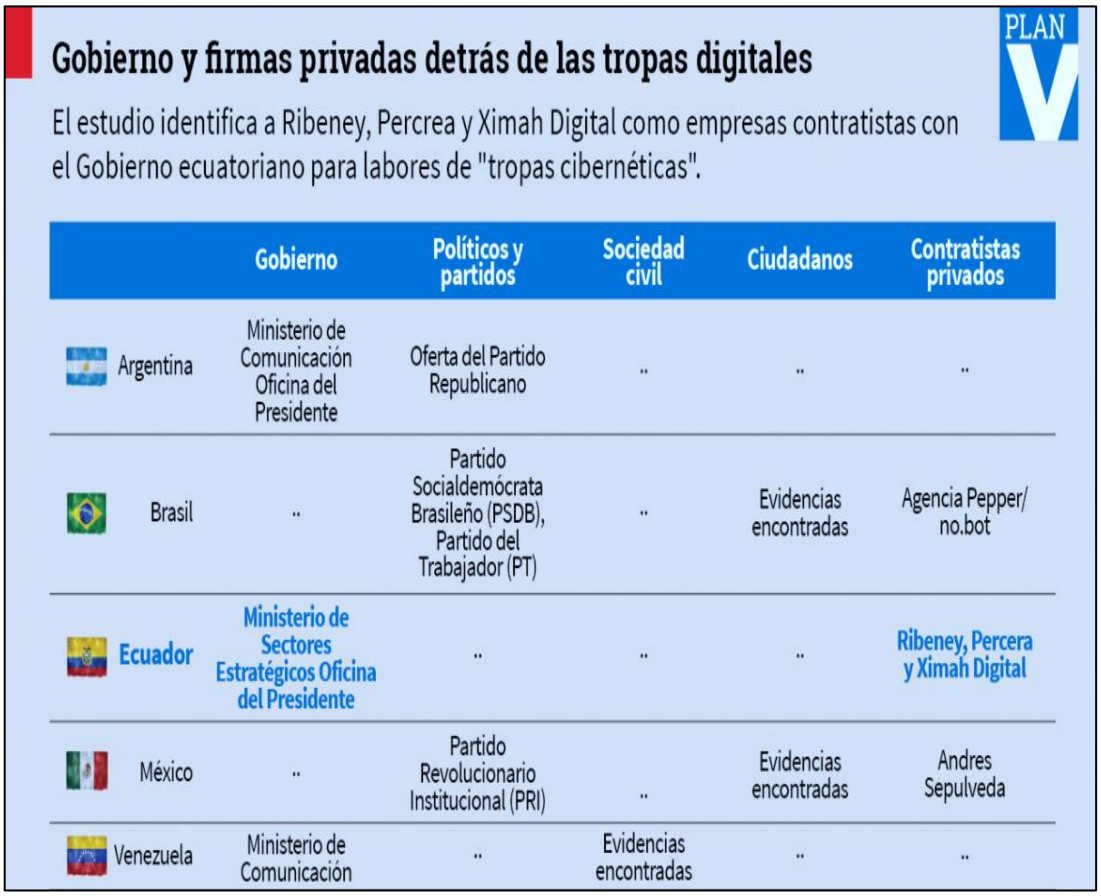
Figura 6 Estrategias, herramientas y técnicas para la manipulación de las redes sociales

Fuente: (Moran, 2017)

Según los estudios realizados se puede ver que además de existir cuentas propias de las personas, muchos equipos de las tropas cibernéticas funcionan con cuentas falsas para enmascarar su identidad e intereses. Y por

esta razón se puede decir que este fenómeno se lo conoce como “astroturfing”, una técnica que consiste en ocultar al verdadero emisor de un mensaje publicitario o propagandístico, y hacerlo pasar por una expresión popular y espontánea.

> En Ecuador el reporte señala que las empresas Ribeney, Percrea y Ximah Digital. Las tres firmas han sido protagonistas de amplios reportes periodísticos. Una filtración de los usuarios de esas cuentas en septiembre de 2014 permitió identificar que la empresa Ximah es una empresa publicitaria vinculada a la administración de cuentas troll identificadas con el Gobierno como @elpatriota. (Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation., 2017).



Gobierno y firmas privadas detrás de las tropas digitales

PLAN V

El estudio identifica a Ribeney, Percrea y Ximah Digital como empresas contratistas con el Gobierno ecuatoriano para labores de "tropas cibernéticas".

	Gobierno	Políticos y partidos	Sociedad civil	Ciudadanos	Contratistas privados
Argentina	Ministerio de Comunicación Oficina del Presidente	Oferta del Partido Republicano	..	..	..
Brasil	..	Partido Socialdemócrata Brasileño (PSDB), Partido del Trabajador (PT)	..	Evidencias encontradas	Agencia Pepper/ no.bot
Ecuador	Ministerio de Sectores Estratégicos Oficina del Presidente	..	..	..	Ribeney, Percera y Ximah Digital
México	..	Partido Revolucionario Institucional (PRI)	..	Evidencias encontradas	Andres Sepulveda
Venezuela	Ministerio de Comunicación	..	Evidencias encontradas	..	..

Figura 7 Gobierno y firmas privadas detrás de las tropas digitales

Fuente: (Moran, 2017)

Según el estudio, los equipos que conforman las tropas cibernéticas van desde 20 personas a redes de dos millones que trabajan para promover la línea partidista (por ejemplo, en China). Sobre el

> presupuesto, el reporte aclara que la cantidad de información pública disponible sobre los gastos es limitada. Pero en el caso del Ecuador señala que los contratos con empresas privadas cuestan, en promedio, USD 200.000. (Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation., 2017).

Con respecto a estos estudios realizados se puede concluir que las tropas cibernéticas están conformadas por un sinnúmero de personas que tienen una misma finalidad que es manipular a las personas a través de las redes sociales, para maniobrar por intermedio de medios públicos la integridad personal. Por esta razón se puede aludir que Ecuador forma parte de los 28 países que tienen tropas cibernéticas, las cuales son destinadas a contratos con empresas públicas y privadas y en especial están vinculadas directamente con las actividades presidenciales.

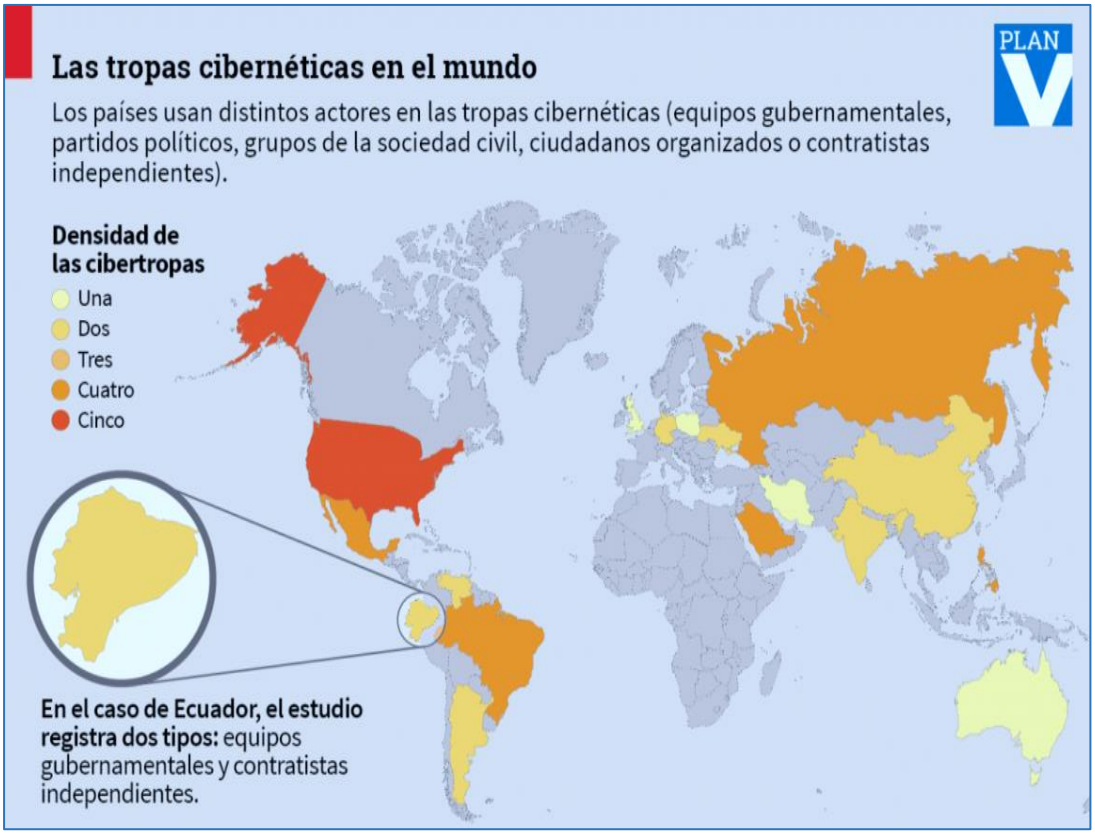


Figura 8 Tropas Cibernéticas en el mundo

Fuente: (Moran, 2017)

c) Micro Contextualización

El presente proyecto será ejecutado en la provincia de Cotopaxi específicamente en las empresas del sector industrial, donde por el nivel de producción y de la actividad que se dedican, poseen un almacenamiento masivo de la información y su seguridad debe ser al cien por ciento, siendo el sector manufacturero una de las actividades de mayor aporte en el desarrollo económico y financiero de la provincia, actualmente existen empresas que pertenecen como son: Novacero, Parmalat, Induacero, Familia Sancela del Ecuador, Molinos Poultier, Carnidem, Calzacuba, Aluminio del Ecuador Cedal, Dlip-Industrial, Aglomerados Cotopaxi, Licorec S.A, Adrián Imceal, Editorial la Gaceta, Corp.-Ice-Cream, Provefrut, Fuentes San Felipe, Prodicereal, Construcciones Ulloa S.A, El Ranchito, las cuales generan una producción muy significativa para el abastecimiento dentro de la zona centro del país y del resto del Ecuador.

La falta de sistemas de protección de datos adecuados para el control de fraudes informáticos, así como capacitación a sus administradores y personal de las empresas genera un desconocimiento de las diferentes seguridades ante posibles vulnerabilidades y ataques que las empresas pueden sufrir en el transcurso de sus actividades.

Conociendo dichos parámetros o estándares de seguridad preestablecidos ayudaría a que las organizaciones del sector no tengan inconvenientes en la operatividad de sus actividades y una coordinación en la toma de decisiones ante cualquier adversidad externa maliciosa que se pueda generar e identificar.

También se puede mencionar que en la Provincia de Cotopaxi y en todo el Ecuador existe poca estadística que sustente hallazgos sobre fraudes informáticos dentro de las empresas que se dedican a la manufactura las cuales pueden ser objeto de intromisión o vulneración de información por parte de los ciberatacantes.

d) Árbol de Problemas

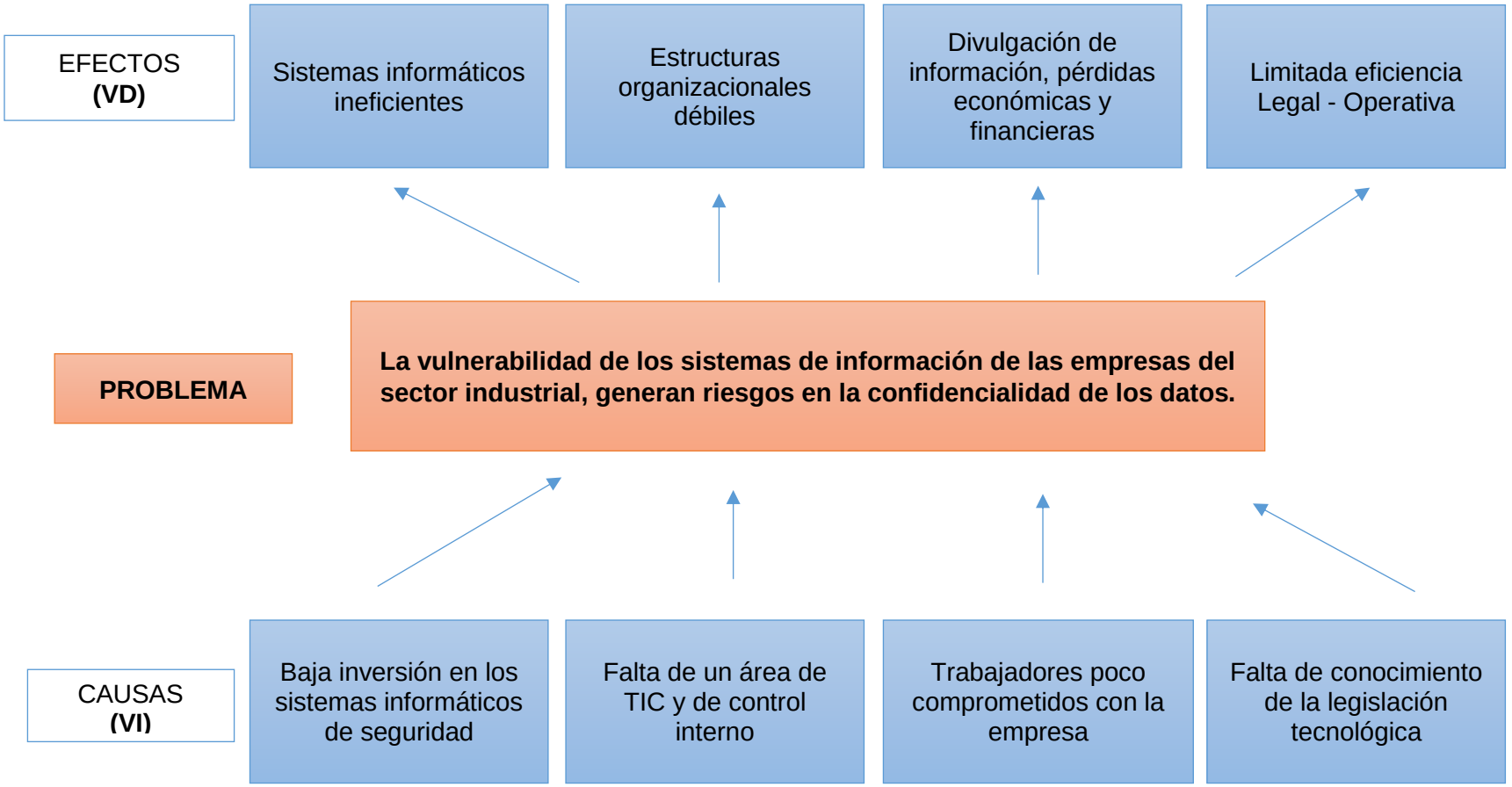


Figura 9 Relación Causa Efecto

e) Análisis Crítico

En las empresas industriales de la provincia de Cotopaxi el desconocimiento del desarrollo tecnológico por parte de los propietarios ha generado que exista una vulnerabilidad de los sistemas informáticos ocasionando fraudes de este sector económico financiero, así como también la falta de capacitación por parte de la administración para quienes están a cargo de las TIC, hace que todos los procesos tecnológicos sean cada vez más fáciles de ataques cibernéticos.

La vulnerabilidad dentro de las empresas del sector industrial tienen el reto de enfrentarse a grandes desafíos con respecto a la seguridad de la información y gestión de riesgos en TI, por lo que deben realizar una importante inversión en recursos tecnológicos y establecer un mecanismo de control y detección los cuales ayudarán a prevenir grandes impactos en la fuga de información para prevenir elevadas pérdidas económicas y financieras.

La inoportuna reacción a las tecnologías de información ha frenado el fortalecimiento de las competencias empresariales quienes están a cargo del manejo de las diversas organizaciones, el mercado de seguridad informática con respecto a las TIC tiene un limitado desarrollo de investigación lo cual ocasiona la vulnerabilidad en los datos de información, por otro lado se puede observar que existe poco conocimiento del sector manufacturero debido a un limitado esfuerzo que cada una de la empresas impulsa quizá porque ninguna ha sufrido alguna anomalía, indicios de fraude informático, o por los insuficientes recursos económicos que destinan a la inversión en tecnologías de información y comunicación, la misma que ayuda en el desarrollo de las actividades principales, promoviendo la eficiencia y eficacia de los procesos de operatividad de las diferentes áreas empresariales.

1.4. Objetivos

1.4.1. Objetivo General

Analizar la vulnerabilidad a fraudes informáticos en las empresas del sector industrial mediante un examen especial que permita establecer parámetros de riesgo en la Provincia de Cotopaxi durante el periodo 2012 – 2016.

1.4.2. Objetivos Específicos

- Describir la problemática de la investigación de acuerdo a las variables objeto de estudio para un mejor desarrollo de la misma.
- Definir las bases teóricas bajo las cuales se sustenta la investigación en torno a la vulnerabilidad de fraudes informáticos en las empresas industriales.
- Determinar los niveles de vulnerabilidad en fraudes informáticos para su posterior evaluación de las debilidades a nivel empresarial del sector industrial de la provincia de Cotopaxi.
- Analizar los hallazgos, resultados y elaborar un informe de auditoría para determinar una opinión, tendencia de control en las empresas del sector industrial de la Provincia de Cotopaxi.
- Elaborar una Guía de Buenas Prácticas para el control de vulnerabilidades en Fraudes Informáticos para las empresas del sector industrial de la Provincia de Cotopaxi.

1.5. Justificación

La investigación contribuirá con el objetivo N° 11 del Plan Nacional del Buen Vivir (2013 – 2017), el mismo que asegura la soberanía eficiente de los sectores estratégicos para la transformación industrial y tecnológica. Las empresas del sector industrial representan la mayor fuente de empleo de la zona centro del país, por lo que es fundamental impulsar la inversión en tecnologías

de información y comunicación a través de la implementación de sistemas de seguridad para un buen manejo de recursos económicos, financieros y tecnológicos, por lo que se contribuye con las áreas vulnerables otorgándoles mayores posibilidades de mitigar los riesgos informáticos.

Para lo cual se estipula las políticas y lineamientos estratégicos alineados al Objetivo N° 11 del Plan Nacional Buen Vivir (2013 – 2017) y se relaciona con la política 11.3. (Plan Nacional del Buen Vivir, 2013)

Política y Lineamiento 11.3

Democratizar la prestación de servicios públicos de telecomunicaciones y de tecnologías de información y comunicación (TIC), incluyendo radiodifusión, televisión y espectro radioeléctrico, y profundizar su uso y acceso universal.

Esta política está relacionada con los siguientes literales:

- Fortalecer las capacidades necesarias dela ciudadanía para el uso de las TIC, priorizando a las PYMES y a los actores dela economía popular y solidaria.
- Fortalecer la seguridad integral usando las TIC.
- Impulsar la calidad, la seguridad y la cobertura en la prestación de servicios públicos, a través del uso de las telecomunicaciones y de las TIC; especialmente para promover el acceso a servicios financieros, asistencia técnica para la producción, educación y salud. (Plan Nacional del Buen Vivir, 2013)

La importancia teórica de esta investigación es realizar un análisis de información relacionada con el tema “Fraude informático, análisis de vulnerabilidad de las empresas del sector industrial de la provincia de Cotopaxi y asociar a las empresas del sector para una comparación clara y precisa de los problemas que pueden seguir brotando sino se posee un sistema de control, una

adecuada capacitación del personal en el área de tecnologías de información ya que en actualidad son muy necesarias debido a los cambios tecnológicos que se presentan día a día, lo cual incita a las organizaciones estar a la vanguardia de las ultimas herramientas con respecto a la protección de datos y seguridad de la información.

1.6. Hipótesis

(H1) = Los fraudes informáticos inciden en los resultados económicos financieros de las empresas del sector industrial de la Provincia de Cotopaxi.

(H0) = Los fraudes informáticos no inciden en los resultados económicos financieros de las empresas del sector industrial de la Provincia de Cotopaxi.

1.7. Variables de la Investigación

1.7.1. Variable Independiente

- Fraude Informático

1.7.2. Variable Dependiente

- Vulnerabilidad de las empresas del sector industrial

1.7.3. Operacionalización de las Variables

Tabla 1

Operacionalización de las Variables

VARIABLE	Definición Conceptual	Dimensiones	Indicadores
Fraude Informático	La mayoría de los Delitos Informáticos se cometen a través de manipulación de información. El único tipo de Delito Informático que se puede salvar es el de espionaje, realizado por medio de la captación a distancia de ondas electromagnéticas producidas por el campo eléctrico de un monitor.	**-FRAUDES** *Tipos de Fraudes *Fraude Informático	-Diagnostico Financiero -Auditoría Informática -Auditoría Forense -Cuestionarios -Tendencias
Vulnerabilidad de las empresas del sector industrial	Se define como la incapacidad de comunicación de una comunidad para absorber mediante el auto ajuste, los efectos de un determinado cambio en su medio ambiente, su inflexibilidad o incapacidad para adaptarse a ese cambio, que para la comunidad constituye un riesgo. Ser vulnerable a un fenómeno natural es ser susceptible de sufrir daño y tener dificultad de recuperase de ello.	**-Vulnerabilidad** *Análisis de Vulnerabilidad de la empresas del sector industrial *Tipos de vulnerabilidades	-Diagnostico Financiero -Auditoría Informática -Auditoría Forense -Cuestionarios -Tendencias

CAPITULO II

2. MARCO TEÓRICO

2.1. Bases Teóricas

2.1.1. Empresa

Según Naranjo & Naranjo (2000) en su libro de Contabilidad Comercial y de Servicios mencionan que “La empresa es una unidad económica que actúa como factor dinámico en el proceso productivo de bienes o servicios, mediante la forma de una sociedad industrial, comercial o servicios, con el fin de obtener beneficios económicos y sociales” (pág. 1).

Podemos definir que una empresa u organización es aquella que está formada por un conjunto de recursos, humanos, tecnológicos, económicos-financieros y entre otros; los mismos que ayudan al desarrollo continuo de las operaciones dedicadas a la producción de bienes o servicios.

a) Análisis Estructural de la Empresa:

Tomando en cuenta las anteriores definiciones, se puede apreciar que la definición de empresa revela los siguientes elementos que componen la estructura básica de lo que es una empresa u organización:

Según el (Diccionario de la Lengua Española, de la Real Académica Española, 2006) manifiesta que “La estructura de una empresa debe estar compuesta de la siguiente manera”:

- **Entidad:** Es decir, que una empresa es una colectividad considerada como unidad (por ejemplo, una corporación, compañía, institución, etc., tomada como persona jurídica) o un ente individual conformado por una sola persona (por lo general, el propietario).

- **Elementos humanos:** Se refiere a que toda empresa está conformada por personas que trabajan y/o realizan inversiones para su desarrollo.
- **Aspiraciones:** Son las pretensiones o deseos por lograr algo que tienen las personas que conforman la empresa.
- **Realizaciones:** Se entiende como las satisfacciones que sienten los miembros de la empresa cuando logran cumplir aquello que aspiraban.
- **Bienes materiales:** Son todas las cosas materiales que posee la empresa, como; instalaciones, oficinas, mobiliario, etc.
- **Capacidad técnica:** Es el conjunto de conocimientos y habilidades que poseen los miembros de la empresa para realizar o ejecutar algo.
- **Capacidad financiera:** Se refiere a las posibilidades que tiene la empresa para realizar pagos e inversiones a corto, mediano y largo plazo para su desarrollo y crecimiento, además de tener liquidez y margen de utilidad de operaciones (por citar algunas).
- **Producción, transformación y/o prestación de servicios:** Se refiere a que la empresa puede realizar una o más de las siguientes actividades:
  Fabricar, elaborar o crear cosas o servicios con valor económico.
  Transformar o cambiar, por ejemplo, una materia prima en un producto terminado.
  Prestar servicios. (Thompson, 2012)

Satisfacción de necesidades y deseos:

> La necesidad humana es el estado en el que se siente la privación de algunos factores básicos (alimento, vestido, abrigo, seguridad, sentido de pertenencia, estimación). En cambio, los deseos consisten en anhelar los satisfactores específicos para éstas necesidades profundas (por ejemplo, una hamburguesa Mc Donalds para satisfacer la necesidad de alimento)". (Kotler, 2010, pág. 7).

En si se puede concluir que una organización o entidad empresarial permite a la generación y transformación de bienes y servicios para cubrir las múltiples necesidades de las personas y todo lo referente a la convivencia con la sociedad como por ejemplo la educación, salud, vestimenta, seguridad y entre otras necesidades que son muy esenciales para la supervivencia humana.

b) Gobierno Corporativo en la Empresas

> El Gobierno Corporativo es un proceso efectuado por el consejo de administración de una entidad, aplicable a la definición de estrategias en toda la empresa y diseñado para identificar eventos potenciales que puedan afectar a la organización, gestionar sus riesgos dentro del riesgo

> aceptado y proporcionar una seguridad razonable sobre el logro de los objetivos. (Ballester, sf, pág. 12)

Por lo que diríamos que un Gobierno corporativo es un conjunto de responsabilidades y prácticas ejecutadas por la junta directiva y la administración ejecutiva de la empresa con la finalidad de promover una dirección estratégica y garantizar que los objetivos planteados se cumplan y de esta manera los recursos de la organización que son usados de manera responsable.

Ibídem menciona que: "El Gobierno Corporativo incluye las siguientes capacidades, las cuales se detallan a continuación":

- Alinear el riesgo aceptado y la estrategia.
- Mejorar las decisiones de respuesta a los riesgos.
- Controlar el acceso a la información.
- Buscar estrategias de mejora.
- Reducir las sorpresas y pérdidas operativas.
- Identificar y gestionar la diversidad de riesgos para toda la entidad.
- Aprovechar las oportunidades.
- Reducir el riesgo.
- Mejorar la dotación de capital. (Ballester, sf, pág. 11).

c) Gobierno de TI

Según ISACA en un estudio realizado sobre los Objetivos de Control para Información y Tecnologías Relacionadas (COBIT4.1) (2007) en su revista de Governance Institute menciona que "Un gobierno de TI es responsabilidad de los ejecutivos, del consejo de directores y consta de liderazgo, estructuras y procesos organizacionales que garantizan que TI en la empresa sostenga y extienda las estrategias y objetivos organizacionales" (pág. 5)

Por lo tanto se puede señalar que el gobierno de TI es responsabilidad de los altos ejecutivos y del consejo de directores de la empresa, ya consta de liderazgo, estructuras y procesos organizacionales que garantizan que las Tecnologías de Información en las organizaciones ayuden a cumplir las metas y objetivos planteados para las diversas áreas o departamentos.

> El gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que TI en las organizaciones soporta los objetivos del negocio. De esta manera, el gobierno de TI facilita y ayuda que la empresa aproveche al máximo su información, maximizando así los beneficios, capitalizando las oportunidades y ganando ventajas competitivas. (ISACA, 2007, pág. 5)

d) Recursos de Ti

> La organización de TI se desempeña con respecto a estas metas como un conjunto de procesos definidos con claridad que utiliza las habilidades de las personas, y la infraestructura de tecnología para ejecutar aplicaciones automatizadas de negocio, mientras que al mismo tiempo toma ventaja de la información del negocio. Estos recursos, junto con los procesos, constituyen una arquitectura empresarial para TI. (ISACA, 2007, págs. 11-12)

Los recursos de TI son de vital importancia en una organización, debido a que ayudan a controlar todos los proceso o requerimientos que se realiza en un negocio, por esta razón se dice que estos recursos constituyen una arquitectura empresarial muy importante que ayuda a cumplir metas y objetivos propuestos a corto y largo plazo por la empresa.

Ibídem en su revista de Governance Institute menciona que “Los recursos de TI identificados se pueden definir como”:

- Las **aplicaciones:** incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.
- La **información:** son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.
- La **infraestructura:** es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.
- Las **personas** son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información en una organización. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran. (ISACA, 2007, pág. 12)

2.1.2. Tipos de Empresas

Según Naranjo & Naranjo (2000) en su libro de Contabilidad Comercial y de Servicios mencionan que las empresas se clasifican:

- De acuerdo a la Organización del Capital.
- Según el origen de su capital.
- De acuerdo a su tamaño.
- De acuerdo con la actividad que cumplan. (pág. 1).

a) De acuerdo a la Organización del Capital

Ibídem menciona que “Las empresas de acuerdo a la organización del capital se dividen en”: (pág. 2)

Compañía de responsabilidad limitada

> La compañía de responsabilidad limitada es la que se contrae entre dos o más personas, que solamente responden por las obligaciones sociales hasta el monto de sus aportaciones individuales y hacen el comercio bajo una razón social o denominación objetiva, a la que se añadirán, en todo caso, las palabras "Compañía Limitada" o su correspondiente abreviatura. Si se utilizare una denominación objetiva será una que no pueda confundirse con la de una compañía preexistente. Los términos comunes y los que sirven para determinar una clase de empresa, como "comercial", "industrial", "agrícola", "constructora", etc., no serán de uso exclusivo e irán acompañadas de una expresión peculiar. (Superintendencia de Compañias y Valores, 2014, pág. 29)

De acuerdo a la definición realizada por varios autores se puede señalar que este tipo de compañía está conformada por dos a más personas, que se comprometen a responder por sus obligaciones y aportaciones, también se puede ver que su capital estará representado por participaciones que podrán transferirse de acuerdo con lo que dispone la ley de compañías.

Compañía de economía Mixta

Según la Ley de Compañías (2014) en el Art. 308 en la sección VIII menciona que:

“El Estado, las municipalidades, los consejos provinciales y las entidades u organismos del sector público, podrán participar, conjuntamente con el capital privado, en el capital y en la gestión social de esta compañía. (pág. 92)

En si podemos decir que este tipo de compañías son aquellas que están encaminadas al desarrollo y fomento de la agricultura y de las diversas industrias convenientes a la economía de un país y su objetivo principal es la satisfacción de necesidades de orden colectivo.

Compañía de Nombre Colectivo

> La compañía en nombre colectivo se contrae entre dos o más personas naturales que hacen el comercio bajo una razón social. La razón social es la fórmula enunciativa de los nombres de todos los socios, o de algunos de ellos, con la agregación de las palabras "y compañía". Sólo los nombres de los socios pueden formar parte de la razón social. (Superintendencia de Compañias y Valores, 2014, pág. 16)

Este tipo de compañía es aquella que se forma entre dos o más personas que hacen el comercio bajo una razón social. Y el nombre de la compañía por general va con el nombre de todos los socios con la agregación de las palabras “y compañía”

Compañías o Sociedades Anónimas

Ibídem menciona que las compañías o sociedades anónimas son:

> Aquellas sociedades cuyo capital está dividido en acciones negociables, están formadas por la aportación de los accionistas que responden únicamente por el monto de sus acciones. Las sociedades o compañías civiles anónimas están sujetas a todas las reglas de las sociedades o compañías mercantiles anónimas. (2014, pág. 46)

Este tipo de compañías son aquellas que su capital está dividido en acciones negociables, ya que se encuentra formado por la aportación de los accionistas o socios que son aquellos responsables únicamente por el monto de sus acciones. También es muy importante recalcar que las compañías civiles anónimas están sujetas a todas las reglas de las sociedades o compañías mercantiles anónimas, todo esto de acuerdo a la legislación vigente para la constitución de sociedades.

Compañías en Comandita Simple

> La compañía en comandita simple existe bajo una razón social y se contrae entre uno o varios socios solidarios e ilimitadamente responsables y otro u otros, simples suministradores de fondos, llamados socios comanditarios, cuya responsabilidad se limita al monto de sus aportes. La razón social será, necesariamente, el nombre de uno o varios de los socios solidariamente responsables, al que se agregará siempre las palabras "compañía en comandita", escritas con todas sus letras o la abreviatura que comúnmente suele usarse. (Superintendencia de Compañias y Valores, 2014, pág. 22).

Este tipo de compañías son creadas bajo una razón social y pueden estar conformadas por uno o varios socios, solidaria e ilimitadamente responsables, siendo simples suministradores de fondos llamados socios comanditarios, por lo tanto cuya responsabilidad se limita al monto de sus aportes.

Compañías en Comandita por Acciones

> En este tipo de Compañía el capital de los socios se dividirá en acciones nominativas de un valor nominal que sea igual. La décima parte del capital social, por lo menos, debe ser aportada por los socios solidariamente responsables (comanditados), a quienes por sus acciones se entregarán certificados nominativos intransferibles. (Superintendencia de Compañias y Valores, 2014, pág. 91)

De acuerdo a las definiciones de la ley de compañías se puede decir como conclusión que en este tipo de compañía solamente las personas naturales podrán ser socios comanditados, y en cambio las personas jurídicas sí podrán ser socios comanditarios.

Compañía Holding o Tenedora de Acciones

> Es la que tiene por objeto la compra de acciones o participaciones de otras compañías, con la finalidad de vincularlas y ejercer su control a través de vínculos de propiedad accionaria, gestión, administración, responsabilidad crediticia o resultados y conformar así un grupo empresarial. (Superintendencia de Compañias y Valores, 2014, pág. 121)

Este tipo de compañías son aquellas que se encuentran vinculadas con otras compañías que elaborarán y mantienen estados financieros individuales por cada compañía, para fines de control y distribución de utilidades de los trabajadores y para el pago de los correspondientes impuestos fiscales.

b) Según el origen de su capital

Empresas privadas

Según Beas (1993) en su libro de Organización y Administración de Empresas, menciona que “la propiedad de su capital es de personas particulares ya se trate de personas físicas o de personas jurídicas” (pág. 3)

Por lo tanto se puede decir que este tipo de empresas están formadas por personas naturales o jurídicas que son inversionistas privados y su principal finalidad es lucrar de sus ventas en su totalidad, y el origen de capital es privado y de acuerdo al alcance de los dueños.

Ibídem menciona que “por su parte las empresas privadas suelen clasificarse en función de su constitución como aquellas empresas que se detalla a continuación”:

- **Empresas individuales**: son aquellas cuyo propietario es una persona física o individual.
- **Empresas societarias:** cuando son varias las personas, físicas, jurídicas o de ambas las que tratan de poner en común capital, trabajo, arte o industria con el fin de obtener un beneficio o lucro. (pág. 3)

Empresas Públicas

Ibídem considera que “la propiedad de su capital es exclusivamente del estado, ya se trate de la administración central, de las comunidades autónomas, de las provincias o de los municipios, o de sus organismos autónomos” (pág. 3).

Se trata de empresas donde su capital principal pertenece al estado, y en las que se pretende satisfacer las necesidades sociales del país. Pueden ser centralizadas, descentralizadas, estatales, mixtas y paraestatales, y no tiene fines de lucro.

Empresas Mixtas

Ibídem manifiesta que las empresas mixtas “son aquellas cuya propiedad de su capital pertenece al estado y a particulares, siempre y cuando la incidencia del capital público en la toma de decisiones, cualquiera fuera su participación en el total, determine limitaciones de cualquier clase” (pág. 3)

c) De Acuerdo a su Tamaño

No cabe la menor duda de que este criterio representa uno de los más discutidos, ya que existen diversos criterios y opiniones sobre la clasificación de las empresas. Uno de los criterios que podemos considerar es el tamaño de un negocio, el número de personas que componen su plantilla, a partir de esta premisa, surgen cuatro criterios de empresas que se enumera a continuación.

> Las MIPYMES en Ecuador tienen un enorme potencial para generar producción, empleo e ingresos y podrían constituirse en el motor del desarrollo del país, alcanzando mayores niveles de participación en el mercado internacional. La falta de información, asistencia técnica, capacitación, acceso a crédito y modernización, son algunos de los factores que han influenciado para que las MIPYMES no hayan podido expandir sus productos en el mercado internacional. Superar estos obstáculos requiere del apoyo decidido de las instituciones del sector público, cámaras y gremios de la producción y de las organizaciones de asistencia técnica internacional. (FLACSO, 2013, pág. 151)

Las medianas y pequeñas empresas día a día han presentado un crecimiento muy significativo con respecto a su producción y a la participación de los mercados nacionales e internacionales y siendo un pilar fundamental para el desarrollo económico y financiero de una provincia o quizá de un país en general.

Microempresa

Se puede aludir que una microempresa está comprendida por un grupo de personas que tienen pocos recursos. Pero en si esta creación pude ser el primer paso de un emprendedor a la hora de realizar su primer negocio para alcanzar un alto nivel empresarial.

> Una microempresa es un negocio que tiene un máximo aproximado de diez trabajadores en plantilla. Se trata de un micro negocio que puede ser administrado por un único profesional. Pese a que su nivel de facturación sea menor que el de otro tipo de negocios, conviene puntualizar que este tipo de proyectos tienen una gran influencia en la economía social al ser un medio de vida para los profesionales. Además, se trata de un tipo de negocio que puede tener potencial, es decir, una evolución de menos a más. (Nicuesa, 2016).

Pequeñas empresas

Las pequeñas empresas u organizaciones se puede decir que son entidades con alta predominación en el mercado del sector comercial, siendo muy pocas o quizá nada del sector industrial ya que estas requieren de grandes inversiones de negocios. Por lo tanto una empresa pequeña nunca podrá superar ciertas ventas anuales o una determinada cantidad de empleados.

> Las pequeñas empresas tienen un personal en plantilla de entre 11 y 49 trabajadores. Este tipo de negocio suele tener una tendencia de crecimiento más destacada que la de la microempresa. Además, en su estructura organizacional también cuenta con una división del trabajo. En

> muchos casos, las pequeñas empresas son negocios familiares. (Nicuesa, 2016).

Medianas empresas

Son aquellas empresas que se dedican por lo general a negocios vinculados a la prestación de servicios, diseñando programas y proyectos cuyo propósito principal sea el impulso de la creatividad e innovación de las necesidades del cliente para de esta manera satisfacer los bienes y servicios que produce. También es muy importante recalcar que este tipo de empresas tienen una gran acogida de los clientes potenciales y por ende tienen mayos ingresos económicos.

> En la clasificación de tipos de negocios en función del tamaño también encontramos los negocios medianos. Que ofrecen una mayor oferta de empleo al poder contratar entre 50 y 250 profesionales. Se trata de un tipo de empresa que tiene una mayor estructura a partir de departamentos diferenciados. Tanto las pequeñas como las medianas empresas tienen mucha fuerza en la economía. (Nicuesa, 2016).

Grandes empresas

Ibídem señala que “el número de personal en plantilla en las grandes empresas supera los 250 profesionales. Algunas empresas se desarrollan como multinacionales que tienen sede en distintos países del mundo. Se trata de negocios en expansión internacional. (Nicuesa, 2016)

Un criterio usual para poder diferenciar el tamaño de estas empresas es el número de trabajadores o también puede ser el monto de su capital que tiene cada una. Hay que observar que este criterio varía de un país a otro de acuerdo a las políticas de cada estado.

d) De acuerdo al con la actividad que cumplen

Según Naranjo & Naranjo (2000) en su libro de Contabilidad Comercial y de Servicios menciona que: “las empresas de acuerdo a la actividad que cumplen se dividen en los siguientes segmentos que se detalla a continuación” (pág. 14).

Empresa de Servicios

> Son aquellas empresas que prestan servicios profesionales y calificados para satisfacer las necesidades del ser humano a cambio de un determinado valor económico. Ejemplo, centros educativos particulares, centros infantiles, clínicas cooperativas de transporte, cooperativas de ahorro y créditos, consultorios médicos o jurídicos, centros de diversión nocturnos, casinos, casinos, entre otros. (Naranjo & Naranjo, 2000, pág. 14).

Son aquellas empresas como su nombre lo indica tiene la finalidad de prestar servicios como transporte, el turismo, recreación, asesoramiento, televisión por cable, hotelería, cultura, los espectáculos públicos, la educación, teatro, servicios de alimentación, entre otros, y satisfacer las necesidades de las personas.

Empresa Comercial

> Es aquella que se dedica a la compra y venta de mercaderías, se caracteriza por que no realiza ninguna transformación de los bienes, sino que lo comercializa a un precio mayor al de la compra, este margen se constituye en utilidad o ganancia. Ejemplo, almacenes de calzado, Farmacias, Supermercados, librerías, imprentas, centros comerciales. (Naranjo & Naranjo, 2000)

Se puede decir que este tipo de empresas como su nombre lo indica son aquellas que se dedican a la compra venta de los productos ya transformados, con la finalidad de realizar sus ventas con un porcentaje de utilidad, los mismos que servirán para el crecimiento de la empresa y el sustento del personal que labore en dicha empresa.

Empresa Industrial

Empresas del Sector Industrial

> Son entes contables dedicados a la transformación total o parcial de un artículo destinado a la venta para empresas comerciales, para este procesos es necesaria la utilización de los denominados medios de producción. Para saber el precio de venta se requiere determinar el costo total de producción y cargar un margen adecuado de utilidad. Ejemplo, fábricas textiles, fábricas de calzados, de licores, entre otros. (Naranjo & Naranjo, 2000)

Son aquellas empresas que se dedican a la transformación de la materia prima en productos elaborados, los mismos que serán distribuidos a otras empresas comerciales para realizar la distribución de los bienes transformados a los diferentes lugares del país, de manera directa al consumidor.

Extractivas. Son aquellas industrias que se dedican a la explotación de recursos naturales, ya sea renovable o no renovable. Ejemplos de este tipo de empresas son las pesqueras, madereras, mineras, petroleras, entre otras.

Manufactureras: Son aquellas empresas que tienen como finalidad primordial transforman la materia prima en materia elaborada, para el consumo de las personas y pueden ser:

- **De consumo final.** Son aquellas que producen bienes y servicios que satisfacen de manera directa las necesidades del consumidor. Por ejemplo: prendas de vestir, muebles, alimentos, aparatos eléctricos, bebidas, juegos electrónicos, entre otros.
- **De producción.** Estas satisfacen a las de consumo final. Ejemplo: maquinaria ligera, productos químicos, entre otros.

> El Ministerio de Industrias y Productividad (MIPRO) impulsa el desarrollo de la industria y la artesanía, para incentivar la inversión y la innovación para que los bienes y servicios que se produzcan en el país tengan mayor valor agregado y niveles convenientes de calidad, en armonía con el medio

> ambiente, para crear empleo de calidad y lograr que los productos conquisten los mercados nacionales e internacionales. (Ministerio de Coordinacion de la Produccion, Empleo y Competitividad, 2011, pág. 12).

La empresas industriales desempeñan un papel muy importante en la economía de un país, ya que su función principal es la de transformarla materia prima en materia elaborada, obteniendo productos y servicios de calidad que satisfacen las necesidades de las personas.

Actividades Productivas en el sector industrial de la Provincia de Cotopaxi

> Según la Encuesta de Manufacturas del año 2007, Cotopaxi, dentro de la Región 3, es la provincia de mayor producción industrial bruta de manufacturas, 339,8 millones de dólares, correspondiente a un consumo de materias primas de 203 millones de dólares, impuestos pagados de 31 millones de dólares, generación de empleo, 4.362 personas ocupadas, y sueldos y salarios pagados de 21, 5 millones de dólares. (Ministerio de Coordinacion de la Produccion, Empleo y Competitividad, 2011, pág. 21).

Según el Ministerio de Coordinación de la Producción, Empleo y Competitividad menciona que “en la provincia de Cotopaxi, están presentes las siguientes industrias las cuales se detallan a continuación”:

Tabla 2

Actividades de Manufactura según el CIIU

• Elaboración de productos de alimentos y bebidas (CIIU 15).
• Fabricación de prendas de vestir, adobo de y teñido de piel (CIIU 18).
• Curtido y adobo de cueros; fabricación de maletas, bolsos de mano (CIIU 19).
• Producción de madera y fabricación de productos de madera, corcho excepto muebles (CIIU 20).
• Fabricación de productos de papel (CIIU 21).

Fuente: (Ministerio de Coordinacion de la Produccion, Empleo y Competitividad, 2011)

e) Clasificación de las Empresas del Sector Industrial según el CIIU.

Según el Ministerio de Coordinación de la Producción, Empleo y Competitividad menciona “específicamente las principales actividades de manufactura, desglosadas a 6 dígitos según el CIIU” (pág. 22).

Como se muestra en la Tabla 3 existe una codificación de 6 dígitos que diferencia a cada una de las actividades que desempeñan las diversas entidades del sector objeto de estudio, donde se caracterizan actividades dedicadas a la producción de alimentos, bebidas, prendas de vestir, artículos de uso doméstico, entre otros; siendo un factor clave en el desarrollo de la provincia.

Tabla 3

Actividades Manufactureras desglosadas en 6 dígitos CIIU

CIIU	Descripción
Total 151112	Elaboración de embutidos: jamón, salchichas, mortadela, chorizo, etc.

Total 151329	Elaboración y conservación de otros preparados de hortalizas, mediante desecación, entre otros.
Total 152001	Pasteurización, homogeneización, preconización o maternización de la leche y envasado en cualquier tipo de envase.
Total 153103	Producción de harinas, sémolas y gránulos de cereales de: trigo, centeno, avena, maíz y otros cereales.
Total 155402	Embotellado de aguas minerales o de manantial, purificadas o artificiales.
Total 181000	Fabricación de prendas de vestir para hombres, mujeres, niños y bebes: ropa exterior, interior, de dormir; ropa de diario y de etiqueta, ropa de trabajo (uniformes) y para practicar deportes (calentadores, buzos de arquero, pantalonetas, etc.).
Total 191103	3 producciones de cueros curtidos o adobados vegetales, mineral o químicamente (rusos, tafilete).
Total 202101	Fabricación de madera terciada, tableros de madera enchapada, tableros de partículas y de fibra y productos similares de madera laminada etc.
Total 202909	Fabricación de otros artículos de madera: palillos, paletas para helados, pinchos, baja lenguas, ataúdes, etc.

Continúa 

Total 210910	Fabricación de pañuelos, pañolitos faciales, papel higiénico, toallas, servilletas, pañales y forros de pañales para bebés, tampones, toallas higiénicas, etc.
Total 252012	Fabricación de artículos de plástico para obras de construcción: puertas, ventanas, marcos, postigos, persianas, etc.
Total 252015	Fabricación de envases de plástico: bolsas, sacos, cajones, garrafones, botellas, tanques, etc.
Total 271012	Fabricación de tubos, caños y perfiles huecos (fundidos, soldados o remachados) y acero hueco para minas.
Total 272012	Fundición, refinación y aleaciones de metales comunes no ferrosos tales como: cobre, plomo, cromo, manganeso, zinc, aluminio, níquel, estaño, etc.

Total 281102	Fabricación de carpintería metálica: balcones, escaleras, incluso de incendio, persianas, postigos, rejas, puertas (incluso enrollables), ventanas y sus marcos de hierro, acero o aluminio.
Total 289109	Otros trabajos de metal forjado, prensado, estampado y laminado
Total 289903	Fabricación de productos de tornillería: tuercas, pernos, tornillos y partes de productos de tornillería sin rosca.

Fuente: (Ministerio de Coordinacion de la Produccion, Empleo y Competitividad, 2011)**.**

Según el Ministerio de Coordinación de la Producción, Empleo y Competitividad menciona que "existe cinco principales actividades de manufactura de las 17 identificadas en la provincia de Cotopaxi, priorizadas por su aporte en la generación de empleo, sueldos pagados, valor de la producción, valor de materia prima e impuestos pagados" (pág. 23).

A continuación se detalla las cinco actividades más importantes de las empresas manufactureras de la provincia de Cotopaxi:

- La principal actividad de manufactura, puesto uno del ranking, es de la rama metalmecánica, más específicamente es "fabricación de tubos, caños y perfiles huecos (fundidos, soldados o remachados) y acero hueco para minas", industria con la mayor producción bruta de la provincia, 104 millones de dólares, con el mayor consumo de materia prima y materiales auxiliares, 72,7 millones de dólares, la que más impuestos paga de la provincia, 11,6 millones de dólares, la tercera de la provincia en cuanto a generación de empleo, 610 personas ocupadas en esta actividad, la tercera en monto de sueldos y salarios pagados, 3,4 millones de dólares.
- La segunda actividad principal de manufactura en la provincia de Cotopaxi, es de la rama productora de papel, específicamente es "fabricación de pañuelos, pañolitos faciales, papel higiénico, toallas, servilletas, pañales y forros de pañales para bebés, tampones, toallas higiénicas, etc.", la primera industria respecto de las demás de la provincia en sueldos y salarios pagados, 4,3 millones de dólares, la segunda en generación de empleo, 718 personas ocupadas, la segunda de la provincia en cuanto a pago de impuestos, 8,1 millones de dólares, la tercera en producción bruta de artículos para la venta, 40,4 millones de dólares, y la quinta industria en consumo de materias primas y materiales auxiliares, 16,6 millones de dólares.

- La tercera actividad principal de manufactura en la provincia, es de la industria maderera, más específicamente “fabricación de madera terciada, tableros de madera enchapada, tableros de partículas y de fibra y productos similares de madera laminada etc.”, industria que es la segunda de la provincia en cuanto a valor bruto de la producción, 57,7 millones de dólares, pero es la cuarta en consumo de materias primas y materiales auxiliares, 18,5 millones de dólares, la cuarta en pago de impuestos, 3,3 millones de dólares, la cuarta respecto de las demás de la provincia en generación de empleo, 483 personas ocupadas, y la cuarta en sueldos y salarios pagados, 2,8 millones de dólares.
- La cuarta principal actividad de la provincia, pertenece a la rama metalmecánica, específicamente “fundición, refinación y aleaciones de metales comunes no ferrosos tales como: cobre, plomo, cromo, manganeso, zinc, aluminio, níquel, estaño, etc.”, industria que respecto a las demás de la provincia es la segunda consumidora de materias primas, 30,5 millones de dólares, la tercera industria en cuanto a pago de impuestos, 3,5 millones de dólares, la cuarta en producción bruta de artículos para la venta, 37,6 millones de dólares, la sexta en sueldos y salarios pagados, 1,4 millones de dólares, y la octava industria de la provincia en generación de empleo, 236 personas ocupadas.
- Finalmente, la quinta principal actividad industrial de la provincia, es de la industria de alimentos y bebidas, más específicamente “elaboración y conservación de otros preparados de hortalizas, mediante desecación, inmersión en aceite o vinagre, etc.”, actividad que es la primera generadora de empleo industrial en la provincia, 1.029 personas ocupadas, la segunda en cuanto a sueldos y salarios pagados, 4,3 millones de dólares, la quinta actividad industrial en producción bruta para la venta, 30,9 millones de dólares, la sexta en consumo de materias primas, 14,4 millones de dólares, y la catorceava actividad de la provincia generadora de recursos para el estado, 71,6 miles de dólares. (Ministerio de Coordinacion de la Produccion, Empleo y Competitividad, 2011).

Luego de haber revisado las cinco principales actividades de las empresas del sector industrial de la Provincia de Cotopaxi, se puede concluir que existen diversas ramas de producción, donde se obtiene una diversidad de productos que son consumidos a nivel nacional y a nivel internacional, los cuales están conformados como productos de primera necesidad para el consumo humano y los otros que son alternativos.

2.1.3. Finanzas

Cada vez es más complicado definir en un solo concepto el término “finanzas”. Ya que hoy día se habla de finanzas prácticamente en todos los medios de comunicación de todo el mundo; existen diarios especializados en noticias financieras, los noticiarios de radio y televisión tienen secciones dedicadas a informar sobre las principales variables económicas y financieras, y abundan las revistas que tratan de tópicos de inversiones y finanzas. Ahora también en las redes sociales como es, el Facebook, Twitter, YouTube y otras aplicaciones sociales.

Según García (2014) en su libro titulado Introducción a las Finanzas define “A las finanzas como el conjunto de actividades mercantiles relacionadas con el dinero de los negocios, de la banca y de la bolsa; y como el grupo de mercados o instituciones financieras de ámbito nacional o internacional” (pág. 1)

> Para la mayoría de las personas las finanzas se perciben como algo complejo, poco accesible y que solo es manejado por los estudiosos; en realidad, estas pueden ser tan sencillas, interesantes y útiles si se cuenta con los conocimientos financieros esenciales. Como toda materia especializada, las finanzas tienen principios básicos y fundamentales; tal vez el más profundo sea la transferencia de dinero de quien lo tiene a quien no lo tiene. Los que poseen dinero están buscando ganar rendimientos y los que no cuentan con él están dispuestos a pagar un precio por obtenerlo y utilizarlo. Las relaciones y actividades generadas por este intercambio de recursos son parte importante de las finanzas. (García, 2014, pág. 1)

Por lo tanto se puede exponer que las finanzas están vinculadas con varias disciplinas, y se le considera como una rama de la economía que se dedica al estudio de la obtención de capital para la inversión en bienes productivos y de las decisiones de inversión de los ahorradores. Está relacionado con las transacciones y con la administración del dinero de las organizaciones públicas o privadas.

2.1.4. Finanzas Corporativas

Según Díaz et al., (2009) en el libro Finanzas Corporativas en la Práctica alude que “Las finanzas corporativas están íntimamente relacionadas con la información contable ya que estas reflejan los efectos de las decisiones pasadas y presentes de la empresa y a partir de ellas se pueden estimar las consecuencias de las decisiones futuras” (pág. 15)

> Por lo tanto cuando una empresa recibe dinero en préstamo por parte de una institución Financiera la empresa se convierte en el emisor y la Institución Financiera en el inversionista. Si recibe dinero de los socios, la empresa “emite” acciones y los individuos son los tenedores de estas, es decir, los inversionistas. En cambio, cuando la empresa “invierte” sus excedentes de tesorería en una cuenta o instrumento bancario, la empresa es el inversionista y el banco el emisor el encargado de resguardar el dinero. (García, 2014, pág. 4)

En si se puede señalar que las finanzas corporativas en una organización es de vital importancia puesto que está relacionada con cada uno de los procesos contables y financieros que realiza la empresa a diaria, también le permite al gerente tomar dediciones a corto o largo plazo.

2.1.5. Economía

> Economía es la rama que analiza cómo los seres humanos satisfacen sus necesidades ilimitadas con recursos escasos que tienen diferentes usos. Cuando un hombre decide utilizar un recurso para la producción de cierto bien o servicio, asume el costo de no poder usarlo para la producción de otro distinto. A esto se lo denomina costo de oportunidad. La función de la economía es aportar criterios racionales para que la asignación de recursos sea lo más eficiente posible. (García, 2014, pág. 14).

En si se podría indicar que la economía busca satisfacer las necesidades humanas que se presentan mediante la producción y distribución de los recursos encaminados al consumo proporcionando la satisfacción de las necesidades del ser humanas.

> Para Adam Smith La economía está naturalmente ordenada a conseguir el aumento de la riqueza, y no se plantea la posibilidad de que ésta se ponga al servicio de otros fines, como el que todos los seres humanos dispongan de los bienes necesarios para vivir decentemente o que la riqueza producida se distribuya justamente. Nada en la naturaleza de la economía exige que se plantee como único o principal objetivo la producción ilimitada de riqueza. Decidir el objetivo último de la economía no pertenece sólo a la propia economía, sino también a la ética o a la política, y ya vimos como los griegos, por ejemplo, rechazaban la idea de que el fin último de la economía fuera aumentar las riquezas. (Paradinas, sf, pág. 14).

De acuerdo a la definición propuesta por Adam Smith podemos concluir que el ser humano tiene un criterio económico impulsado por el propio interés de satisfacer sus deseos personales, lo cual le ayudara a tener una mejor condición de vida.

Según Miller (2002) en su libro Economía Hoy mención que “la economía es el estudio de como las personas distribuyen sus recursos limitados a fin de satisfacer sus deseos limitados. Como tal, la economía estudia la manera como las personas eligen” (pág. 5).

> Por lo tanto este mismo autor menciona que la economía forma parte de las ciencias sociales analizan el comportamiento humano, a diferencia de las ciencias físicas que, por lo general, analizan el comportamiento de los electrones, los átomos y otros fenómenos no humanos. (Miller, 2002, pág. 5).

Dentro de la teoría de Miller (2002) considera dos tipos de análisis económico como es la microeconomía y la macroeconomía que se detallan a continuación:

a) Microeconomía

Ibídem considera que “La microeconomía es la parte del análisis económico que estudia la toma de decisiones adoptadas por el individuo (o las familias) y las empresas. Es como observar a través de un microscopio para concentrarse en las partes de la economía” (pág. 5)

b) Macroeconomía

> Es la parte del análisis económico que estudia el comportamiento de la economía en su totalidad. Y por lo tanto tiene que ver con los fenómenos globales de la economía como los cambios registrados en el desempleo, el nivel general de precios y el ingreso nacional. (Miller, 2002, pág. 5).

En general como conclusión se dice que la economía es una sola, aunque la realidad económica pude ser estudiada por diversos medios como son los análisis macroeconómicos y microeconómico.

2.1.6. Economía Sostenible

Según Bermejo (2005) en su libro de La gran Transición hacia la Sostenibilidad menciona que "Una economía sostenible puede crecer aumentando la productividad de una entidad de recursos que no agota los stocks existentes, así obtiene más servicios de sus recursos, es decir más producto económico" (pág. 39).

Por lo tanto se puede señalar que una economía es sostenible cuando alcanza un nivel máximo y mínimo de utilización de sus recursos, humanos, materiales, tecnológicos, económicos, entre otros, y de diversas emisiones compatibles, con el propósito que el resto de economías alcancen el mismo nivel sin degradar la naturaleza, y se evolucione a partir de la misma preservando su base propia.

Agenda 2030 y los Objetivos de Desarrollo Sostenible

Dentro de la Agenda 2030 y los Objetivos de Desarrollo Sostenible una Oportunidad para América Latina y el Caribe podemos mencionar unos de los objetivos que concuerdan con la investigación de la economía y el desarrollo sostenible y como está influye dentro de un país, y en la economía en cada una de las empresas, para de esa manera poder proyectarse hacia un futuro mejor y mayores posibilidades de participación e inclusión económica y productiva.

La presente investigación está ligada con uno de los objetivos que se toma en cuenta dentro de la Agenda 2030 es el Nº 9, el cual tiene como finalidad construir infraestructuras recipientes, promover la industrialización inclusiva y sostenible y fomentar la innovación.

> Las inversiones en infraestructura (transporte, riego, energía y tecnología de la información y las comunicaciones) son fundamentales para lograr el desarrollo sostenible y empoderar a las comunidades en numerosos países. Además de la financiación gubernamental y la asistencia oficial para el desarrollo, se está promoviendo la financiación del sector privado para los países que necesitan apoyo financiero, tecnológico y técnico. (Organizacion de las Naciones Unidas, sf).

Dentro de este objetivo se deslindan metas en las cuales destaca la meta 9.5 y dentro de esta se encuentran actividades que ayudan de manera inclusiva al desarrollo tecnológico y económico.

Meta Nº 9.5

> Aumentar la investigación científica y mejorar la capacidad tecnológica de los sectores industriales de todos los países, en particular los países en desarrollo entre otras cosas fomentando la innovación y aumentando considerablemente, de aquí a 2030, el número de personas que trabajan en investigación y desarrollo por millón de habitantes y los gastos de los sectores público y privado en investigación y desarrollo. (Organizacion de las Naciones Unidas, sf)

a) Facilitar el desarrollo de infraestructuras sostenibles y resilientes en los países en desarrollo mediante un mayor apoyo financiero, tecnológico y técnico a los países africanos, los países menos adelantados, los países en desarrollo sin litoral y los pequeños Estados insulares en desarrollo.
b) Apoyar el desarrollo de tecnologías, la investigación y la innovación nacionales en los países en desarrollo, incluso garantizando un entorno normativo propicio a la diversificación industrial y la adición de valor a los productos básicos, entre otras cosas.
c) Aumentar significativamente el acceso a la tecnología de la información y las comunicaciones y esforzarse por proporcionar acceso universal y asequible a Internet en los países menos adelantados de aquí a 2020. (Organizacion de las Naciones Unidas, sf).

2.1.7. Economía Empresarial

Según Méndez (2012) en su libro de Economía de la Empresa menciona que “la economía empresarial se sigue basando en los mecanismos tradicionales como es, acumulación privada de capitales, protección estatal, penetración de inversiones extranjeras y producción de bienes de consumo intermedios y de capital” (pág. 71)

Por lo tanto se puede decir que la economía empresarial en las naciones de Latino América corresponde al avance y desarrollo de la economía en su conjunto, de esta manera el mayor desenvolvimiento empresarial se ubica en diversos pases como es Argentina, México Brasil y Venezuela, en tanto que Bolivia Uruguay y Colombia y Paraguay presentan un menor grado de avance en la economía empresarial.

2.1.8. Economía digital

> La economía digital es un sector de la economía que incluye los bienes y servicios en los que su desarrollo, producción, venta o aprovisionamiento dependen de forma crítica de las tecnologías digitales. Está compuesta por cuatro subsectores: infraestructuras y aplicaciones, por un lado; y comercio electrónico y nuevos intermediarios, por otro. El objetivo del presente trabajo es explicar qué se entiende por economía digital e identificar sus componentes, así como su impacto en la empresa. Además, se realiza una aproximación a su análisis en el contexto español, considerando sus diferentes sectores. (Del Aguila, Padilla, Serarols, & Veciana, 2001, pág. 5)

Por lo tanto se expresaría que las empresas que hoy en día quieran conseguir una ventaja competitiva sostenible en el mundo entero mediante el uso de tecnologías de información y comunicación deberán tener presente los aspectos que la literatura estratégica ha formulado, sólo a través dos formas: eficacia operativa, haciendo las mismas cosas que tus competidores pero haciéndolas mejor; o mediante un posicionamiento estratégico de tal forma que hagas las cosas de manera diferente a tus competidores y que los clientes incrementen su valor por la misma.

Por esta razón las empresas, ahora más que nunca deben posicionarse en el mercado teniendo en cuenta esta nueva tecnología, como es Internet, y aprovechar las ventajas que brinda o puede brindar al sistema de valor.

2.1.9. Economía de la Información

Ibídem menciona que uno de los problemas fundamentales en la economía de la información es la disyuntiva entre regalar información para hacer saber a la gente lo que les estamos ofreciendo, y cobrar por ella para poder recuperar los costes. (Del Aguila, Padilla, Serarols, & Veciana, 2001).

La economía de la información presenta una tendencia muy significativa en las redes sociales donde las empresas o personas tratan de expandir su información de alguna actividad o servicio que ofertan a domicilio.

2.1.10. Tecnología de información y Comunicación (TIC)

Las tecnologías de la información y comunicación (TIC) son un factor de vital importancia en la transformación de la economía global y en los ligeros cambios que se presenta en el mundo entero. Ya que en los últimos tiempos, las nuevas herramientas tecnológicas de información y comunicación han obtenido un cambio muy significativo de manera que los individuos se comunican e interactúan de manera muy fácil en el ámbito de los negocios, y por esta razón se pude mencionar que la tecnología provoca cambios imprevisibles en las diversas organizaciones como son industriales, agricultura, ganadería, pesqueras, petroleras, mineras, entré otros campos.

> Son aquellas que desempeñan un papel clave en la generación de valor, ya que son relevantes en el ensamble de las redes de los proveedores, los sistemas de administración de relaciones con los clientes (CRM), los sistemas de administración de cadenas de suministros (SMC). (Scheel, 2011, pág. 53)

En general, las tecnologías de Información y comunicación son un factor fundamental para crear las condiciones en donde el valor de la información se

genera, se difunde y se potencia en forma efectiva y directa a todos los niveles tecnológicos.

2.1.11. Tecnologías de Información e Innovación

> Los procesos de globalización y la importancia que han adquirido las tecnologías de información e Innovación en el mercado mundial, radica en gran medida, en la convergencia de distintas áreas de la vida social y económica. Lo que usualmente eran cuatro industrias separadas que operaban independientemente (computación, comunicaciones, consumo electrónico y contenido) ahora son parte de una misma área, la más poderosa e influyente del momento, que determina radicalmente los flujos de información y los procesos de comunicación: la industria de la información y la comunicación. (Betancourt, 2004, pág. 3)

El impacto que este fenómeno tiene en las distintas esferas de la vida social se traduce, especialmente en los países más desarrollados del mundo, en una agudización de las condiciones de pobreza, en la exacerbación y ampliación de las brechas sociales, entre ellas, la llamada brecha digital, que no es sino reflejo y extensión de las brechas estructurales existentes.

Las Tecnologías de la Información e Innovación hoy en día pueden reducir la pobreza humana facilitando el acceso a las aplicaciones y servicios de salud, gobierno, educación etc. Las TIC también pueden ayudar a los productores a conectarlos con los mercados internacionales de manera fácil y oportuna.

2.2. Fraude

Según Estupiñan (2006) en su libro de Control Interno y Fraudes define al fraude como: “despojar mediante engaño, ya sea a una persona natural o jurídica, dentro de las menciones que se relacionan con los llamados delitos de cuello blanco son referidos a las defraudaciones que se han hecho a los entes corporativos” (pág. 257).

Ibídem menciona que “el fraude se divide en dos categorías las cuales se detalla a continuación”:

- Adueñarse de fondos (efectivo o valores) o activos de la empresa.
- La declaración falsa de la situación financiera de la empresa (omisión de operaciones, registros falsos manipulación de los registros contables del ente económico). (pág. 257)

Por lo tanto es importante mencionar que cualquier empresa está expuesta a diferentes tipos de riesgos o fraudes informáticos que se presentan a diario en sus actividades, en consecuencia a esto se debe exigir mucha responsabilidad a la parte directiva, comprometiéndose a mitigar profesionalmente los riesgos que se presente en la organización.

También es muy importante recalcar que existen algunos indicadores, herramientas de evaluación métodos y técnicas cuantitativas con respecto a fraudes para lo cual se debe tener en cuenta al momento de realizar una investigación forense encontrando indicios para contrarrestarlos durante la ejecución y posterior monitorización.

2.2.1. Tipos de Fraude

Dentro de los tipos de fraude existe una gran variedad de irregularidades, actos delictivos, actos ilegales para de esa forma engañar o entregar una información falsa o ilegal.

El Marco Internacional para la Práctica Profesional del Instituto de Auditores Internos definen el fraude como:

> Cualquier acto ilegal caracterizado por engaño, ocultación o violación de confianza. Estos actos no requieren la aplicación de amenaza de violencia o de fuerza física. Los fraudes son perpetrados por individuos y por organizaciones para obtener dinero, bienes o servicios, para evitar pagos o pérdidas de servicios, o para asegurarse ventajas personales o de negocio. (Frett, 2014)

Dentro de los tipos de fraudes más comunes se incluyen 14 que se detallan a continuación:

- Malversación de activos que involucra el robo de efectivo o activos (suministros, inventarios, equipos e información) de la organización. En muchos casos, el perpetrador intenta ocultar el robo, usualmente incorporando ajustes en los registros.
- El descremado (skimming, en inglés) se produce cuando el efectivo de una organización es robado antes de ser registrado en los libros y registros de la organización. Por ejemplo, un empleado acepta el pago de un cliente, pero no registra la venta.
- El fraude por reembolso de gastos se produce cuando a un empleado se le paga por gastos ficticios o inflados. Por ejemplo, un empleado presenta un informe de gastos fraudulento y reclama reembolso por viajes personales, alimentos inexistentes, kilometraje extra, etc.
- El fraude por rol de pagos ocurre cuando quien comete el fraude hace que la organización emita un pago luego de presentar reclamos falsos por compensación. Por ejemplo, un empleado reclama trabajo durante horas extras en las que no ha trabajado o un empleado añade empleados fantasmas al rol de pago y recibe el respectivo cheque de pago.
- El fraude de estados financieros involucra la inclusión de información falsa como parte de los estados financieros, por lo general sobreestimando los activos o ingresos o subestimando pasivos y gastos. El fraude de estados financieros es generalmente perpetrado por los gerentes de una organización quienes buscan afianzar la imagen económica de la misma. Miembros de la gerencia podrían beneficiarse directamente del fraude al vender acciones, recibir bonos de desempeño, o al utilizar el reporte falso para ocultar otro fraude.
- El fraude de desembolso se produce cuando una persona hace que la organización emita un pago por bienes o servicios ficticios, facturas infladas o facturas por compras personales. Por ejemplo, un empleado puede crear una compañía cascarón / de fachada (Shell Company, en inglés) y luego facturar al empleador por servicios inexistentes.
- La presentación de información falsa involucra la inclusión de información adulterada, usualmente para quienes están fuera de la organización. Más frecuentemente estos fraudes involucran estados financieros fraudulentos, aunque también puede ocurrir que se falsifique la información utilizada como medición de desempeño.
- Corrupción es el mal uso del poder confiado, para lucro personal. La corrupción incluye soborno y demás usos impropios del poder. La corrupción constituye con frecuencia un fraude fuera de libros, significando esto que existe escasa evidencia disponible en los estados financieros para probar que el delito ha sido cometido. Los empleados corruptos no tienen que cambiar fraudulentamente los estados financieros para encubrir sus delitos, simplemente reciben pagos en efectivo bajo la mesa.
- El soborno es el ofrecimiento, suministro, aceptación o solicitud de cualquier cosa de valor para influir en el resultado. Los sobornos pueden ser ofrecidos a empleados clave o gerentes tales como agentes de compras quienes cuentan con discreción para adjudicar compras a

vendedores. En el caso típico, un agente de compras acepta beneficios para favorecer a un vendedor externo en la compra de bienes o servicios.

- Un conflicto de interés se da cuando un empleado, gerente o ejecutivo de una organización tiene un interés personal y económico no divulgado dentro de una transacción que perjudica a la organización o a los intereses de sus accionistas.
- Una desviación es el acto de desviar una transacción potencialmente rentable, que normalmente generaría utilidades para la organización, hacia un empleado o hacia una tercera parte externa.
- El uso no autorizado o ilegal o el robo de información confidencial y de propiedad de la organización para beneficiar equivocadamente a alguien.
- Actividad entre partes relacionadas constituye una situación en donde una de las partes recibe de la otra relacionada algún beneficio que no se obtendría en una transacción de negocios normal y justa.
- La evasión de impuestos constituye un reporte intencional de información falsa en una declaración de impuestos con el fin de disminuir los impuestos que se adeudan. (Frett, 2014).

2.2.2. Fraude Informático

Según Gutiérrez (1991) en su artículo de investigación sobre el Fraude Informático y Estafa menciona que “la mayoría los fraudes informáticos conocidos por los tribunales y que han transcendido a la opinión publica tuvieron lugar en los Estados Unidos o involucraron de algún modo, a entidades, institucionales o empresas norteamericanos” (pág. 82).

a) Origen y Evolución del Fraude Informático

El origen del Fraude Informático se remonta desde mucho tiempo atrás con la iniciación de la guerras mundiales tanto la primera como la segunda guerra mundial, donde ya se empezaba haber indicios de violación o intromisión a los sistemas de los ejércitos armados con el afán de conocer sus estrategias sus táctica militares y de esa forma apropiarse de dicha información.

b) Definición del Fraude Informático

En si el fraude informático se da cuando el individuo procede al ingreso de datos de manera ilegal, para lo cual el ciberdelincuente debe tener un alto nivel

acerca de los conocimientos informáticos, llevando a suponer que el mismo puede ser un empleado de una organización que tiene acceso a los sistemas o redes de información, donde se puede ingresar y alterar los datos de esta manera beneficiando información relevante para el delincuente y afectando de manera directa a las actividades de la organización.

> El fraude Informático es conocido como un acto deliberado e ilegitimo que causa perjuicio patrimonial a una persona provocando un beneficio económico al cibercriminal o a una tercera persona, mediante la introducción, alteración, borrado o supresión de datos informáticos o cualquier interferencia en el normal funcionamiento de un sistema informático. (Chungata, 2015, pág. 29).

Con respecto al fraude informático se puede expresar que simplemente no se trata de una estafa cualquiera sino de una apropiación ilícita de información confidencial de una persona física u organización ya que cuando la manipulación fraudulenta de datos tiene lugar dentro un sistema informático autorizado, el proceso en sus diversas fases es muy susceptible a la captación o manipulación de registros existentes en las diversas áreas de una organización

c) Análisis de los tipos de incidentes de Seguridad de la Información en el Ecuador.

Según el Centro de respuesta a incidentes informáticos en el Ecuador: nos enumera “Los siguientes casos de delitos informáticos o incidentes más comunes que se presentan a continuación” (ECUCERT, 2017).

- **Fraude IP-PBX:** Las amenazas específicas del VoIP son muy distintas a las amenazas de datos y requieren soluciones únicas sofisticadas para evitar que los piratas informáticos realicen ataques maliciosos que puedan tener como resultado denegaciones de servicios (DoS), llamados de larga distancia no autorizada y robo de información confidencial.
- **Phishing:** Es una técnica de ingeniería social que emplea el envío masivo de correos electrónicos spam en nombre de alguna entidad con la finalidad de obtener datos personales y financieros (principalmente aquellos asociados a claves de acceso).
- **Open Proxy:** Es un mecanismo que funciona como pasarela web y permite hacer de puente entre nuestro navegador y el servidor al que

queremos conectar. Estos tipos de herramienta son utilizados en campañas para restringir el contenido que se puede visitar.

- **BotNet:** Es un grupo de computadoras comprometidas a través de bots, estos son programas de softwares que permiten tomar el control remoto de la PC de una víctima desprevenida. Se le conoce a la PC comprometida de esta manera como PC zombi.
- **Defacement:** Es un término usado en informática para hacer referencia a la deformación o cambio producido de manera intencionada en una página web por un atacante que haya obtenido algún tipo de acceso a ella, bien por algún error de programación de la página, por algún bug en el propio servidor o por una mala administración de este.
- **Fraudes en redes sociales:** Las nuevas tecnologías han logrado cambiar la forma de relacionarse entre las personas, pero también han cambiado la forma de cometer delitos. Hoy los delincuentes utilizan correos electrónicos, mensajes de voz, etc., para llevar adelante fraudes. (ECUCERT, 2017)

El fraude electrónico es la amenaza más peligrosa que enfrentan los internautas, y se da a través de un virus, que una vez ingresado a la computadora, altera el funcionamiento bloqueando el acceso a redes, dañando archivos, etc. Así, a través de mensajes, imágenes, o solicitud de actualización de datos o información, se logra robar claves, tarjetas de crédito, etc.

d) Fraude Informático en las Empresas

> Un 75% de todos los fraudes cometidos contra una empresa son perpetrados por su propio personal, de ahí que la prevención es preferible y menos costosa que los remedios. Como consecuencia la introducción de buenas medidas preventivas es esencial para que esta empresa combata esta amenaza con éxito. (Cano & Lugo, 2008, pág. 82)

Para poder combatir eficazmente el fraude informático en las empresas se ven obligados a crear diversas estrategias y lineamientos de control que puedan resguardar en caso necesario, ya que para ello existen leyes que brindan respaldos adecuados para la protección de información.

Todas las empresas ya sean nacionales o internacionales hoy en día han visto la necesidad de realizar actividades de prevención contra ciberataques con la finalidad de evitar los fraudes informáticos en cada uno de sus departamentos,

especialmente en la área de TIC y el departamento financiero, cuyas actividades a nuestro criterio personal serán detalladas a continuación.

- Revisión periódicamente los antecedentes del personal.
- Mejora de la comunicación y el clima laboral, con la de evitar el fraude como forma de compensación de injusticias laborales.
- Instalar monitores de circuito cerrado en cada uno de los departamentos.
- Restringir el acceso a computadoras, archivos y áreas clasificadas
- Elaborar convenios de confidencialidad y no competencia.
- Capacitar al personal constantemente para saber lo que debe hacer en caso de estar ante un fraude o robo en la empresa.
- Establecer políticas internas en cuanto al uso de información confidencial y las consecuencias jurídicas aplicables en caso de no cumplir con dichas políticas.

e) Delitos Informáticos más comunes

a.1 Phishing

> El método más común es el Phishing ya que 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. (Guerrero, 2012, pág. 23).

A esta modalidad se la conoce también como estafa ya que cuyo objetivo es conseguir la mayor cantidad posible de datos de información de los bancos donde se encuentra información importante de empresas multinacionales, nacionales y de personas comunes, con la finalidad de utilizar inadecuadamente al momento de realizar los fraudes financieros.

b.1 Pharming

Se puede decir que esta es una variante del Phishing, ya que cuyos objetivos son los mismos el robo de identidad y la obtención de los datos bancarios del afectado utilizando la navegación por internet a través de páginas usuales como google transmitiendo virus que direccionen de manera inmediata a los servidores de los atacantes.

> Básicamente consiste en la manipulación del servicio de los 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 dirige a otra exactamente igual, pero completamente falsa. (Guerrero, 2012, pág. 31).

En conclusión podemos mencionar que este tipo de delito informático tiene una finalidad muy común a la del Phishing que es el robo de información confidencial de las personas u organizaciones, mediante la manipulación de los navegadores web de las diversas páginas informáticas.

c.1 Phishing CAR

Este tipo de delito está encaminado en publicaciones de productos o servicios de calidad a bajos costos mediante diversas redes sociales.

> Esta es una modalidad que consiste en la publicación, en diferentes medios de la red, de anuncios de ventas de vehículos de alta gama o precios muy por debajo del mercado, se trata habitualmente de ofertas irresistibles, combinando pocos kilómetros, perfecto estado y equipamientos de lujo. (Guerrero, 2012, pág. 34).

Se puede decir que este tipo de delito informático hoy en día está de moda, debido al gran avance de la tecnología y gracias a la facilidad del acceso al internet, donde se encuentra constantemente publicaciones de personas desconocidas, en las cuales ofrecen productos o servicios vía redes sociales, con el objetivo de buscar blancos de ataques fáciles mediante engaños a las

personas como por ejemplo; el reclamo de un premio que ha sido favorecido, donde pueden otorgar sus datos personales de manera ligera al cibercriminal.

Características comunes de Phising CAR

Según Guerrero (2012) en su libro sobre el Fraude en la Red menciona que: “existe dos características comunes que se detallan a continuación” (pág. 35).

- Solicitud de dinero como señal o reserva de transporte.
- Pago a través de compañías de envió de dinero o empresas intermediarias.

d.1 Ventas trampa

Según Guerrero (2012) en su libro sobre el Fraude en la Red menciona que “es lo contrario del Phising Car, en este tipo de estafa somos nosotros los que tenemos anuncio en internet, si recibe mensajes de personas interesadas, habitualmente desde el extranjero, que incluso le ofrecen una cantidad superior al precio de venta” (pág. 49)

Por lo tanto se puede decir que estos interesados proponen pagar de una manera inmediata por medio de talones informativos, transferencias bancarias o empresas de envió de dinero.

e.1 Scam

Según Guerrero (2012) en su libro sobre el Fraude en la Red menciona que “es la captación de personas por medio del correo electrónicos, anuncios en foros, páginas de empleo o similares, donde se ofrece un trabajo con condiciones muy ventajosas a realizar desde casa y con un gran beneficio” (pág. 49)

En general se puede decir que se tratan de empresas ficticias, que al interesado le pedirán como único requisito que disponga de una cuenta bancaria para poder operar con sus activos. Consistiendo su trabajo en recibir ciertas cantidades de dinero en su cuenta y a su vez transferirlos a otra o remitirlo a través de empresas dedicadas al envío de dinero.

f.1 Sorteos, herencias y asimilados

> Otra forma de fraude muy extendida y que sobre todo usa como soporte el mail, consiste en que usted recibe un correo electrónico, donde se lo notifica que ha resultado ganador de una cantidad importante de dinero, un viaje, o cualquier otro bien. (Guerrero, 2012, pág. 57).

Es importante recalcar que para poder recibir el supuesto benéfico se le pide a la persona vulnerable una cierta cantidad de dinero en concepto de gastos personales, impuestos u otras tasas, curiosamente, una vez que se adelante el dinero simplemente desaparecen el criminal.

g.1 Scam Baiting

Ibídem menciona que “no se trata de un nuevo tipo de fraude, sino de un movimiento anónimo que surge como respuesta al perjuicio causado por las estafas mencionadas hasta ahora” (pág. 67)

En si podríamos exponer que este tipo de delito informático se refiere a una trampa en la cual se utiliza datos falsos o indebidos, que consiste en engañar a los presuntos cibercriminales haciéndoles perder tiempo y recursos económicos.

h.1 Dialers

> Este es uno de los primeros fraudes informáticos que se dieron en la red, los Dialers en un primer momento eran pequeños programas que los proveedores de acceso proporcionaban a sus clientes, para configurar los

> datos y aplicaciones de los sistemas operativos de su conexión de forma rápida y sencilla. (Guerrero, 2012, pág. 69).

Los Dialers son un tipo de fraude donde se utilizan aplicaciones y datos que marcan un número de teléfono de tarificación especial, por lo tanto se puede decir que el costo de estos números es superior al de una llamada nacional normal, debido al gran benéfico que otorgaran los ciberdelincuente al obtener cualquier tipo de información.

i.1 Vishing

> Este fraude podríamos considerarlo una variante del Phishing, concretamente se beneficia del actual boom de la telefonía a través de internet VoIP, esta tecnología mediante la técnica adecuada, permite al usuario que su número corresponda a una ciudad, aunque en realidad, se encuentra en cualquier otra parte del mundo. (Guerrero, 2012).

Este tipo de fraude actualmente presenta un boom en los mercados tecnológicos a través de las redes telefónicas que mediante una llamada electrónica de cualquier parte del mundo se puede conseguir cualquier tipo de información que sirve para el ciberdelincuente como fuente de ataque.

A continuación se menciona varias características comunes las de esta modalidad de fraude informático los cuales se detallan:

- Llamadas centralitas autónomas
- Solicitud de datos bancarios
- Solicitud de datos personales para verificar la identidad del usuario. (pág. 79)

2.2.3. Vulnerabilidad

Según Gómez (2011) en su Enciclopedia de la Seguridad Informática menciona que “La vulnerabilidad es cualquier debilidad en el sistema informático que puede permitir a las amenazas causarle daños y producir perdidas muy relevantes en la organización” (pág. 61)

Por lo tanto una vulnerabilidad es un fallo en un programa o sistema, pero no cualquier abertura, sino de seguridad. Ya que es necesaria hacer esta distinción donde no todos los errores de programación se derivan en grietas o aperturas de seguridad. Un error en un programa puede llevar a que no funcione correctamente o que su comportamiento no sea el esperado, pero no todos estos tipos de problemas pueden considerarse fallos de seguridad, dependiendo de la capacidad de aprovecharse de este defecto, la vulnerabilidad será más o menos grave.

a) Vulnerabilidad en los Sistemas Informáticos

> La vulnerabilidad en los sistemas de información se dan por el acceso no autorizado, errores y la destrucción de datos que pueden ocurrir en cualquier momento ya sea en el software y hardware de los sistemas en línea. También es muy importante recalcar que entre las áreas de vulnerabilidad, se incluyen procedimientos manuales, hardware de terminal de computadoras, concentradores en línea, procesadores frontales de control, software del sistema y programas de aplicación, archivos en discos de sistemas, aplicaciones y archivos en cinta. (Laudon & Laudon, 1996, pág. 704)

Existe varias razones para que los sistemas de información y comunicación que se encuentran adecuadamente guardados o protegidos sean vulnerables o susceptibles de destrucción, fraude, error y mal uso, puesto que a los archivos de los ordenadores pueden tener acceso fácilmente por empleados de las mismas organizaciones así como también de personas externas quienes podrían manipular y dar un uso erróneo, sino se cuentas con la debida protección.

b) Vulnerabilidades que afectan a los equipos

Después de haber analizado minuciosamente la vulnerabilidad en los sistemas informáticos se realizara una descripción de los tipos de vulnerabilidades más frecuentes, que pueden afectar tanto a los equipos como a las aplicaciones informáticas.

a.1 Routers y Cable- Módems

> Las vulnerabilidades detectadas en estos dispositivos permiten acceder a los equipos y redes conectadas por los Routers y módems afectados, o facilitan la ejecución de ataques de denegación de Servicios (DoS) que tengan como consecuencia el bloqueo total o parcial de las redes de ordenadores conectadas a través de estos dispositivos. (Gómez, 2011, pág. 182).

Mediante estos tipos de dispositivos las empresas industriales, comerciales y de servicios hoy en día están muy propensas a ataques informáticos o robos de información confidencial que pueden servir como blancos de ataques por mafias internacionales que se dedican a captar información para mediante chantajes o espionaje recibir una determinada cantidad de dinero para devolver la información que fue extraída de manera ilegal.

b.1 Cámaras Web y Servidores de Video

> Los fallos detectados en este tipo de dispositivos permitirían el control remoto de la cámara por parte de un usuario malicioso (que podría de este modo, captar las imágenes y cambiar la configuración de la cámara en cuestión) o la ejecución de un ataque de Denegación de Servicios contra el dispositivo vulnerable. (Gómez, 2011, pág. 83).

Por lo tanto podríamos aludir que las cámaras web en las organizaciones empresariales tienen sus respectivas ventajas como es grabar de manera corrida las actividades que realiza el personal de la empresa en algún sitio indebido o restringido por parte de la administración de la misma manera tienen sus desventajas que por medio de este servicio el atacante puede recaudar información o imágenes que le sirva como recurso para realizar los ataques cibernéticos.

c.1 Impresoras, Escáner, Faxes

Ibídem considera que “las vulnerabilidades en este tipo de dispositivos podrían tener como consecuencia la sustracción de información reservada, la

Denegación del Servicio para los usuarios de los dispositivos afectados, el cambio de configuración para provocar un funcionamiento incorrecto" (Gómez, 2011, pág. 183).

Este tipo de servidores gracias al avance de la tecnología del siglo XXI son más propensos al acceso de su información personal, por esta razón los departamentos de TIC en cada organización darían implantar medidas de seguridad que contrarresten o bloquen los filtros de acceso directo de información que necesita mafias cibernéticas para actuar de manera indebida y perjudicar las actividades de las empresas.

d.1 Teléfonos Móviles

> El fenómeno como "snarfing" o "bluesnarfing", consiste en el acceso y control remoto de teléfonos móviles y agendas electrónicas, se está convirtiendo cada vez más en un problema, más serio. De hecho el software para acceder a la información contenida con teléfonos con tecnología bluetooth hoy en día se encuentra disponible en cualquier lugar del mundo. (Gómez, 2011, pág. 184).

Este tipo de dispositivo es una de los más accesibles al robo de información, debido a su fácil acceso, por medio de las aplicaciones que cada teléfono móvil tiene, también se puede que gracias a su elevada producción que presenta cada una de sus marcas auspiciantes cada día es más competitivo en el mercado tecnológico.

c) Vulnerabilidades que afectan a programas y aplicaciones informáticas

a.1 Sistemas Operativos, Servidores y Bases de Datos

> Durante estos últimos años se han descubierto multitud de fallos y vulnerabilidades en todos los sistema operativos del mercado mundial, gracias a la aparición de las distintas versiones de Windows de Microsoft, las familias de Linux MacOS, entre otros, se han descubierto numerosas vulnerabilidades en gestores de bases de datos como Oracle o SQL Sever

> y, de hecho, una de ellas facilitó la rápida programación del virus Slammer en el año 2003. (Gómez, 2011, pág. 185)

Los sistemas operativos en la última década han presentado grandes cambios, gracias al avance tecnológico, y de esta razón han servido como base principal para el desarrollo de muchas empresas en el mundo, agilitando sus labores de trabajo para obtener productos de calidad.

b.1 Navegadores

> Desde su presentación en el año 1994, se han detectado multitud de problemas y fallos de seguridad que han afectado a los principales navegadores como es: Internet Explorer de Microsoft, Netscape, Opera, Firefox, Chrome o safari ocurriendo graves consecuencias para los usuarios en la ejecución de códigos arbitrarios. (Gómez, 2011, pág. 186).

Por esta razón se puede exponer que no existe un control total en ningún tipo de tecnología o software informático que adquieren o contratan las personas u organizaciones, ya que cada día la tecnología presenta nuevas innovaciones que tienen grandes ventajas y desventajas para el desarrollo de las grandes y pequeñas empresas que brindan diversos servicios en el mundo entero.

c.1 Aplicaciones Ofimáticas como Word o Excel

Ibídem señala que “este tipo de aplicaciones se han visto afectadas por agujeros de seguridad que permitían acceder a información sensible en el equipo de la víctima, ejecutar código mediante lenguajes de macros sin tener en cuenta las medidas de protección contra macros entre otros” (Gómez, 2011, pág. 186).

Las aplicaciones de Microsoft Office de los equipos electrónicos son las principales fuentes o agujeros por el cual el atacante puede acceder a la información más relevante de una persona u organización, debido a esto es recomendable tener un Password de seguridad para cada una de las aplicaciones que se tenga mayor acceso durante las actividades de trabajo del personal.

d.1 Otras Utilidades y Aplicaciones Informáticas

Gracias al acelerado crecimiento de los sistemas tecnológicos se ha podido detectar múltiples casos de vulnerabilidades en los ficheros mal formados en compresores tan populares como WinZip o en aplicaciones de tratamiento de imágenes de las aplicaciones informáticas.

> Los reproductores de ficheros de audio también han resultado ser vulnerables a determinados ficheros “maliciosos”. Así, por ejemplo, mediante ficheros MP3 maliciosos, con etiquetas ID3V2 malintencionadas, se podía provocar un desbordamiento de memoria en el popular Winamp y ejecutar código arbitrario en los equipos afectados. (Gómez, 2011, pág. 187)

d) Causas de las vulnerabilidades de los sistemas informáticos

Según Gómez (2011) en su Enciclopedia de la Seguridad Informática menciona que “existe un sinnúmero de causas como las responsables de las vulnerabilidades que afectan a los sistemas informáticos de las empresas o de las personas” (Gómez, 2011, pág. 174).

a.1 Existencia de “puertas traseras” en los sistemas informáticos

Ibídem menciona que “las puertas traseras o agujeros también conocidos como “backdoors” constituyen una vía de acceso no autorizado a un sistema informático, saltándose las medidas de protección previstas e implementadas por sus administradores” (pág. 181)

Es muy importante recordar que en algunos casos las puertas traseras, puntos blancos de ataque o medios de intromisión pueden tener sus orígenes en una serie de medios o servicios que se utilizan durante los procesos de desarrollo de un sistema informático.

b.1 Descuido de los fabricantes

Ibídem menciona que “Se refiere a cuando los fabricantes contribuyen a la programación de virus y programas dañinos, al incluir su código en los discos duros de sus equipos o en las memory flash con los distintos programas y herramientas de los sistemas que se están utilizando” (pág. 182).

e) Consecuencias de las vulnerabilidades de los sistemas Informáticos

Los sistemas informáticos debido al avance de las tecnologías de información y comunicación, soportan varios efectos de vulnerabilidad, debido a las fallas naturales del hardware y software y al uso inadecuado de los programadores, operadores de computadoras personales de mantenimiento y usuarios finales quienes tienen acceso a los archivos empresariales.

Los sistemas informáticos son vulnerables a tales desafíos por las siguientes razones que detallare a continuación de acuerdo a nuestro criterio personal.

- Complejidad en el manejo de la información.
- Cambios de sistemas informáticos no autorizados por los gerentes de la organización.
- Desconocimiento en el uso de los nuevos sistemas de información.
- Abuso de confianza por parte de los empleados al realizar copias no autorizadas de los archivos de información con fines ilegales.
- Programación errónea
- Perdida de información relevante der la empresa
- Manipulación de datos.
- Descuido de información
- Filtración de datos ocultos

f) Seguridad Informática

La seguridad informática es una disciplina que se encarga de la protección, la integridad, y la privacidad de información almacenada en una organización. Es decir un sistema informático es protegido desde un punto de vista lógico (con el desarrollo de software) o físico (vinculado al mantenimiento eléctrico).

> La seguridad se refiere a las políticas, procedimientos y medidas técnicas usadas para evitar un acceso no autorizado, alteración, robo o daños físicos a los sistemas de registros. La seguridad informática puede promoverse mediante un conjunto de técnicas y herramientas para salvaguardar el hardware, software, las redes de información y datos. (Laudon & Laudon, 1996, pág. 708)

Los recursos del sistema de información (material informático o programas) de una organización deben ser utilizados de la manera eficiente a fin de mantener un control adecuado de la información y de su respectiva modificación si fue el caso necesario.

a.1 Seguridad de la Información

> La seguridad de la información hace referencia a todas aquellas medidas preventivas reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar; así como proteger la información buscando mantener la confidencialidad, la disponibilidad e Integridad de la misma, tiene como objetivo, la protección de la información, de los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada. (Terán, 2014, pág. 155)

Por lo tanto a la seguridad de la información se refiere a la integridad, confidencialidad, disponibilidad de información y datos, independientemente de la forma que se realice los procesos en la organización, y estos datos pueden ser, impresos, electrónicos u de otras formas de acuerdo a las actividades cotidianas de la empresa.

b.1 Confidencialidad

Es la propiedad de resguardar la divulgación de información a sistemas o personas no autorizadas. Como un ejemplo muy común podríamos decir realizar compras con tarjeta de crédito vía internet. La pérdida de confidencialidad de información podrá adoptar muchas formas como, hacker las claves de una tarjeta de crédito, el robo de computadoras portátiles en una organización y que no tengan sus claves de seguridad respectiva, envió de información en teléfonos móviles, entre otros.

c.1 Integridad

Según Terán (2014) en su libro de Administración Estratégica de la Función Informática menciona que la integridad "es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. La violación de integridad se presenta cuando un empleado, programa, procesa, modifica o borra los datos importantes que son parte de la información de una empresa" (pág. 156).

La integridad de las aplicaciones electrónicas debe ser segura y bien controlada, con la finalidad de prevenir posibles modificaciones o violación de los programas tecnológicos que manejan los empleados durante sus actividades diarias dentro de la organización

Disponibilidad

Ibídem menciona que: "la disponibilidad es variada en el sentido que existe varios mecanismos para cumplir con los niveles de servicio que se requiere, tales mecanismos se implementan en infraestructura tecnológica, servidores de correo electrónicos, de bases de datos y de sitios web" (pág. 157)

La disponibilidad se hace referencia a la cantidad de recursos tecnológicos que una organización posee para la ejecución de sus actividades o prestación de servicios en distintas áreas o departamentos empresariales.

g) Principales Atacantes Informáticos

Son aquellas personas que poseen habilidades extraordinarias, que les permite acceder a sistemas de información seguros sin ser descubiertos, también tiene la posibilidad de difundir sus conocimientos para que las demás personas se enteren de cómo es que realmente funciona la tecnología, para que conozcan las debilidades de sus propios sistemas de información.

Según Terán (2014) señala “los principales atacantes informáticos que pueden afectar a las organizaciones y personas las cuales se clasifican en”:

- **Hacker:** es una persono que posee amplios conocimientos en tecnología, ya sea en tele-comunicaciones, electrónica o informática; se mantiene permanentemente actualizando y conoce a fondo todo lo relacionado con sistemas complejos y programaciones informáticas.
- **Cracker:** es aquella persona con comportamiento compulsivo, que ostenta de su capacidad para estallar sistemas informáticos y electrónicos. Por lo tanto se dice que esta persona es un hábil conocedor de programación de hardware y software.
- **Lammer:** son aquellas personas deseosas de alcanzar el nivel de un hacker, pero su poca formación y conocimiento, les impiden realizar este sueño.
- **Copyhacker:** son una nueva generación de falsificadores dedicados al “crackeo” de Hardware, específicamente en el sector de tarjetas inteligentes. Su estrategia radica en establecer amistad con los verdaderos hackers para copiarles los métodos de rupturas y luego venderlos a los bucaneros.
- **Bucaneros:** son los comerciantes de la red, mas no existen en ella; aunque no poseen ningún tipo de formación en el área de los sistemas, pero si poseen un amplio conocimiento en el área de los negocios.
- **Phreaker:** se caracterizan por poseer grandes conocimientos en el área de telefonía terrestre, hibrida, móvil, etc.; incluso poseen más información que los propios técnicos de las compañías telefónicas.
- **Newbie:** es el típico novato de la red que sin proponérselo, tropieza con una página de hacking que descubre que en ella existen áreas de descarga de buenos programad de hackeo.

- **Script Kiddie: “**son simples usuarios del internet, sin conocimientos sobre hack o crack, aunque muy aficionados a estos temas pero en realidad no los comprenden realmente, simplemente son internautas que se limitan a recopilar información de la red” (pág. 161).

h) Virus Informáticos

Son pequeños programas que están diseñados para interferir en el funcionamiento normal de un ordenador, representan uno de los principales problemas para los usuarios de la tecnología, habitualmente borrando o impidiendo los accesos a los datos de información.

a.1 Tipos de Virus Informáticos

Según Guerrero (2012) en su libro sobre el Fraude en la Red menciona que: “existe varios tipos de virus más comunes que los usuarios pueden encontrar en los ordenadores informáticos”:

- **Virus de Boot (virus de sector de arranque):** es un virus que afecta al sector de arranque del disco duro del ordenador, habitualmente se hace con el control del mismo, sustituyendo o borrando la información que contiene el sector de arranque original.
- **Virus de Fichero:** este virus afecta fundamentalmente a los archivos que ejecutan códigos de sus ordenador, los más comunes son los que tienen extensión .com, .exe o .bat, no obstante, cualquier archivo que ejecute un programa es susceptible de ser infectado.
- **Virus de macro:** tienen como objetivo la infección de los archivos creados y abiertos por programas que contienen macros, como por ejemplo el paquete Office de Microsoft.
- **Troyanos (Spyware):** es un virus al uso, aunque lo englobamos en esta categoría, se trata de un programa con código malicioso, cuya finalidad más común es permitir a un tercero a acceder a su ordenador a través de la red.
- **Gusanos (Worms):** es un programa cuyo único objetivo es replicarse de forma automática y extenderse rápidamente infectando la mayor cantidad posible de ordenadores. (Guerrero, 2012)

Es muy importante mencionar que los virus informáticos son aquellos que crean una puerta trasera, permitiendo que el usuario no se percate de su daño o

perjuicio y pueda tomar un control previo con anterioridad al ordenador a tevés de la red.

Una de sus principales características de este tipo de virus es que no necesita la intervención del usuario para su utilización o para duplicarse o extenderse en los archivos del ordenador, principalmente toma el control de los programas más importantes encargados de los servicios de comunicación de la organización.

2.2.5. Control Interno

Desde las épocas primitivas del ser humano y a largo de la historia se han establecido herramientas de control, con la necesidad de resguardar y controlar sus cosechas, ganado o pertenencias.

Para empezar con una breve introducción al Control Interno, se puede decir que nos es nada fácil su aplicabilidad dentro de las empresas si estas no cuentan con una cultura organizativa y mucho menos si no hay decisión en lo directivos en implementarlo, lo que se busca es alcanzar un fin o un objetivo organizacional que se puede llegar a cumplir.

En la actualidad en el mundo empresarial, con la globalización en auge, las evolución de las organizaciones, el avance de la tecnología entre otros factores, conllevan a un aumento de tareas, operaciones, funciones, responsabilidades, protección de la información, el aumento en los niveles de riesgo, lo que ha significado que las empresas se orienten a establecer planes organizacionales relacionados con métodos, técnicas y procedimientos que ayuden al cumplimiento de objetivos de la dirección.

a) Perspectivas

Perspectivas dentro del Control Interno haciendo alusión desde una óptica general y la aparición en sus inicios se menciona las principales dentro del estudio y la aplicabilidad del control interno que son:

a.1 Perspectiva profesional

El primer estudio conocido sobre el control interno fue publicado en Estados Unidos en 1949 bajo el título de Internal Control - Elements of a coordinated System and Its Importance to Management and the Independent Public Accountant, de donde se deriva la primera definición del Control Interno de la siguiente manera:

> El control interno comprende el plan de la organización y todos los métodos y medidas coordinados que se adoptan en un negocio para salvaguardar sus activos, verificar la exactitud y la confiabilidad de sus datos contables, promover la eficiencia operacional y fomentar la adherencia a las políticas prescritas. (Mantilla & Cante, 2005, pág. 11)

Otra definición dentro del contexto profesional y que se sumó como complemento del control interno fue emitida por el Institute of Internal Auditors (IAI) así: “Son las acciones tomadas por la administración para planear, organizar y dirigir el desempeño de acciones suficientes que provean seguridad razonable de que estarán logrando los siguientes objetivos”:

- Logro de los objetivos y metas establecidos para las operaciones y para los programas.
- Uso económico y eficiente de los recursos.
- Salvaguardia de los activos.
- Confiabilidad e integridad de la información.
- Cumplimiento de políticas, planes procedimientos, leyes y regulaciones.

b.1 Perspectiva reguladora

> Dentro de esta perspectiva como nos menciona Mantilla, Cante. (2005) existen entes reguladores internacionales como el Comité de Basilea y el International Organization of Securities Commissions (IOSCO) quienes se encargan de vigilar los estándares de calidad y de independencia, de igual manera menciona al control interno en línea con el Committee of Sponsoring Organizations of the Treadwey Commissions (COSO) y el Basle Committee on Banking Supervisión (Comité de Basilea sobre supervisión bancaria), emitieron en el 1998 una estructura conceptual sobre los sistemas de control interno dentro de las organizaciones bancarias, con un muy alto interés de resaltar los relacionado con la evaluación de los sistemas. (pág. 15)

El Basle Committee on Banking Supervisión (Comité de Basilea sobre supervisión bancaria) define al control interno de la siguiente manera:

> Control Interno es un proceso efectuado por la junta de directores, la administración principal y todos los niveles del personal. No es únicamente un procedimiento o una política desempeñada en un cierto punto del tiempo, sino que está operando continuamente en todos los niveles del banco o la organización. La junta de directores y la administración son responsables por el abastecimiento de la cultura apropiada para facilitar un efectivo proceso de control interno y por monitorear su efectividad sobre una base ongoing; sin embargo, cada individuo dentro de una organización tiene que participar en el proceso. (Mantilla & Cante, 2005, pág. 17).

En conclusión de acuerdo a las definiciones realizadas por varios autores podríamos mencionar que el control interno es efectuado por la junta directiva de la administración de la empresa, ya que es un lineamiento que ayuda a la empresa en el desempeño de las actividades personales y al cumplimiento de los objetivos de los mismos.

c.1 Perspectiva académica

Esta es una perspectiva que se enfoca netamente en tres autores académicos ya no desde lo profesional o regulador, para los cual se tiene de preferencia de estudio a Wallace, Root y Chorafas.

Cada uno de estos autores que se menciona a continuación tiene un importante complemento de percepción acerca de control interno y como ayudan al desarrollo de las organizaciones.

- **Wanda Wallace:** considerada una persona importante dentro de las auditorías de estados financieros y autora del más importante manual sobre control interno, su estudio empieza con la evaluación que se realiza del control interno para los propósitos de auditoría.
- **Steven Root:** analiza el impacto de COSO y muestra los desarrollos que van más allá de este, sobre todos los derivados de las nuevas prácticas gerenciales: control interno para enriquecer el gobierno corporativo, de igual manera el foco de atención del control interno lo centra en resolver las diversas situaciones entendidas como oportunidades, amenazas, fortalezas y debilidades.
- **Dimitris Chorafas:** centra sus estudios en el control interno de los entes de interés público y principalmente de los que participan en mercado de capital (financiero y de valores). (pág. 21)

b) Control Interno

El Control Interno puede significar varias cosas para diferentes personas y de acuerdo al ámbito que se vaya aplicar, lo que origina una serie de contradicciones y de los resultados que se puedan obtener sea bueno o malo dentro de las organizaciones o empresas.

a.1 Definiciones

Según Mantilla (2005) señala que “El control interno se define ampliamente como un proceso realizado por el consejo de directores, administradores y otro personal de una entidad, diseñado para proporcionar seguridad razonable mirando el cumplimiento de los objetivos”. (pág. 4)

Dentro de los objetivos que manifiesta Mantilla (2005) son los siguientes:

a) Efectividad y eficiencia de las operaciones.
b) Confiabilidad de la información financiera
c) Cumplimiento de las leyes y regulaciones aplicables.

Según la International Federation of Accountants (2008), menciona al Control Interno de la siguiente manera “El control interno es diseñado e implementado por la administración para tratar los riesgos del negocio y de fraude identificados que amenazan el logro de los objetivos establecidos, tales como la confiabilidad de la información financiera.” (pág. 43)

b.1 Componentes dentro del Control Interno

Dentro del Control Interno existen cinco componentes interrelacionados estrechamente con el manejo y la administración de la empresa ya que al implementarlos se los puede hacer de diferente manera pero su estructura es la misma y estos componentes son:

- Ambiente de Control
- Valoración de Riesgos
- Actividades de Control
- Información y Comunicación
- Monitoreo o Supervisión

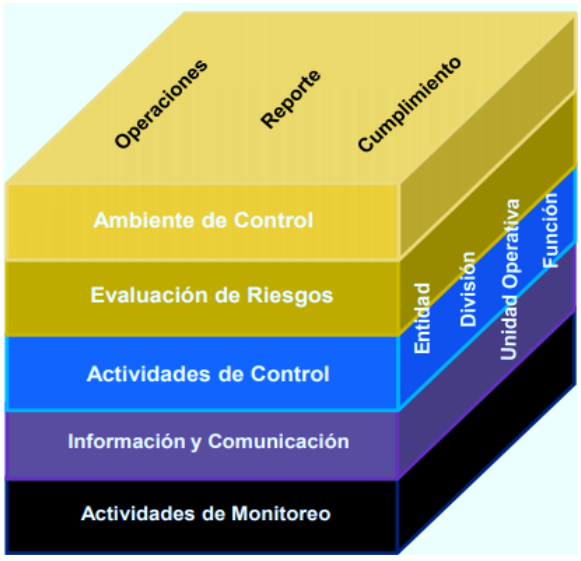


Figura 10 Componentes del COSO

Fuente: (Deloitte, 2015)

Podemos decir que aunque el control interno ayuda de una manera significativa a conseguir los objetivos planteados por las empresas, acatar las regulaciones y cumplimiento de las leyes, y a la confiabilidad de la información financiera, no es la panacea total dentro de las organizaciones.

c) COSO ERM

Un Sistema de Control Interno provee una serie de políticas y procedimientos adoptados y adecuados por una organización a su sistema de gestión para asegurar el cumplimiento de sus objetivos en la medida que le sea posible, aportar a un desarrollo eficiente del negocio, garantizar el apego a políticas de administración por parte de la gerencia, salvaguarda eficiente y eficaz de activos, prevención y detección de riesgos así como de fraude y error, registro precisos e íntegros de registros contables y primordialmente la preparación oportuna y confiable de información financiera.

a.1 Definición

> Es un proceso efectuado por la Junta de Directores, la administración y otro personal de la entidad, aplicando en la definición de la estrategia y a través del emprendimiento, diseñado para identificar los eventos potenciales que pueden afectar la entidad, y para administrar los riesgos que se encuentran dentro de su apetito por el riesgo, para proveer seguridad razonable en relación con el logro de objetivos. (Estupiñan, 2006, pág. 66).

De esta manera un Sistema de Control Interno como es el COSO II ERM, tiene un enfoque mucho más amplio, no se enmarca en asuntos estrictamente relacionados a un sistema de contabilidad confiable y eficaz, pues aporta directamente a la gestión organizacional permitiendo mitigar el riesgo más no desaparecerlo en su conjunto.

b.1 Fundamentos de COSO-ERM

> Las empresas con ánimo o sin ánimo de lucro deben propender a crear valor a sus protectores, dueños o accionistas, así como la de enfrentar y superar la incertidumbre, desafiándolas con preparación suficiente, para poder proveer una estructura conceptual, así la gerencia trate de manera efectiva la incertidumbre que representan los riesgos y oportunidades, y así enriquecer su capacidad para generar valor. (Estupiñan, 2006, pág. 67)

El ERM o Administración de Riesgo Empresarial está compuesto por ocho componentes los cuales comprenden:

- Ambiente Interno
- Establecimiento de Objetivos.
- Identificación de Acontecimientos.
- Evaluación de Riesgos.
- Respuesta al Riesgo.
- Actividades de Control.
- Información y Comunicación.
- Supervisión o Monitoreo (Estupiñan, 2006)

i Ambiente Interno

> Consiste en el establecimiento de un entorno que estimule e influencie la actividad del personal con respecto al control de sus actividades. Es en esencia el principal elemento sobre el que se sustenta o actúan los demás componentes e indispensable, a su vez, para la realización de los objetivos de control. (Estupiñan, 2006, pág. 27)

> El Ambiente Interno establece el tono de una organización, para influenciar la conciencia de control de su gente. Es el fundamento de todos los demás componentes del control interno, proporcionando disciplina y estructura. El Ambiente Interno tiene una influencia profunda en la manera como se estructuran las actividades del negocio, se establecen los objetivos y valoran los riesgos. (Mantilla & Cante, 2005, pág. 25)

Dentro del Ambiente Interno encontramos:

- **Integridad y valores éticos.** Tienen como propósito establecer los valores éticos y de conducta que se espera de todos los miembros de la organización durante el desempeño de sus actividades, ya que la

efectividad del control depende de la integridad y valores del personal que lo diseña, y le da seguimiento.

- **Competencia.** Son los conocimientos y habilidades que debe poseer el personal para cumplir adecuadamente sus tareas.
- **Junta Directiva. Consejo de Administración y/o Comité de Auditoría.** Debido a que estos órganos fijan los criterios que perfilan el Ambiente de Control, es determinante que sus miembros cuenten con la experiencia, dedicación y compromisos necesarios para tomar las decisiones adecuadas e interactúen con los auditores internos y externos.
- **Filosofía Administrativa y Estilo de Operación.** Los factores más relevantes son las actitudes mostradas hacia la información financiera, el procesamiento de la información, y los principios y criterios contables, entre otros (Estupiñan, 2006)

En este primer componente del COSO ERM se realiza un estudio de cómo está el ambiente interno de la empresa u organización ese clima organizacional que debe existir tanto entre directivos y los trabajadores, para medir el clima de trabajo, su valores institucionales, verificar si cuentan con misión, visión y si esta es conocida por todos quienes forman parte de la empresa.

ii Establecimiento de Objetivos

> Dentro del contexto de la misión o visión, se establecen objetivos estratégicos, selecciona estrategias y establece objetivos relacionados, alineados y vinculados con la estrategia, así como los relacionados con las operaciones que aportan efectividad y eficiencia de las actividades operativas, ayudando a la efectividad en la presentación de reportes o informes internos y externos (financiera y no financiera), como la de cumplir con las leyes y regulaciones aplicables y de sus procedimientos internos determinados. (Estupiñan, 2006)

Dentro del establecimiento de objetivos de la empresa se tiene que preparar estrategias o formas de cómo llegar a ellos, y que cada una de las unidades que participen del desarrollo productivo se comprometa para el cumplimiento de los mismos, recalcando en todos los niveles operativos.

iii Identificación de Acontecimientos

La Alta Gerencia reconoce normalmente que existen incertidumbres que no se puede conocer con certeza cuándo, dónde y cómo ocurrirá un evento, o si ocurrirá su resultado, existiendo factores internos y externos que afectan la ocurrencia de un evento.

La metodología de identificación de eventos pueden comprender una combinación de técnicas vinculadas con herramientas de apoyo, como la identificación de eventos pasados (cesación de pagos, cambios en los precios, pérdidas por accidentes) y futuros (cambios demográficos, mercados nuevos y acciones de los competidores). Las técnicas que se centran en las planeaciones consideran asuntos como cambios demográficos, mercados nuevos y acciones de los competidores. Potencialmente los eventos tienen un impacto negativo, positivo o de ambos, representando los primeros riesgos inmediatos, mediatos o de largo plazo, los cuales deben ser evaluados dentro del E.R.M.

> Dentro de las metodologías más conocidas para la identificación de eventos, las cuales se han aplicado de parte de varias firmas de auditores y dentro de las metodologías internas de la empresa son las matrices "análisis PETS o GESI", "análisis FODA o DOFA", "análisis de las cinco fuerzas" y "matriz de conocimiento del negocio e identificación de riesgos". (Estupiñan, 2006)

iv Evaluación de Riesgos

> Le permite a una entidad considerar como los eventos potenciales pueden afectar logro de los objetivos. La gerencia valora los eventos bajo las perspectivas de probabilidad (la posibilidad de que ocurra un evento) e impacto (su efecto debido a su ocurrencia), con base en datos pasados internos (pueden considerarse de carácter subjetivo) y externos (son más objetivos). (Estupiñan, 2006)

Se evalúa de una manera sistemática, luego de haber identificado los riesgos por la alta gerencia y por los distintos niveles organizacionales, para así poder contrarrestar de una manera eficaz y oportuna, adoptando medidas de resolución para la mitigación de los riesgos.

v Respuesta al Riesgo

> Identifica y evalúa las posibles respuestas de los riesgos y considera su efecto en la probabilidad y el impacto. Evalúa las opciones en relación con el apetito del riesgo en la entidad, el costo y su beneficio de la respuesta a los riesgos potenciales, y el grado que más reporta las posibilidades de riesgo. Las respuestas al riesgo caen dentro de las categorías de evitar, reducir, compartir y aceptar el riesgo. (Estupiñan, 2006)

Aquí se evalúa la probabilidad de la adopción de las medidas para la reducción o eliminación del riesgo, de manera económica y financiera y como poder compartirla que no afecte de manera directa a un punto, sino que esto se pueda diversificar el riesgo como se conoce en la administración del riesgo.

vi Actividades de Control

> Son las políticas y los procedimientos que ayudan a asegurar que se están ejecutando de manera apropiada las respuestas al riesgo, hacen parte del proceso mediante el cual una empresa intenta lograr sus objetivos de negocio. Se clasifican en controles generales y de aplicación. Controles generales representan la infraestructura de la tecnología, seguridad y adquisición del hardware; y el desarrollo y mantenimiento del software y los controles de aplicación aseguran complejidad, exactitud, y validez de la base de datos. (Estupiñan, 2006)

Son herramientas que ayudan al cumplimiento de los pasos, procesos que se llevan a cabo para el cumplimiento de los objetivos en la organización, ya que estos pueden ser de tecnología software y hardware, para de esa manera consolidar la información.

vii Información y Comunicación

> Identifica, captura y comunica información de fuentes internas y externas, en una forma y en una franja de tiempo que le permita al personal llevar a cabo sus responsabilidades. La comunicación efectiva también ocurre en un sentido amplio, hacia abajo o a través y hacia arriba en la entidad. En todos los niveles, se requiere información para identificar, valorar y responder a los riesgos, así como para operar y lograr los objetivos. (Estupiñan, 2006)

Este componente así como los demás son indispensables dentro de la evaluación de una organización a través del COSO-ERM, es la información indispensable para la aplicación del mismo sistema, ya que esta información debe provenir de manera endógena y exógena que permitan conocer con mayor amplitud de los posibles riesgos y en todos los niveles que se puedan suscitar.

viii Supervisión o Monitoreo

> Es un proceso que valora tanto la presencia como el funcionamiento de sus competencias y la calidad de su desempeño en el tiempo. Se puede realizar mediante actividades de ongoing o través de evaluaciones separadas, las dos asegura que la administración de riesgos continua aplicándose en todos los niveles y a través de la evaluación continua y periódica que hace la gerencia de la eficacia del diseño y operación de la estructura del control interno, para lograr una adecuada de identificación del riesgo, de acuerdo a lo planificado, modificando los procedimientos cuando se requiera. (Estupiñan, 2006)

Donde una vez realizado el control previo del COSO-ER dentro de la empresa se tiene que realizar un seguimiento necesario y muy indispensable para que se pueda establecer parámetros de cumplimiento con respecto a políticas, controles que se haya sugerido dentro de la empresa.

2.2.6. Auditoría

Dentro de la naturaleza con la que cuenta la auditoría se puede mencionar que es una revisión cuantificable de datos e información económica de una empresa u organización, para de esa manera establecer una revisión y los criterios establecidos para determinar hallazgos que sirven de ayuda al cumplimiento a los objetivos organizacionales.

a) Definición de Auditoría

Según Arens, Elder, Beasley (2007) en su libro de Auditoría un Enfoque Integral menciona que “la Auditoría es la acumulación y evaluación de la evidencia basada en información para determinar y reportar sobre el grado de

correspondencia entre la información y los criterios establecidos. La auditoría debe realizarla una persona independiente y competente". (pág. 4).

En si una auditoría se refiere a un trabajo que realiza un auditor con la finalidad de verificar hechos a circunstancias que han pasado o están pasando dentro de una organización. El principal propósito es brindar una opinión independiente y competente acerca de los resultados encontrados durante la ejecución de su trabajo.

b) Principios de Auditoría

Dentro de los principios que se manejan dentro de la auditoría se pueden mencionar los más importantes como son:

- Integridad
- Veracidad
- Correcta Valuación

c) Tipos de Auditoría

Dentro de los diferentes tipos de auditoría podemos mencionar varias de acuerdo a su aplicación o al campo que va estar dirigidas en una empresa las mismas que se mencionan a continuación:

a.1 Auditoría Financiera

> También es conocida como auditoría de estados financieros para determinar si el conjunto de estados financieros se presenta de acuerdo con los criterios especificados como son los principios de contabilidad generalmente aceptados u otra norma que se tenga que cumplir para de esa manera tener una razonabilidad de los saldos. (Arens & Loebbecke, Auditoría un Enfoque Integral, 1996, pág. 4).

La auditoría financiera es aquella que se encarga de examinar los estados financieros y a través de ellos todas las actividades financieras realizadas por el

ente contable bajo los principios de contabilidad generalmente aceptados con la finalidad de proporcionar un criterio técnico y profesional de los mismos.

b.1 Auditoría Operacional

Ibídem manifiesta que “Es una revisión de cualquier parte del proceso y métodos de operación de una compañía con el propósito de evaluar su eficiencia y eficacia en las operaciones”. (Arens & Loebbecke, Auditoría un Enfoque Integral, 1996, pág. 5).

Este tipo de auditoría se refiere a la acumulación de evidencias obtenidas por parte de un auditor mediante un examen sistemático dentro del departamento de control interno de una empresa, en si su propósito es principal es verificar si los recursos económicos y financieros están siendo utilizados de manera adecuada.

Ejemplo:

Evaluar la eficiencia, precisión y satisfacción del cliente en la distribución de cartas y paquetes que hace una compañía como Servientrega Ecuador.

c.1 Auditoría de Cumplimiento

Ibídem menciona que “Mediante la auditoría de cumplimiento es determinar si el auditado está cumpliendo con algunos procedimientos, reglas o reglamentos específicos que fije alguna autoridad superior.” (Arens & Loebbecke, Auditoría un Enfoque Integral, 1996, pág. 5).

Por lo tanto se podría mencionar que una auditoría de cumplimiento como su nombre lo india es aquella que se encarga de verificar si las operaciones financieras, económicas, administrativas y de otra índole se estén cumpliendo de acuerdo a las normas legales y estatutos planteados por parte de la administración o cualquier ente controlador. Este tipo de auditoría se lleva a cabo

mediante la revisión de los documentos que constatan las actividades realizadas en la empresa.

Ejemplo:

Determinar si el personal de contabilidad está siguiendo la normativa fiscal vigente y aplicando el salario básico unificado como monto mínimo de pago y la afiliación al IESS desde el primer día de trabajo.

d.1 Auditoría Forense

Según Badillo (2008) señal que “La auditoría forense es una auditoría especializada que se enfoca en la prevención y detección del fraude financiero a través de los siguientes enfoques: preventivo y detective. (pág. 5).

Este tipo de auditoría se refiere al trabajo que realizan un grupo de personas especializadas en fraudes informáticos como contadores, auditores, abogados informáticos y entre otras personas especializadas en el área forense. Y está enfocada en la prevención y detección de fraudes económicos financieros.

e.1 Auditoría Informática

“Es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos” (Piattini, 2001, pág. 28).

Con respecto a la definición propuesta por este autor y nuestro criterio personal diríamos que la auditoría informática es un examen que se realiza con carácter crítico y objetivo con el fin de recoger, agrupar y evaluar evidencias informáticas para salvaguardar los activos y los recursos tecnológicos de una empresa.

f.1 Examen Especial

> El examen especial, es uno de los principales servicios que brinda la Contraloría, como parte de la auditoría gubernamental, es, pues, como lo expresa el Art.19 de la LOC, el examen que verificará, estudiará y evaluará aspectos limitados o de una parte de las actividades relativas a la gestión financiera, administrativa, operativa y medio ambiental; con posterioridad a su ejecución, aplicará las técnicas y procedimientos de auditoría, de ingeniería o afines, o de las disciplinas específicas, de acuerdo con la materia de examen y formulará el correspondiente informe que deberá contener comentarios, conclusiones y recomendaciones. (Contraloria General del Estado, 2016).

En si un examen especial comprende la verificación del cumplimiento de políticas y lineamientos que fueron aprobados dentro de una organización por la máxima autoridad y su principal propósito es analizar a una cuenta, área o departamento específico mediante la ejecución de procesos planteados por parte del personal encarga a realizar dicho trabajo.

d) Auditoría Informática

Al finalizar el siglo XX, ha existido un crecimiento importante en los sistemas informáticos que son muy esenciales para el desarrollo de las organizaciones siendo vitales para la operatividad adoptando una buena gestión de recursos de TI, en protección de datos e información y comunicación.

> En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado el "management" o gestión de la empresa. Cabe aclarar que la Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma. Por ende, debido a su importancia en el funcionamiento de una empresa, existe la Auditoría Informática. (Infovia.Ar, 2002)

a.1 Definiciones

Según Piattini (2001) define como “el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los

activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos" (pág. 28)

Según Echenique (2001) define a la auditoría informática de la siguiente manera:

> Es la revisión y evaluación de los controles, sistemas y procedimientos de la informática, de los equipos de cómputo, su utilización, eficiencia y seguridad; de la organización que participa en el procesamiento de la información y comunicación, a fin de que por medio del señalamiento de recursos alternativos se logre un utilización más eficiente, confiable y segura de la información que servirá para una adecuada toma de decisiones. (pág. 27).

Existen muchas definiciones de la auditoría informática o auditoría de sistemas como también se le conoce dentro del mundo informático y computacional, pero que se llega a una sola conclusión de revisar la seguridad informática de las empresas para una mejor operatividad total.

b.1 Alcance de la Auditoría Informática

Dentro del alcance de la auditoría informática debe existir un acuerdo concreto entre los auditores y la empresa sometida a la revisión, para de esa forma conocer de manera abierta las funciones, las áreas, los sistemas a auditar.

La auditoría informática no solo deberá comprender no solo la evaluación de los equipos de cómputo o de un sistema o procedimiento especifico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, comunicación, controles, archivos, seguridad, personal y obtención de información.

> El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoría informática, se completa con los objetivos de ésta. El alcance ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado no solamente hasta qué puntos se ha llegado, sino cuáles materias fronterizas han sido omitidos. (Joven Club de Computacion, 2010)

En este sentido un ejemplo del control surge al plantearse las siguientes cuestiones:

- ¿Se someterán los registros grabados a un control de integridad exhaustivo?
- ¿Se comprobará que los controles de validación de errores son adecuados y suficiente?

c.1 Objetivos de la Auditoría Informática

Dentro de los objetivos que se plantea Piattini (2001) dentro de la auditoría informática tenemos los siguientes:

- Objetivos de protección de activos e integridad de los datos.
- Objetivos de gestión que abarcan, no solamente los de protección de activos, sino también los de eficiencia y eficacia. (pág. 29)

Según una investigación argentina y como documento de soporte en relación a la auditoría informática nos menciona un objetivo fundamental dentro de esta rama como es la operatividad.

i Operatividad

> La operatividad es una función de mínimos consistente en que la organización y las maquinas funcionen, siquiera mínimamente. No es admisible detener la maquinaria informática para descubrir sus fallos y comenzar de nuevo. La auditoría debe iniciar su actividad cuando los Sistemas están operativos, es el principal objetivo el de mantener tal situación. Tal objetivo debe conseguirse tanto a nivel global como parcial. La operatividad de los Sistemas ha de constituir entonces la principal preocupación del auditor informático. Para conseguirla hay que acudir a la realización de Controles Técnicos Generales de Operatividad y Controles Técnicos Específicos de Operatividad, previos a cualquier actividad de aquel. (Canaves, 2002)

Dentro de la operatividad se refiere a dos controles sumamente importantes dentro del cumplimiento de la operatividad como son y se describen a continuación:

- **Los Controles Técnicos Generales:** son los que se realizan para verificar la compatibilidad de funcionamiento simultaneo del Sistema Operativo y el Software de base con todos los subsistemas existentes, así como la compatibilidad del Hardware y del Software instalados.
- **Los Controles Técnicos Específicos:** de modo menos acusado, son igualmente necesarios para lograr la operatividad de los sistemas. Un ejemplo de lo que se puede encontrar mal son parámetros de asignación automática de espacio en disco que dificulten o impidan su utilización posterior por una sección distinta de la que lo generó. También, los periodos de retención de ficheros comunes a varias aplicaciones pueden estar definidos con distintos plazos en cada una de ellas, de modo que la pérdida de información es un hecho que podrá producirse con facilidad, quedando inoperativa la explotación de alguna de las aplicaciones mencionadas. (Canaves, 2002, pág. 10)

d.1 Características de la Auditoría Informática

Dentro de las principales características que se puede mencionar y en las cuales se hace alusión a tres tipos de auditorías que son esenciales dentro de una organización o empresa para poder salvaguardar la información.

- La información de la empresa y para la empresa, siempre importante, se ha convertido en un Activo Real de la misma, como sus Stocks o materias primas si las hay. Por ende, han de realizarse inversiones informáticas, materia de la que se ocupa la Auditoría de Inversión Informática.
- Del mismo modo, los Sistemas Informáticos han de protegerse de modo global y particular: a ello se debe la existencia de la Auditoría de Seguridad Informática en general, o a la auditoría de Seguridad de alguna de sus áreas, como pudieran ser Desarrollo o Técnica de Sistemas.
- Cuando se producen cambios estructurales en la Informática, se reorganiza de alguna forma su función: se está en el campo de la Auditoría de Organización Informática. (Canaves, 2002).

e) Auditoría Forense

a.1 Origen

Para exponer una breve reseña de cómo se inició la auditoría forense, sus orígenes y su relación con hechos reales desde muy antes, y los juicios de valor que se emitían en esos tiempos, para lo cual se toma un fragmento del libro de Auditoría Financiera Forense que se presenta a continuación:

El primer auditor forense, fue probablemente un funcionario del Departamento del Tesoro, que se vio en la cinta de los intocables, donde un contador desenmascaró al mafioso Al capone en los años 30 en los Estados Unidos, entonces se considera que la auditoría forense sea tan antiguo que se inició con la primera ley escrita conocida como el Código de Hammurabi, primer documento conocido por el hombre y que trata sobre leyes, en ellas Hammurabi (1792-1750 a.C), donde se incluyó tablillas de arcilla, actividades comerciales, administrativas diplomáticas, normas sobre el comercio, recaudación de impuestos, la propiedad, no existía la contabilidad por partida doble, pero el Código de Hammurabi en sus fragmentos 100 al 126 da entender el conceptos de auditoría forense como:

“La auditoría forense consiste en demostrar con documentación contable un fraude o una mentira y también de hacen referencia a cálculos de ganancias y pérdidas en los negocios para los cuales se debe utilizar un contador.” (Cano & Lugo, 2008)

b.1 Definiciones

Ibídem define de la siguiente manera: “Una auditoría especializada en descubrir, divulgar y atestar sobre fraudes y delitos en el desarrollo de las funciones públicas y privadas”. (pág. 31)

Según Badillo (2008) define a la auditoría forense como “La auditoría forense es una auditoría especializada que se enfoca en la prevención y detección del fraude financiero a través de los siguientes enfoques: preventivo y detective”. (pág. 5)

La auditoría forense está relacionada con fraudes, delitos, estafas, encubrimiento de estados maquillados, por lo que centra dentro de una revisión profunda, buscando de manera contable indicios, hallazgos y errores, con el fin de sacar a la luz las pruebas y evidencias que ayuden a la resolución de estos problemas, para la designación de culpa y responsabilidad.

La auditoría forense tiene dos tipos de enfoques que coadyuvan a determinar cuál será el plan de acción en una organización para el tratamiento del problema de fraude, y podemos definirlos como:

c.1 Tipos de Auditoría Forense

i Auditoría forense preventiva

> Orientada a proporcionar aseguramiento (evaluación) o asesoría a las organizaciones respecto a su capacidad para disuadir, prevenir (evitar), detectar y reaccionar ante fraudes financieros, puede incluir trabajos de consultoría para implementar: programas y controles antifraude, esquemas de alerta temprana de irregularidades y sistemas de administración de denuncias. Este enfoque es proactivo por cuanto implica tomar decisiones y acciones en el presente, para evitar fraudes en el futuro. (Auditool, 2011)

Se puede mencionar como una auditoría que previene antes de que sucedan los hechos delictivos o mal intencionados para de esa manera evitar, de una manera ordenada y sistemática con procedimientos que permitan tener un control previo de hechos relevantes que puedan significar a un buen o mal funcionamiento de las operaciones dentro de las empresas.

ii Auditoría forense detectiva:

> Orientada a identificar la existencia de fraudes financieros mediante la investigación profunda de los mismos, establece, entre otros aspectos, los siguientes: cuantía del fraude; efectos directos e indirectos; posible tipificación (según normativa penal); presuntos autores, cómplices y encubridores; en muchas ocasiones los resultados de un trabajo de auditoría forense detectiva son puestos a consideración de la justicia que se encargará de analizar, juzgar y dictar la sentencia respectiva. Este enfoque es reactivo por cuanto implica tomar acciones y decisiones en el presente respecto a fraudes sucedidos en el pasado. (Auditool, 2011)

Esta auditoría forense detectiva se refiere a la identificación de fraudes una vez que dentro de las organizaciones se presentan inconsistencias o mal funcionamiento de los sistemas, tal vez por una intromisión de delincuentes en este caso cibernéticos para la expropiación de la información.

d.1 Alcance de la Auditoría Forense

Dentro del alcance que puede tener la auditoría forense es del periodo que se va auditar y este puede ser un año o dos o más, según el tiempo de revisión.

e.1 Objetivos de la Auditoría Forense

El principal objetivo de la auditoría forense es prevenir, detectar y divulgar los actos delictivos cometidos en las organizaciones públicas y privadas.

Sin embargo, tiene otros objetivos; entre los cuales están:

- Luchar contra la corrupción y el fraude;
- Disuadir, en los individuos, las prácticas deshonestas; y
- Exponer al asunto a las autoridades administrativas y judiciales competentes. (Benavides & Acosta, 2015)

f.1 Características de la Auditoría Forense

Según Badillo (2008) nos menciona las siguientes características:

- **Propósito:** Prevención y detección del fraude financiero. Debe señalarse que es competencia exclusiva de la justicia establecer si existe o no fraude (delito). El auditor forense llega a establecer indicios de responsabilidades penales que junto con la evidencia obtenida pone a consideración del juez correspondiente para que dicte sentencia.
- **Alcance:** El periodo que cubre el fraude financiero sujeto a investigación (auditoría).
- **Orientación:** Retrospectiva respecto del fraude financiero auditado; y, prospectiva a fin de recomendar la implementación de los controles preventivos, detectivos y correctivos necesarios para evitar a futuro fraudes financieros. Cabe señalar que todo sistema de control interno proporciona seguridad razonable pero no absoluta de evitar errores y/o irregularidades.
- **Normatividad:** Normas de auditoría financiera e interna en lo que fuere aplicable; normas de investigación; legislación penal; disposiciones normativas relacionadas con fraudes financieros.
- **Enfoque:** Combatir la corrupción financiera, pública y privada.
- **Auditor a cargo (Jefe de Equipo):** Profesional con formación de auditor financiero, Contador Público Autorizado.
- **Equipo de Apoyo:** Multidisciplinario: abogados, ingenieros en sistemas (auditores informáticos), investigadores (públicos o privados), agentes de oficinas del gobierno, miembros de inteligencia o contrainteligencia de entidades como policía o ejército, especialistas. (Badillo, 2008, pág. 15)

Todas estas características son las principales dentro de la auditoría forense ya que se inmersa en todo el campo de investigación mediante la auditoría, porque nos da a conocer desde el propósito de la auditoría, su alcance, el enfoque y la normativa con la que se va aplicar este tipo de examen o revisión dentro de la empresa u organización, objeto de estudio con la única finalidad de la detección de errores, fraudes o hallazgos significativos, que permitan tomar acciones positivas y suplir esos errores.

2.2.7. Informe de Auditoría

Los informes de auditoría son fundamentales dentro de un proceso de auditoría valga la redundancia, se puede decir como el producto final que entrega el auditor, hallazgos y la conclusiones que emite a la empresa, organización, junta de accionistas según fuese el caso.

a) Definiciones

> El informe de auditoría es el paso final de un proceso de auditoría. Los informes son esenciales para cualquier compromiso de auditoría o de certeza de cumplimiento puesto que comunican los hallazgos del auditor. Los usuarios de los estados financieros dependen del informe del auditor para tener certeza sobre los estados financieros de la compañía, es muy probable que al auditor se le impute responsabilidad por un informe de auditoría impreciso. (Arens, Elder, & Beasley, Auditoria,Un enfoque integral, 2007)

El informe de auditoría es la forma más clara y concreta que un auditor puede expresar su opinión de manera independiente, con respecto al examen previo de las cuentas de una empresa, para de esa manera determinar signos erróneos de un manejo inadecuado de la parte operativa, contable y administrativa.

b) Estructura del Informe

Ibídem menciona que a fin de permitir a los usuarios entender el leguaje de los informes de auditoría, las normas profesionales del American Institute of Certified Public Accountants (AICPA) ofrecen un estilo uniforme de redacción. (pág. 46)

> La principal característica del informe de auditoría es plasmar, de acuerdo a su alcance de su trabajo, su opinión respecto a las cuentas anuales de la empresa auditada, que expresan la imagen fiel del patrimonio, de sus situación financiera, de los resultados y en el caso que lo requiera de los flujos de efectivo. (Pallerola & Monfort, 2013, pág. 61)

Dentro de una estructura general podemos mencionar a lo más relevante que va redactado dentro del informe de auditoría que se menciona a continuación:

- Título del informe.
- Destinatarios del informe de auditoría.
- Párrafo introductorio.
- Párrafo de alcance.

- Párrafo de opinión.
- Nombre del despacho de CPC.
- Fecha del informe de auditoría. (2013)

A continuación se realiza una descripción de cada parte del informe:

- T**ítulo del Informe.-** Las normas exigen que el informe tenga un título y que este contenga la palabra independiente. Por ejemplo, los títulos apropiados serian “informe de auditoría independiente”, “informe de auditor independiente”, u “opinión del contador independiente”. El requisito de que el titulo contenga la palabra independiente tiene la intención de transmitir a los usuarios que la auditoría fue imparcial en todos los aspectos.
- **Destinatarios del informe de auditoría.-** El informe normalmente está dirigido a la compañía, a sus accionistas o al consejo de administración. En años recientes, se ha hecho costumbre dirigirlo al consejo de administración y a los accionistas para indicar que el auditor es independiente de la compañía.
- **Párrafo introductorio.-** El primer párrafo del informe cumple tres funciones: primero, presenta la simple declaración de que el despacho de CPC realizo una auditoría. El segundo párrafo enumera los estados financieros que fueron auditados, incluidas las fechas del balance y los periodos contables de resultados y del estado de flujos de efectivo, y el tercer párrafo introductorio afirma que los estados son responsabilidad de la administración, mientras que la del auditor es expresar una opinión sobre los estados fundamentada en la auditoría.
- **Párrafo de Alcance.-** El párrafo del alcance es una afirmación de hechos en cuanto a lo que el auditor realizo en la auditoría. En primer lugar, este párrafo señala que el auditor siguió las normas de auditoría generalmente aceptadas en Estados Unidos.
- **Párrafo de opinión.-** El párrafo final del informe estándar contiene las conclusiones del auditor basadas en los resultados de la auditoría. Esta parte del informe es tan importante que a menudo a la totalidad del informe de auditoría se le conoce simplemente como la opinión del auditor. La intención es mostrar que las conclusiones se basan a un juicio profesional.
- **Nombre del despacho del CPC:** El nombre identifica el despacho del CPC o la persona que practico la auditoría, toda vez que este es el que tendrá la responsabilidad legal y profesional para asegurar que la calidad de la auditoría satisface las normas profesionales.
- **Fecha del informe de auditoría.**- La fecha apropiada del informe es aquella la que el auditor ha completado los procedimientos de auditoría más importantes en el campo, y que marca el último día de responsabilidad del auditor hacia la revisión de los eventos significativos que ocurrieron después de la fecha de los estados financieros. (Arens, Elder, & Beasley, Auditoria,Un enfoque integral, 2007)

c) Dictamen / Opinión

> El dictamen estándar tiene su origen en los Estados Unidos en la década de la Gran Depresión, cuando la bolsa de Nueva York (New York Stock Exchange) y el Instituto Americano de Contadores Públicos (American Institute of Certified Public Accountants AICPA), unieron sus propósitos para lograr uniformar todos los dictámenes de los Contadores Públicos que eran presentados acompañando a los Estados Financieros de las Compañías inscritas en la bolsa. (Auditores & Gerentes. Contadores Publicos Ltda, 2017)

El dictamen u opinión es la conclusión a la que ha llegado el auditor de acuerdo al examen o la revisión previa, es algo primordial dentro de las empresas hoy en día, realizar una auditoría externa y que esta arroje resultados significativos que ayuden a la empresa a tener un adecuada información financiera confiable que promuevan el cumplimiento de su objetivos organizacionales.

a.1 Definición

> El dictamen es el documento que suscribe el contador público conforme a las normas de su profesión, relativo a la naturaleza, alcance y resultado del examen realizado sobre los estados financieros de la entidad que se trate. La importancia del dictamen en la práctica profesional es fundamental, ya que usualmente es lo único que el público conoce su trabajo. (Santillana, 2004, pág. 168)

d) Tipos de Dictamen / Opinión

a.1 Dictamen limpio o sin salvedades

Es aquel que emite el contador público cuando durante el desarrollo de su examen no se encontró desviación en la aplicación de principios de contabilidad ni se le presentaron limitaciones a su trabajo, ya sea impuesta por la entidad auditada o por las circunstancias. Dicho en otras palabras, este dictamen se emite cuando el auditor encontró razonablemente bien y pudo llevar a cabo su trabajo son contratiempos.

- **Dictamen con salvedades**

Es aquel que emite el contador público cuando detecto desviaciones en la aplicación de principios de contabilidad, o cuando se le presentaron limitaciones en el alcance del examen practicado. Cuando existan desviaciones en la aplicación de dichos principios contables, el auditor deberá describir en forma precisa en qué consisten, cuantificar su efecto en los estados financieros y su efecto neto. Si las referidas salvedades no pueden cuantificarse razonablemente así deberá indicarse en su dictamen.

- **Dictamen negativo**

El auditor debe expresar una opinión negativa o adversa, cuando, como consecuencia de su examen, concluye que los estados financieros no están de acuerdo con los principios de contabilidad, y las desviaciones son a tal grado importante que la expresión de una opinión con salvedades no sería adecuada. El hecho de expresar una opinión negativa no eximirá al auditor de la obligación de revelar todas las desviaciones importantes que haya tenido en el alcance de su trabajo.

- **Abstención de opinión**

El auditor debe abstenerse de expresar una opinión cuando el alcance de su examen haya sido limitado en forma tal que no proceda la emisión de un dictamen con salvedades. En este caso, deberá indicar todas las razones que dieron lugar a dicha abstención. La abstención de opinión no debe usarse en sustitución de una opinión negativa.

- **Opinión Adversa**

Se usa cuando el auditor cree, que la información en su conjunto tiene errores importantes o son engañosos y no presentan de manera objetiva la información. Este tipo de opinión es poco usada.

Dentro de cada dictamen que emite el auditor lo debe realizar de una manera independiente y sin afinidad a ningún empleado o directivo de la empresa para que de esa forma no exista conflicto de intereses, y así emitir un informe con total transparencia, reflejando la integridad y confiabilidad en los resultados encontrados mediante la auditoría.

2.3. Base Legal

2.3.1. Código Orgánico Integral Penal

- **Art.190.- Apropiación Fraudulenta por medios electrónicos.-** La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando , manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. (COIP, 2014).

Los medios electrónicos en la actualidad constituyen un gran campo de intromisión y acceso a los sistemas para el cometimiento de fraudes o delitos informáticos, no es tarea fácil la investigación de los mismos, porque se debe realizar una revisión exhaustiva para la determinación de sanciones como en la actualidad ya existen.

> La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes. (COIP, 2014).

Dentro del Código Orgánico Integral Penal dentro de la Sección Tercera donde se tipifica los Delitos contra la seguridad de los activos de los sistemas de información y comunicación se mencionan los siguientes artículos:

- **Art.229.- Revelación ilegal de la base de datos.-** La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. (COIP, 2014).

La información de las empresas se debe considerar en el grado de confidencial, para que ninguna persona sea esta empleada de la organización, pueda otorgar o revelar información importante a u tercero buscando un beneficio económico, donde ya se rompe un principio fundamental dentro de cada empresa como es la lealtad hacia el patrono.

- **Art.232.- Ataques a la integridad de los sistemas informáticos.-** La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático, o de telecomunicaciones a todo o partes de sus componentes lógicos que los rigen, será sancionada con pena privativa de libertad de tres a cinco años. (COIP, 2014)

Es muy importante que dentro de las leyes jurídicas del país como se contempla en el COIP, se sancionen a quienes cometan intromisiones dentro de los sistemas de información y datos de las empresas, provocando daños informáticos y económicos que afectarían de manera importante de acuerdo al tamaño del impacto o fraude informático.

- **Art.234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.-** La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente al acceso logrado, modificar un portal web, desviar o redireccionar de

> tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años. (COIP, 2014).

Es legítimo que dentro de la administración de la justicia y por la transformación de la tecnologías de información y comunicación se incluya una sanción a quienes que sin autorización accedan a los sistemas de las empresas o de una persona, para la obtención de información que lo pueda utilizar de manera malintencionada y maliciosa, con el fin de conseguir un pago económico, todo esto debido a la.

CAPÍTULO III

3. METODOLOGÍA

3.1. Tipos y diseño de Investigación

3.1.1. Tipo de Investigación

El presente proyecto de investigación está fundamentado en un estudio de campo, es decir es de tipo exploratorio, el mismo que se basa en un diseño de investigación transaccional, con la finalidad de obtener información pertinente, suficiente y relevante, sobre nuestro problema principal, recolectando información que nos ayude a establecer juicios de valor y comparaciones pertinentes.

La investigación está encaminado al análisis cuantitativo, para lo cual se realizara un análisis de medición profundo entre la variable independiente y dependiente previamente mencionadas como es el (Fraude Informático y la Vulnerabilidad de las empresas del sector industrial).

Por lo tanto para la ejecución del presente proyecto de investigación se utilizara los siguientes tipos de investigación los cuales se detalla a continuación cada uno de ellos.

a) Investigación bibliográfica documental

Según Díaz, Escalona, Ricalde, León & Ramírez (2015) en su libo de Metodología de Investigación, menciona que la Investigación bibliográfica documental: “se basa en análisis de datos obtenidos de diferentes fuentes de información” (pág. 25)

Según los autores antes mencionados manifiestan que las principales fuentes bibliográficas documentales son”:

- Documentos escritos (libros, periódicos, revistas, actas, notariales, tratados, conferencias transcritas, entre otros.)
- Documentos fílmicos (películas Diapositivas, filmaciones, entre otros)
- Documentos gravados (discos, cintas, casetes, disques, entre otros.) (pág. 25).

Por lo tanto se dice que una investigación bibliográfica documental está basada en varias fuentes de información, donde nos ayudara a consultar varias bibliografías y otros materiales de utilidad para cumplir con el propósito de nuestra investigación.

b) Investigación de Campo

Según Baena (2014) considera que “Las técnicas específicas de la investigación de campo, tienen como finalidad recoger y registrar ordenadamente los datos relativos al tema escogido como objeto de estudio. La observación y la interrogación son las principales técnicas que usaremos en la investigación”. (pág. 12)

Para realizar una investigación de campo también debemos guiarnos en sus principales fuentes como son:

- Observación
- Entrevista
- Encuestas
- Cuestionarios

Para la ejecución de nuestro proyecto es necesario utilizar este tipo de investigación, como es la investigación de campo, debido a que la información relativa a nuestra investigación es la recolección de datos directos en escenario real, es decir de esta manera se recopilara la información más relevante y necesaria la cual nos ayudara a cumplir con nuestros objetivos de investigación.

c) Investigación Descriptiva

Según Quezada (2010) menciona que “La investigación descriptiva comprende la descripción, registro, análisis, e interpretación de la naturaleza actual y la composición o procesos de los fenómenos; la investigación descriptiva trabaja sobre realidades de hechos y sus característica fundamental es presentarnos una interpretación correcta”. (pág. 26)

Una investigación descriptiva en si comprende un análisis general de los resultados obtenidos en una investigación, con la finalidad de tener una comprensión especifica del fenómeno que se está investigando.

d) Investigación Analítica

Según Hurtado de Barrera (2000) en su libro de Metodología de Investigación Holística, manifiesta que: “la investigación analítica incluye tanto el análisis como la síntesis. Es decir significa desintegrar o descomponer una totalidad en sus partes para estudiar en forma intensiva uno de sus elementos y la relación de estos elementos entre sí”. (pág. 69).

Por lo tanto se puede decir que una investigación analítica tiene como objetivo principal analizar un evento de una manera minuciosa o específica y comprenderlo cada uno de sus objetos.

3.1.2. Diseño de la Investigación

Según Fassio, Pascual & Suarez (2006) en el libro de Introducción a la Metodología de la Investigación, menciona que “el diseño de la investigación puede definirse como la planificación de las actividades que deben llevarse a cabo para solucionar los problemas o contestar a preguntas planteadas en la investigación” (pág. 42)

Este proyecto de investigación tiene un diseño de investigación no experimental debida a que está enfocado a una investigación de campo, donde se empleara encuestas.

> Los diseños no experimentales son aquellos que no incorporan los elementos de control disponibles en los diseños anteriores. No se controlan y manipulan las variables no se utiliza un grupo de control, no se asigna aleatoriamente los sujetos y no se pretende medir la reacción causa – efecto entre una variable dependiente y una independiente. (Fassio, Pascual, & Suarez, 2006, pág. 50)

Según estos mismos autores menciona que los diseños no experimentales realizan las siguientes actividades.

- Ofrecen información sobre cómo se manifiestan y que características tienen los procesos que desembocan en un proceso determinado.
- Pretenden descubrir si los componentes de un cierto fenómeno están relacionados entre sí.
- Permiten entender las complejas interacciones que se producen entre los grupos humanos.
- Por todas las razones mencionadas, sus resultados no son generalizables, pero resultan de gran utilidad para la toma de decisiones. (pág. 51)

A continuación describiremos algunos de los diseños no experimentales como son:

- Diseño Longitudinal
- Diseño Transversal
- Diseño de estudio de casos
- Diseño de estudios Etnográficos

En la investigación se aplicara el diseño de estudio de casos, debido a que implica el estudio a profundidad sobre las características de un fenómeno determinado para facilitar su comprensión y una mayor perspectiva.

> En general persigue los siguientes objetivos: registrar los hechos los hechos tal y como han sucedido, describir situaciones, brindar conocimiento. Acerca del fenómeno no estudiado y/ o comprobar o

> contrastar ciertos efectos, relaciones o hipótesis dentro de contextos diversos. (pág. 52)

Un caso puede ser una persona, un programa, una situación, un acontecimiento particular, un barrio, una comunidad, una organización en su conjunto o unidades o actividades específicas dentro de una organización.

a) Niveles de Investigación

La investigación tiene un nivel exploratorio, debido a que nuestro tema es conocer los fenómenos realmente desconocidos, obteniendo información relevante sobre el contexto a investigar.

Según Hernández, Fernández & Baptista (2006) en su libro de Metodología de la Investigación, menciona que: “Los estudios exploratorios se realizan 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” (pág. 100).

Por lo tanto se dice que los estudios exploratorios sirven para familiarizarnos con fenómenos relativamente desconocidos, obtener información sobre la posibilidad de llevar a cabo una investigación más completa respecto de un contexto particular, investigar nuevos problemas, identificar conceptos o variables promisorias, establecer prioridades para investigaciones futuras, o sugerir afirmaciones y postulados.

Según Bonilla, Hurtado & Jaramillo (2009) en su libro de La Investigación (Aproximaciones a la construcción del conocimiento Científico), mencionan que: “existe varios niveles de investigación los cuales se detallan a continuación” (pág. 158).

- El primer nivel de investigación, es el cotidiano, es el “aspectual”, en el que es suficiente la apariencia o el aspecto de “algo”.
- El segundo nivel se descubre que el aspecto de los “algos” depende del contexto.

- En un tercer nivel surge la pregunta acerca del porqué o en razón de qué algo tiene tal o cual aspecto dentro de un contexto dado.
- El cuarto nivel es el “sistémico” o “estructural”, en el cual los “algos” se ven como sistemas constituidos de una cierta sustancia (sus componentes están organizados de acuerdo con ciertas relaciones (la estructura)). (pág. 158)

3.2. Población y Muestra

3.2.1. Población

Según Leiva (2002) en su obra de Nociones de Metodología de Investigación Científica, menciona que: “la población es el universo de todo un grupo de personas u objetos que poseen alguna característica común. Igual denominación se da al conjunto de datos que se han obtenido en una investigación” (pág. 36).

> La población es un conjunto de elementos reunidos por el interés de estudio de un investigador. Aunque el término población se asocia corrientemente con conjunto de personas, en estadística su uso se ha extendido a conjuntos de elementos de cualquier naturaleza. Lo importante es el interés que despierte en correspondencia con los objetivos de una investigación. (Ortiz, 2013, pág. 23).

Por lo tanto se puede mencionar que la población es una totalidad del objetivo a investigar, pero para la ejecución de esta investigación se tomara una pequeña parte llamada muestra tomando como referencia para la investigación, comprenderá totas las empresas industriales de la Provincia de Cotopaxi que posean TIC, debido a que constituyen los actores principales de la investigación.

Tabla 4

Empresas del sector industrial

N°	DENOMINACIÓN	CIUDAD	ACTIVIDAD ECONÓMICA
1	CARNIDEM CIA. LTDA.	LATACUNGA	C1010.22 - Fabricación de productos cárnicos, embutidos, etc.
2	INDUSTRIA DE LICORES ECUATORIANOS LICOREC S.A.	LATACUNGA	C1101.02 - Elaboración de mezcla de bebidas alcohólicas destiladas y preparados alcohólicos.
3	HISPANALIBROS CIA. LTDA.	LATACUNGA	C1811.02 - Actividades de impresión de libros, diccionarios, enciclopedias y folletos.
4	IMPORTADORA ADRIÁN IMCEAL CIA. LTDA.	LA MANÁ	C1410.02 - Fabricación de prendas de vestir de telas tejidas, de punto y ganchillo.
5	DLIP INDUSTRIAL S.A.	TANICUCHI	C1030.11 - Elaboración de alimentos compuestos (mezcla) principalmente de frutas legumbres u hortalizas.
6	ANDES KINKUNA S.A.	PUJILI	C1079.29 - Elaboración de otros alimentos especiales: concentrados de proteínas; alimentos preparados con fines dietéticos.
7	MOLINOS POULTIER S.A.	LATACUNGA	C1061.11 - Molienda de cereales, producción de harina, semolina, sémola y gránulos de: trigo, centeno, avena, maíz y otros cereales.
8	INDUACERO INDUSTRIA DE ACERO DEL ECUADOR CIA. LTDA.	LATACUNGA	C2512.01 - Fabricación de tanques, depósitos y recipientes similares de metal, del tipo habitualmente utilizado para almacenamiento y elaboración.
9	CONSTRUCCIONES ULLOA CIA. LTDA.	LATACUNGA	C2813.02 - Fabricación de bombas para líquidos, dispositivos de medición.
10	EDITORIAL LA GACETA S.A.	LATACUNGA	C1811.01 - Actividades de impresión de periódicos, revistas y otras publicaciones periódicas.
11	CALZACUBA CIA. LTDA.	LATACUNGA	C1520.01 - Fabricación de calzado, botines, polainas y artículos similares para todo uso.

Continúa

12	CEDAL S.A.	LATACUNGA	C2420.23 - Producción de aleaciones de: aluminio; plomo, zinc, estaño, cobre, etcétera.
13	FUENTES SAN FELIPE S.A.	LATACUNGA	C1104.02 - Producción de aguas minerales naturales y otras aguas embotelladas.
14	ALIAGUASANTA CIA. LTDA.	SALCEDO	C1010.22 - Fabricación de productos cárnicos: salchichas, salchichón, chorizo.
15	LA FINCA CIA. LTDA.	LATACUNGA	C1050.04 - Elaboración de mantequilla, queso, cuajada y suero.
16	NOVACERO S.A.	LASSO	C2410.22 - Fabricación de barras, varillas y secciones sólidas de hierro.
17	EL RANCHITO CIA. LTDA.	SALCEDO	C1010.22 – Elaboración de productos lácteos y derivados.
18	PRODICEREAL S.A.	LATACUNGA	C1061.11 - Molienda de cereales, producción de harina, semolina, sémola y gránulos de: trigo.
19	AGLOMERADOS COTOPAXI S.A.	LASSO	C1621.01 - Fabricación de hojas de madera reforzadas con papel cortadas en figuras.
20	CORPICECREAM S.A.	SALCEDO	C1050.05 - Elaboración de helados (de todo tipo), sorbetes, bolos, etcétera.
21	INDULAC CIA LTDA.	LATACUNGA	C1050.01 - Elaboración de leche fresca líquida, crema de leche líquida, bebidas a base de leche.
22	MOLINOS OROBLANCO CIA. LTDA.	LATACUNGA	C1061.11 - Molienda de cereales, producción de harina.
23	PARMALAT	LASSO	C1050.01 - Elaboración de leche fresca líquida, crema de leche líquida, bebidas a base de leche, yogurt.
24	PROVEFRUT S.A.	LATACUNGA	C1030.12- Elaboración de productos alimenticios, conservación de frutas.
25	FAMILIA SANCELA S.A.	LASSO	C1709.11 - Fabricación de productos de papel de higiene personal y pañuelos de limpieza.

Fuente: (Superintencia de Compañias, Valores y Seguros, 2015)

3.2.2. Muestra

Según Hernández, Fernández & Baptista (2006) en su libro de Metodología de la Investigación, menciona que “la muestra es en esencia un subgrupo de la población. Digamos que es un subconjunto de elementos que

pertenecen al conjunto definido en sus características al que llamamos población” (pág. 240).

De acuerdo a la definición de varios autores se puede mencionar que la muestra es una parte o un subgrupo de una población, lo cual se toma de referencia para una investigación, estas muestras pueden ser de personas, cosas, animales, entre otros.

a) Pasos para la selección de la muestra

Definir la población, identificar el marco muestral, determinar el tamaño de la muestra, elegir el proceso de muestreo, seleccionar la muestra.

b) Calculo de la muestra

La muestra para la presente investigación es calculada de manera intencional, debido a que se ha tomado como población todas las empresas del sector industrial de la provincia de Cotopaxi que posean TIC, o un mínimo de inversión en tecnologías, para lo cual se ha realizado sus respectivos cálculos de acuerdo a información obtenida de diferentes fuentes, de esa manera determinar qué valor tienen en inversión en equipo de cómputo o sistemas de información.

Además se toma un porcentaje aleatorio, donde las empresas que posean mayor o igual al 0.9% en inversión en equipo de cómputo del total de propiedad planta y equipo serán sujetas como muestra para nuestra investigación.

Tabla 5

Empresas del Sector Industrial

N°	Denominación	Edificios y Otros Inmuebles Costo Histórico	Maq. Equipo y Otras Insta. Costo Histórico	Muebles y Enseres	Otras PP&E	Equipo Computo	TOTAL	% Inversión
1	**CARNIDEM CIA. LTDA.**	$ 97.500,00	$ 810.266,44	$ 7.596,20	$ 0,00	**$ 16.758,01**	$ 932.120,65	**1,80%**
2	**LICOREC S.A.**	$ 230.808,89	$ 959.749,23	$ 42.522,89	$ 214.841,33	**$ 97.493,21**	$ 1.545.415,55	**6,31%**
3	**IMP.ADRIAN IMCEAL**	$ 0,00	$ 2.292,37	$ 6.040,51	$ 0,00	**$ 4.737,75**	$ 13.070,63	**36,25%**
4	**DLIP INDUSTRIALS.A.**	$ 219.000,00	$ 1.314.842,48	$ 13.661,28	$ 3.916,48	**$ 15.501,48**	$ 1.566.921,72	**0,99%**
5	**MOLINOS POULTIER S.A.**	$ 587.338,44	$ 2.569.992,31	$ 33.860,34	$ 0,00	**$ 183.064,20**	$ 3.374.255,29	**5,43%**
6	**INDUACERO CIA. LTDA.**	$ 508.888,58	$ 664.474,91	$ 11.793,86	$ 0,00	**$ 16.159,67**	$ 1.201.317,02	**1,35%**
7	**CONSTRUC. ULLOA**	$ 0,00	$ 197.509,58	$ 0,00	$ 13.396,05	**$ 2.065,00**	$ 212.970,63	**0,97%**
8	**EDITORIAL LA GACETA S.A.**	$ 70.243,60	$ 35.000,00	$ 1.845,00	$ 3.480,32	**$ 25.440,85**	$ 136.009,77	**18,71%**
9	**CALZACUBA CIA. LTDA.**	$ 0,00	$ 25.241,13	$ 13.645,17	$ 0,00	**$ 7.260,74**	$ 46.147,04	**15,73%**
10	**CEDAL S.A.**	$ 5.501.819,58	$ 0,00	$ 109.492,84	$ 0,00	**$ 638.071,29**	$ 6.249.383,71	**10,21%**
11	**FUENTES SAN FELIPE S.A.**	$ 503.417,57	$ 350.073,32	$ 60.670,93	$ 21.040,55	**$ 68.555,72**	$ 1.003.758,09	**6,83%**
12	**NOVACERO S.A.**	$ 21.798.024,79	$ 91.555.522,89	$ 1.202.615,80	$ 1.014.822,40	**$ 1.120.705,28**	$ 116.691.691,16	**0,96%**
13	**EL RANCHITO CIA. LTDA.**	$ 1.586.412,57	$ 5.216.384,54	$ 29.561,89	$ 6.444,32	**$ 65.048,06**	$ 6.903.851,38	**0,94%**
14	**PRODICEREAL S.A.**	$ 681.748,44	$ 336.615,86	$ 53.407,77	$ 0,00	**$ 13.721,58**	$ 1.085.493,65	**1,26%**
15	**AGLOMERADOS**	$ 3.476.865,13	$ 22.282.083,53	$ 425.214,11	$ 0,00	**$ 847.522,57**	$ 27.031.685,34	**3,14%**
16	**CORPICECREAM S.A.**	$ 131.092,29	$ 208.211,53	$ 20.543,58	$ 0,00	**$ 12.731,43**	$ 372.578,83	**3,42%**
17	**MOLINOS OROBLANCO**	$ 0,00	$ 168.588,86	$ 1.840,08	$ 0,00	**$ 1.187,36**	$ 171.616,30	**0,69%**
18	**PARMALAT DEL ECUADOR**	$ 1.951.086,55	$ 7.123.863,81	$ 67.133,83	$ 0,00	**$ 114.719,36**	$ 9.256.803,55	**1,24%**
19	**PROVEFUT S.A.**	$ 3.349.088,16	$ 12.089.095,23	$ 15.987,30	$ 34.980,00	**$ 181.870,46**	$ 15.671.021,15	**1,16%**
20	**FAMILIA SANCELA S.A.**	$ 9.104.462,17	$ 40.580.996,81	$ 1.212.590,13	$ 0,00	**$ 2.064.542,26**	$ 52.962.591,37	**3,90%**

Fuente: (Superintencia de Compañias, Valores y Seguros, 2015)

3.3. Técnicas e Instrumentos de recolección de datos

Para la ejecución de nuestra investigación se utilizara encuestas para la recolección de información necesaria para cumplir con los objetivos específicos de nuestro proyecto.

- **Encuesta**

> La encuesta es una forma de entrevista planeada que por ende persigue un fin, lograr la información mediante datos que se obtienen a través de preguntas similares que se formulan a personas que están involucradas en lo que se investiga, cuyas respuestas tienen que ser cuantificadas para que a través de los resultados muestren una realidad. (Moreno, 2000, pág. 94).

Entonces la encuesta es una técnica que congrega hechos para expresar una investigación, ya que a través de ello podemos conocer y cuantificar los las inquietudes de nuestra infestación.

3.3.1. Instrumento de Investigación

Esta investigación tiene una modalidad cuantitativa, debido a que se utilizará como instrumentó de investigación un cuestionario, que tendrá una serie de preguntas de diferentes tipos como serán cerradas, abiertas y de escala.

> El cuestionario es un conjunto de preguntas diseñadas para generar los datos necesarios, con el propósito de alcanzar los objetivos del proyecto de investigación. Se trata de un plan formal para recabar información de la unidad de análisis objeto de estudio y centro del problema de investigación. (Bernal, 2010, pág. 250).

En general, un cuestionario consiste en un conjunto de preguntas respecto a una o más variables que van a medirse. Por lo tanto se puede decir que un cuestionario permite estandarizar y uniformar el proceso de recopilación de datos.

a) Criterios básicos para el diseño de un cuestionario

> Antes de iniciar la elaboración de un cuestionario, es necesario tener claros los objetivos y las hipótesis o preguntas de investigación que impulsan a diseñar el cuestionario. Además, es preciso tener cierta seguridad de que la información podrá conseguirse usando los métodos de que se dispone y requiere el objeto de estudio. (Bernal, 2010, pág. 251).

Ibídem menciona que “cuando se prepara un instrumento para recabar datos, deben examinarse los siguientes aspectos básicos que se mencionan a continuación” (pág. 251).

- La naturaleza de la información que se busca.
- La naturaleza de la población o muestra de sujetos que aportarán la información.
- El medio o los medios de aplicación del instrumento. (pág. 251)

Ibídem considera que “existe básicamente, existen tres tipos de preguntas: abiertas, cerradas y de respuesta a escala”:

- Preguntas **abiertas:** Este tipo de preguntas le permiten al encuestado contestar en sus propias palabras, es decir, el investigador no limita las opciones de respuesta.
- Las preguntas **abiertas** ofrecen diversas ventajas para el investigador. Permiten que las personas entrevistadas indiquen sus reacciones generales ante un determinado aspecto o rasgo.
- Preguntas **cerradas:** Le solicitan a la persona encuestada que elija la respuesta en una lista de opciones. La ventaja de este tipo de preguntas es que se elimina el sesgo del entrevistador, que es muy común en las preguntas abiertas; además, son fáciles de codificar y se obtienen respuestas muy concretas.
- Preguntas de **respuesta a escala:** Son aquellas preguntas básicamente dirigidas a medir la intensidad o el grado de sentimientos respecto a un rasgo o a una variable por medir; usualmente se les conoce como escalas de medición de actitudes, entre las cuales la más común es la escala de Likert. (pág. 252)

Ibídem manifiesta que “Las preguntas cerradas se subdividen en dos clases dicotómicas y de opción múltiple”:

- **Dicotómicas:** es el tipo más sencillo de preguntas cerradas. Por ejemplo: En ocasiones se agrega una opción neutra o la opción “sin opinión/no sabe” a las preguntas dicotómicas.
- **De opción múltiple:** como todas las preguntas cerradas, las de opción múltiple proporcionan información limitada, y se le pide al entrevistado que indique la alternativa que exprese su opinión o, en algunos casos, es necesario indicar varias opciones. (Bernal, 2010)

3.4. Diseño de la Encuesta

La técnica que se va utilizar para la presente investigación será una encuesta ya que este método es una búsqueda sistemática de información en la que se detallara cada una de las preguntas o incógnitas, sobre los datos que desea conocer.

Es de vital importancia recordar que la encuesta además de ser una técnica de recolección de datos, es muy utilizada por su gran versatilidad en la obtención de información dentro de diferentes campos de investigación, ya que de esa manera podemos palpar los problemas reales en los ámbitos sociales, políticos, tecnológicos, demográficos y económicos, debido a que hoy en la actualidad el mundo se encuentra en constante cambio y desarrollo gracias al avance de la tecnología. Posteriormente se procederá a reunir todas las encuestas realizadas a cada una de las empresas del sector industrial de la Provincia de Cotopaxi, con la finalidad de conocer la información más relevante sobre el tema que se está realizando la presente investigación.

3.5. Auditoría Informática

PA - 1/1

CALZACUBA CIA. LTDA.
AUDITORÍA INFORMÁTICA

PROGRAMA DE AUDITORÍA INFORMÁTICA PARA EL DEPARTAMENTO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN (TIC)

DEL 1 DE ENERO AL 31 DE DICIEMBRE DE 2017

OBJETIVO: Determinar la vulnerabilidad de los sistemas informáticos de la empresa CALZACUBA CIA. LTDA. En el periodo 2012 – 2016.

Tabla 6
Programa de auditoría

N°	Procedimientos	Referencia P/T	Elaborado por	Fecha
1	Verificar el monto de inversión en Tecnología de Información y Comunicación (TIC) por medio de los estados financieros de la empresa.	CS - 1/1	DFPD	14/08/2017
2	Solicitar al encargado del Departamento/Área de Tecnología de Información y Comunicación (TIC). la lista de equipos que se usen, cuantos usuarios la usan y cuantas horas al día son usados estos equipos	LE - 1/1	KGQZ	14/08/207
3	Elaboración de Cuestionarios de Control Interno al Departamento/Área de Tecnología de Información y Comunicación.	CCI - 1/3	KGQZ	15/08/207

Continúa

4	Aplicación de Cuestionarios de Control Interno al Departamento/Área de Tecnología de Información y Comunicación (TIC).	**CCI - 1/3** **MCR -1/1**	DFPD	16/08/207
5	Realizar un examen especial a los sistemas más vulnerables del Departamento/Área de Tecnología de Información y Comunicación (TIC).	**EXE - 1/4**	DFPD	16/08/207
6	Análisis Forense de los sistemas operativos dentro del área de TIC.	**AF - 1/4**	KGQZ	16/08/207
7	Elaboración de una hoja de Hallazgos de los resultados obtenidos.	**HH - 1/3**	KGQZ	18/08/207
8	Elaboración de un Informe de Auditoria de los resultados obtenidos.	**IA - 1/7**	DFPD	21/08/207

Elaborado por: K.G.Q.Z. – D.F.P.D	Fecha: 14/08/2017
Revisado por : L.A.L.C	Fecha: 15/08/2017

Tabla 7
Cédula Sumaria

CS - 1/1

EMPRESA CALZACUBA CIA. LTDA						
CÉDULA SUMARIA DE LA CUENTA EQUIPO DE COMPUTO						
AL 31 DE DICIEMBRE DEL 2016						
AÑO	CUENTAS	REF P/T	S/S CONTABILIDAD	ASIENTOS DE RECLASIFICACIÓN		S/S AUDITORÍA
				DEBE	HABER	
2012	Equipo de Computo	EEFF- 1/5	$ 4.375,03			$ 4.375,03
2013	Equipo de Computo	EEFF- 2/5	$ 4.571,46			$ 4.571,46
2014	Equipo de Computo	EEFF- 3/5	$ 4.571,46			$ 4.571,46
2015	Equipo de Computo	EEFF- 4/5	$ 7.010,74			$ 7.010,74
2016	Equipo de Computo	EEFF- 5/5	$ 7.260,74			$ 7.260,74
						$ 27.789,43
Elaborado por: K.G.Q.Z. – D.F.P.D				Fecha: 14/08/2017		
Revisado por : L.A.L.C				Fecha: 15/08/2017		

Tabla 8
Abreviaturas

LISTA DE ABREVIATURAS

PA	Programa de Auditoría
CS	Cedula Sumaria
LE	Lista de Equipos
CCI	Cuestionario de Control Interno
MCR	Matriz de Calificación del Nivel de Confianza y Riesgo
EXE	Examen Especial
AF	Análisis Forense
HH	Hoja de Hallazgo
IA	Informe de auditoría
EEFF	Estados Financieros
Ref./PT	Referencia Papel de Trabajo
LALC	Luis Alfonso Lema Cerda
DFPD	Diego Fernando Pinsha Defaz
KGQZ	Kleber Gonzalo Quevedo Zambonino
Elaborado por: K.G.Q.Z. – D.F.P.D	Fecha: 14/08/2017
Revisado por : L.A.L.C	Fecha: 15/08/2017

CALZACUBA CIA. LTDA.

LE - 1/1

AUDITORÍA INFORMÁTICA

LISTA DE EQUIPOS DEL DEPARTAMENTO O ÁREA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN

Tabla 9

Lista de Equipos

Lista de Equipos					
Nº	**Nombre del equipo de Computo**	**Responsable**	**Marque con una X**		**Horas de Uso**
			Uso Único	**Compartido**	
1	Servidor		X		24
2	Computador HP	Marco Acuña		X	10
3	Computador SONY	Pamela Bautista	X		10
4	Computador LG	Jessy Moreno	X		10
5	Computador SAMSUNG	José Bautista	X		10
6	Impresora EPSON Matricial	Todos		X	10
7	Impresora EPSON	Todos		X	10
8	Teléfono Fijo PANASONIC	Todos		X	10
9	2 Cortapicos	Todos		X	10
Elaborado por: K.G.Q.Z. – D.F.P.D			Fecha: 14/08/2017		
Revisado por: L.A.L.C			Fecha: 15/08/2017		

3.5.1. Elaboración y Aplicación del Cuestionario de Control Interno

CCI - 1/3

Tabla 10
Cuestionario de Control Interno

CALZACUBA CIA. LTDA.					
MATRIZ DE CALIFICACIÓN DE RIESGO Y CONFIANZA			**AUDITOR:** DP- KQ		
CUESTIONARIO DE CONTROL INTERNO			**FECHA:** 16/08/2017		
N°	PREGUNTAS	PONDERACIÓN	**RESPUESTAS**		CALIFICACIÓN
			SI	NO	
DEPARTAMENTO/ÁREA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN.		**PT**			**CT**
SUMAN:					
PROCESOS INTERNOS					
1	¿Existe una persona responsable o encargada del área o departamento de TIC?	1		X	0
2	¿El área de TIC forma parte de la estructura organizacional de la empresa?	1		X	0
3	¿Existe un organigrama con la estructura del área de TIC?	1		X	0
4	¿Existe lealtad o confidencialidad con respecto a la información de la empresa?	1		X	0
5	¿La instalación eléctrica de los equipos de cómputo es independiente de otras instalaciones?	1		X	0
6	¿Se han instalado equipos que protejan la información y los dispositivos en caso de variación de voltaje como: reguladores de voltaje, supresores pico, generadores de energía?	1		X	0
7	¿Se efectúan respaldos físicos o digitales de la información?	1		X	0
8	¿La empresa posee cámaras web o servidores de video?	1		X	0
9	¿Se realizan informes periódicos del rendimiento de los sistemas informáticos?	1		X	0
10	¿Existe una adecuada capacitación para el manejo de los sistemas informáticos a los usuarios dentro de la empresa?	1		X	0

Continúa

CCI - 1/2

11	¿Cuenta los sistemas de la empresa con claves de seguridad?	1		X	0
12	¿Se realiza un adecuado mantenimiento a los sistemas informáticos de la empresa?	1		X	0
13	¿Los sistemas pueden ser actualizados de acuerdo a los avances tecnológicos que se presentan?	1		X	0
14	¿Los sistemas dentro de la empresa cuentan con personal técnico que ayuden cuando se presente un problema?	1		X	0
15	¿Existe un manual o instructivo para el manejo y uso del Software informático?	1		X	0
16	¿Existen políticas para la seguridad de los sistemas informáticos?	1		X	0
17	¿Los sistemas informáticos cuentan licencia?	1	X		1
18	¿La empresa cuenta con un registro de accesos a la información de los sistemas informáticos para el personal?	1	X		1
19	¿La empresa posee sistemas protección como antimalware, antivirus y anti espías; frente a ataques informáticos?	1	X		1
20	¿Existe una conexión a red para dispositivos e impresoras empresa?	1	X		1
21	¿La empresa posee un software/ licencia para almacenar la información dentro de una nube?	1	X		1
22	¿Existe un lugar adecuado y estratégico para los sistemas informáticos?	1	X		1
23	¿Se realizan procedimientos de detección de inmunización de virus en copias no autorizadas o datos procesados en otros equipos?	1	X		1
24	¿La empresa cuenta con un formato de encriptación para la protección de sus datos?	1		X	0

Continúa

CCI - 1/2

25	¿Los sistemas de información implementados aseguran la calidad, pertinencia, veracidad, oportunidad, accesibilidad, transparencia, objetividad e independencia de la información?	1		X	0
26	¿La empresa realiza auditorias para asegurar la integridad y controles de seguridad a los sistemas de información?	1		X	0
27	¿El cableado dentro de la empresa se encuentra correctamente instalado para que no se produzca fuga de información?	1		X	0
28	¿La empresa cuenta con una aplicación de notificaciones en el caso de acceso indebido a la información?	1	X		1
29	¿Los usuarios tienen acceso a redes sociales?	1		X	0
30	¿La empresa posee un servidor central de datos?	1		X	0
Calificación Total Componente 1: CT					8
Ponderación total componente 1 : PT					30
Nivel de Confianza: NC = CT / PT * 100			NC= (8/30)*100= 60%		26,67
Nivel de riesgo inherente: RI = 100% - NC %			RI = 100% - 26,67% = 73,33%		73,33

Elaborado por: K.G.Q.Z. – D.F.P.D	Fecha: 14/08/2017
Revisado por : L.A.L.C	Fecha: 15/08/2017

EMPRESA CALZACUBA CIA. LTDA. **MCR - 1/1**

AUDITORÍA INFORMÁTICA

MATRIZ DE CALIFICACIÓN DEL NIVEL DE CONFIANZA Y RIESGO

DEL 01 DE ENERO AL 31 DE DICIEMBRE DE 2016

EQUIPO DE CÓMPUTO

1. Valoración

P.T = Ponderación Total.

C.T = Calificación Total.

C.P = Calificación Porcentual

C.P = C.T * 100 / P.T

C.P = 8*100/ 30 = 26.67%

2. Determinación de los niveles de riesgo

Tabla 11

Nivel de Confianza

BAJO	MODERADO	ALTO
15%-50%	51% - 75%	76% - 95%
85%-50%	49% - 25%	24% - 5%
ALTO	MODERADO	BAJO

Tabla 12

Nivel de Riesgo

NR=(100-NC)			
CT	8	RIESGO	ENFOQUE
PT	30		
NC	26.67%	BAJO	
RC	73.33%	ALTO	CUMPLIMIENTO

3. Conclusión

Del análisis realizado a la empresa Calzacuba Cía. Ltda., sobre el componente de tecnología de información y comunicación, se determinó que el nivel de confianza es Bajo con 26,67% y el riesgo de Seguridad es Alto con 73,33%; por lo que se pudo constatar que no existe un control eficiente en los sistemas de la parte operativa de la empresa, los mismos que recaen a ser inmersos a posibles ataques informáticos, y hacia y una posible inoperatividad de la organización.

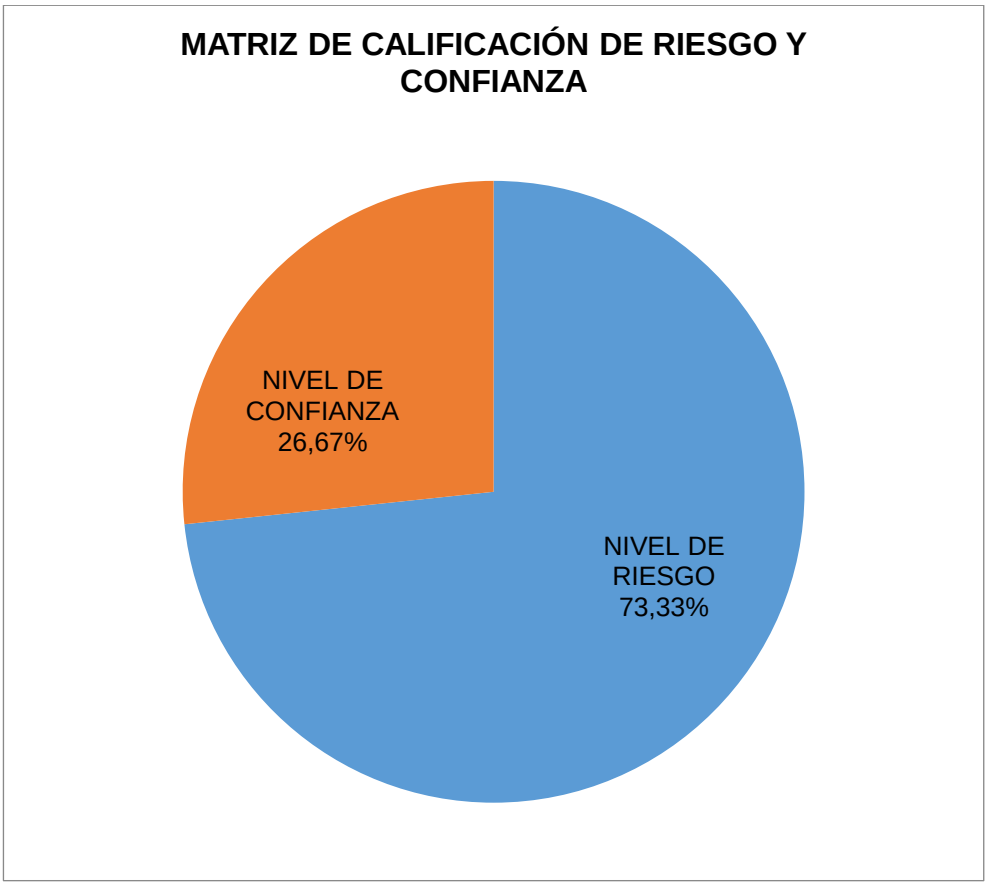


Figura 11 Matriz de Calificación de Riesgo y Confianza

3.6. Examen Especial

3.6.1. Examen especial a los sistemas más vulnerables del departamento/área de Tecnología de Información y Comunicación.

a) Motivo del examen

El examen especial se realizó a la empresa Calzacuba, en cumplimiento a la investigación denominada “Fraude informático, Análisis de vulnerabilidad de las empresas del sector industrial de la Provincia de Cotopaxi, dado a la circunstancias de haber encontrado hallazgos muy significativos durante la evaluación de control Interno lo cual permitió conocer múltiples vulnerabilidades que tenían los sistemas de información de la empresa antes mencionada.

b) Objetivos del Examen

- Determinar el grado de seguridad y confiabilidad de los sistemas informáticos de la empresa Calzacuba Cía. Ltda.
- Establecer si los sistemas informáticos fueron instalados de acuerdo a las necesidades de la empresa.
- Sugerir mejoras en los sistemas de protección, almacenamiento y procesamiento de la información de la empresa.

c) Alcance del Exámen

El examen especial se realizó al departamento/área de tecnología de información y comunicación de la empresa Calzacuba Cía. Ltda., por el periodo comprendido del 1 de enero del 2016 al 30 de junio del 2017.

d) Base legal

Mediante la autorización del Ingeniero José Bautista Gerente general de la de la empresa Calzacuba Cía. Ltda., y el Señor Marco Acuña administrador de la empresa, se procedió a revisión de dos computadores de

marca LG y SONY tomados como muestra para la revisión de los sistemas de información.

e) Estructura orgánica

La estructura orgánica de las unidades que intervienen en el proceso es la siguiente:

Gerente: Ingeniero José Bautista

Administrador: Señor Marco Acuña

Apoyo operativo: Señorita Pamela Bautista

Apoyo Administrativo: Ingeniera Jessy Moreno

f) Monto de los recursos examinados

Tabla 13

Montos de los recursos examinados

Cantidad	Descripción	Valor USD
1	Computador de escritorio marca LG, procesador de 64 bytes, memoria RAN de 4 GB con Windows 8.	900, 00 $
2	Computador portátil de marca SONY VAIO, procesador de 64 bytes, memoria RAN de 4 GB con Windows 10.	1.200,00 $

3.6.2. Resultados del Examen Especial

a) Grado de seguridad y confiabilidad

Mediante la revisión de los dos equipos tomados como muestra se pudo constatar que existen debilidades e inseguridad en el manejo de los sistemas y las aplicaciones informaticas que se utilizan dentro de cada uno de los ordenadores ya que nos revelaron las fallas inherentes y formas de ataques informáticos, que se pueden dar a través de las redes o sistemas de información, como es el caso de las redes sociales que están siendo blancos

de intromisión para la fuga o robo de información, de esa manera se puede medir que no se está invirtiendo lo suficiente en medidas tecnológicas.

De la misma manera se pudo determinar que los ordenadores no se encuentran actualizados debido a que las instalaciones de los navegadores web no poseen una protección cortafuegos que restringa el acceso a malware que puedan inhabilitar las operaciones de la empresa.

b) Sistemas Informáticos

Se pudo establecer que los sistemas informáticos van de acuerdo a la actividad de la empresa, obteniendo como herramienta principal y más utilizada el sistema Fénix que cuenta con todo los niveles de protección y seguridad en claves de acceso a la información, siendo un instrumento de fácil manejo con funcionalidades en la red e internet, conexión remota vía internet y soporte técnico.

c) Mejora en la protección de datos

Sugerir a la empresa responsable de la protección de la información que se almacena en la nube de datos y se realicen informes periódicos de las actividades ejecutadas a diario con la finalidad de tener como respaldo el cumplimiento de preservación de los datos de una manera responsable e integra.

Es recomendable mantener actualizados los sistemas y programas que se utilice a diario, sobre todo aquellos que permitan navegar por internet, puesto que son la puerta de entrada a los ordenadores donde se dan la mayoría de las posibles amenazas cibernéticas.

d) Conclusiones del Exámen Especial

- Podemos concluir que dentro del examen realizado a la empresa Calzacuba Cía. Ltda., se pudo identificar que la empresa no posee un departamento/área de TIC, además sus aplicaciones informáticas no

cuentan con control de spam, control de antivirus y una protección de los datos a través de un firewall que permita trabajar con la mayor seguridad y proteger posibles ataques cibernéticos por mafias internacionales.

e) Recomendaciones del Exámen Especial

- Se recomienda al administrador de la empresa mantener actualizado los firewalls o cortafuegos de manera anual ya que ayudaran a mantener a los ciberdelincuente alejados de la información de la empresa, prevenir ataques exteriores a las redes locales.
- Es recomendable no tener archivos adjuntos al correo electrónico de personas desconocidas, sospechosas, de una fuente de poca confianza o si el asunto del mensaje es dudoso, pueden contener "virus", los cuales podrían dañar su PC.
- Se recomienda a todos los usuarios que no se debe conectar un ordenador que contenga datos protegidos directamente a Internet, debido a que este debe estar en una red local protegida y aislada de Internet mediante un “cortafuegos” o firewall que le proteja de posibles atacantes.

3.7. Análisis Forense Digital

ANÁLISIS FORENSE

EMPRESA CALZACUBA CIA LTDA.

Dentro del Análisis Forense Digital, podemos destacar las siguientes fases, que serán desarrolladas con más detalle a lo largo de este documento:

a) IDENTIFICACIÓN DEL INCIDENTE/ FRAUDE

a.1 Cuál es la vulneración o fraude informático que tuvo su empresa

Encriptación de la información e inhabilitación de los sistemas de operatividad dentro de la empresa.

b.1 Es la primera que se suscita este incidente informático.

Primera vez.

b) RECOPILACIÓN DE EVIDENCIAS

a.1 En qué fecha se generó el robo de la información.

La fecha en la que se realizó el fraude fue a inicios del año 2017 en enero para ser más específicos.

b.1 De qué manera identificaron el acceso o robo a la información.

Según la información proporcionada por la empresa, con la inhabilitación de los sistemas los cuales no podían ingresar para realizar sus actividades diarias, mucho menos al paquete de Microsoft Office, se encontraban totalmente bloqueadas.

c.1 Se identificó el responsable del ataque o vulneración a sus sistemas

De manera concreta el administrador de la empresa no supo manifestar que fue provocado por una mafia internacional, que pedía un pago de dinero para des-encriptar la información y poder acceder a sus sistemas, pero el Sr, Administrador nos comentaba que había tenido una charla de prevención en agosto del año 2016 acerca de la seguridad de la información en la Pymes, y que pese a esa advertencia para que puedan tener a buen resguardo la información, hicieron caso omiso, quizá por el simple hecho de no ser una grande empresa que les pueda ocurrir estas vulneraciones, hasta que se suscitó el fraude informático y entonces se observó que no se necesita ser un imperio de empresa, sino que las pequeñas empresas son las más delicadas y vulnerables y que si no cuentan con un sistema de protección de datos.

d.1 Que acciones correctivas se tomaron luego del hecho.

Luego del fraude sufrido, por la empresa se adoptaron medidas de seguridad para el apoyo y soporte de la información con la empresa ADS soluciones, ya que se venía laborando sin ninguna protección y respaldo de la información. En este caso la empresa ya mencionada se encarga de copias de seguridad de la información de manera diaria.

e.1 Tras el ataque ocurrido, las actividades de la empresa se realizaron de manera normal.

No, si tuvieron un paro de una semana en sus actividades

f.1 Se analizó de manera integral el incidente ocasionado.

Si se analizaron cuáles fueron las causas y los acontecimientos previos al hecho.

g.1 La información sustraída cuan relevante fue para la empresa

Fue muy relevante porque era de suma importancia para las actividades diarias de la empresa, donde constaban datos como proveedores y cuentas por cobrar a los clientes.

h.1 Posee un sistema de protección de datos.

El soporte de la empresa ADS.

i.1 Cuál fue el costo o el monto de perdida dentro del fraude informático.

6000 dólares

j.1 Existe evidencia física y disponible del ataque informativo que sufrió la empresa.

Los discos duros que fueron extraídos y reemplazados por nuevos para que se reinicien las actividades.

c) PRESERVACIÓN DE LA EVIDENCIA.

En la conservación de la evidencia y para el análisis de la información encriptada se encuentra los discos duros de las computadoras que fueron vulneradas, en la empresa ADS para la recuperación y obtención de la información que fue ocultada**.**

d) ANÁLISIS DE LA EVIDENCIA.

Debido a que esta investigación no es de manera técnica pura, sino de manera exploratoria, se procedió a recabar la información más relevante del hecho suscitado dentro de la empresa Calzacuba Cía. Ltda., con el apoyo incondicional de los socios mayoritarios y fundamentalmente de los empleados operativos dentro del área de TIC, se pudo evidenciar físicamente

los equipos de la empresa mismos que fueron manipulados para ver las inconsistencias y posibles vulnerabilidades que puedan tener, donde se encontró que no existe un tipo de firewall que permita la restricción de páginas indebidas y maliciosas que afecten a la información de la empresa y sus sistemas.

También como evidencia se pudo constatar la inexistencia de cámaras de video vigilancia tanto interna como externamente para una mayor seguridad no solo de la información de la empresa, sino de sus activos tangibles que son fundamentales para la operatividad de la misma. Dentro de la empresa no posee una guía de buenas prácticas para el uso adecuado de los equipos y de su información que puede ser vulnerada.

3.8. Elaboración de la hoja de hallazgos

HH - 1/3

CALZACUBA CIA. LTDA.

HOJA DE HALLAZGOS

ÁREA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN

AL 31 DE DICIEMBRE DEL 2016

Tabla 14
Hoja de Hallazgos

N°	Nombre del Hallazgo	Ref./PT	Condición	Criterio	Causa	Efecto	Recomendación
1	Inexistencia de cámaras de video vigilancia en la empresa.	CCI - 2/4	La empresa Calzacuba Cía. Ltda., presenta un perfil bajo de imagen empresarial por lo cual no posee cámaras de video vigilancia de manera interna y externa, debido a que realiza sus actividades en una vivienda familiar.	La empresa Calzacuba Cía. Ltda., no posee con un manual de políticas y una guía de buenas prácticas para el uso de los sistemas informáticos	El administrador de la empresa no considera necesario adaptar esta herramienta de seguridad para no exponer a posibles robos de infraestructura de la empresa.	La infraestructura de la empresa se encuentra vulnerable a posibles robos físicos y ataques a los sistemas informáticos por medio de intrusos y mafias internacionales.	Se recomienda al administrador de la empresa instalar cámaras de video vigilancia en la parte interna y externa, con el objetivo de precautelar y resguardar los bienes de la misma.

Continúa

HH - 2/3

N°	Nombre del Hallazgo	Ref./PT	Condición	Criterio	Causa	Efecto	Recomendación
2	No posee un firewall para restricción de páginas indebidas y el acceso a redes sociales.	CCI - 3/4	La empresa Calzacuba Cía. Ltda., debido a la actividad que desempeña, manifiesta que está autorizado a sus empleados al uso de redes sociales, siempre y cuando sean utilizados para su difusión y promoción de los productos que fabrica la empresa.	Debido al avance de la tecnología y a recomendaciones de grandes empresas como es el caso de Karpersky, a que las pymes deben contar con software de protección de datos.	La empresa Calzacuba Cía. con respecto a las páginas indebidas no posee un corta fuegos para de esa manera poder bloquear a enlaces maliciosas.	La información de la empresa por medio de enlaces maliciosos, puede ser vulnerada o sufrir ataques informáticos.	Se recomienda a la empresa implementar un firewall de seguridad de acuerdo a su condición económico, y a las necesidades de la empresa.
3	No cuenta con una aplicación de notificaciones en el caso de acceso indebido a la información.	CCI - 4/4	La empresa ADS quien es la encargada de brindar el servicio de protección de la información no proporciona una aplicación enmarcada a comunicar las vulnerabilidades que presentan los sistemas informáticos.	En el mundo del internet de las cosas se considera necesario activar mecanismos de defensa y protección que poseen las mismas herramientas de Office que se utiliza.	La empresa al no recibir notificaciones del acceso a su información, presenta puertos abiertos para ser atacados o vulnerados por hackers que puedan hacer uso indebido de los datos.	Al no contar con una aplicación que les permita verificar el buen resguardo de la información, la empresa está inmersa a diversos fraudes informáticos, los cuales obligan a tener un bloqueo de sus operaciones.	Se recomienda al personal encargado de los ordenadores, que activen diferentes comandos para la protección de la información, en las herramientas que ofrece Microsoft.

Continúa

HH - 2/3

N°	Nombre del Hallazgo	Ref./PT	Condición	Criterio	Causa	Efecto	Recomendación
4	El área de TIC no forma parte de la estructura organizacional de la empresa.	CCI - 1/4	Debido al tamaño y a la actividad de la empresa, no posee dentro de su estructura organizacional el área de TIC.	Dentro del Marco de Referencia de Cobit 4.0 indica que el área de TI forma una parte esencial dentro de las organizaciones y como estas influyen de manera positiva a su desempeño.	Por la falta de información y conocimiento por parte de la Gerencia y del área administrativa la empresa Calzacuba Cía. Ltda., no cuenta con el área de TIC de manera formalizada para para un mejor desempeño laboral y social.	Al no poseer en la misma empresa el área o departamento de TIC el personal operativo puede utilizar de manera negativa o impropia la información de la empresa.	Se recomienda al administrador de la empresa establecer dentro de la estructura a organizacional de la empresa una área de TIC, que será de gran ayuda para el desarrollo de la misma.
5	No existen informes periódicos del rendimiento de los sistemas informáticos.	CCI - 2/4	La empresa encargada del resguardo de la información no presenta ningún tipo de informe donde se pueda evidenciar las actividades diarias de respaldo de datos que se realiza dentro de la empresa.	Como respaldo de información y de las actividades de la empresa sería necesario que se cuente con respaldos de informes constantes del manejo de los sistemas de información.	La empresa que se encarga de la protección de datos no emite ningún reporte y que se estipulo dentro del contrato	No se tiene reportes físicos que evidencien el adecuado rendimiento de los sistemas, lo que conlleva un control débil de los mismos.	Se recomienda al administrador de la empresa que solicite a la empresa ADS un reporte de la evaluación de sus sistemas el rendimiento y su funcionamiento.

Elaborado por: K.G.Q.Z. – D.F.P.D	**Fecha: 14/08/2017**
Revisado por : L.A.L.C	**Fecha: 15/08/2017**

3.9. Informe de Auditoría Informática

Informe de Auditoría Informática

EMPRESA CALZACUBA CIA. LTDA

INFORME DE AUDITORÍA

1) Identificación del informe

Auditoría física y constatación y manipulación de los sistemas.

2) Identificación del departamento/área Auditada

Área de tecnología de información y comunicación.

3) Identificación de la entidad auditada

Empresa Calzacuba Cía. Ltda.

4) Antecedentes

La Empresa Calzacuba Cía. Ltda., conjuntamente con estudiantes de la Universidad de las Fuerzas Armadas, y con la autorización del Ingeniero José Bautista Gerente General de la organización antes mencionada, y en coordinación con los empleados, se solicitó la realización de la Auditoría Informática, misma que se realizó desde el 2 de Agosto al 9 de Agosto del 2017.

El equipo de Auditoría, fue conformado por los egresados de la Carrera de Ingeniería en Finanzas y Auditoría de la UFA-ESPE.

El marco de referencia base que se utilizo fue COBIT 4.0 de acuerdo a los lineamientos y a los dominios que nos proporciona, para tal efecto se realizaron el cumplimiento de visitas a la empresa y al área que se analizó, donde se aplicaron de manera previa encuestas a las diferentes empresas de manera global que forman parte del estudio de investigación Fraude Informático, Análisis de Vulnerabilidad de las empresas de la Provincia de Cotopaxi, de igual forma se ejecutó un examen especial al área critica, como son: sistemas de los ordenadores, conexiones de red, verificación de navegadores web, intervención y restricción de páginas maliciosas o indebidas.

Cabe indicar que durante la revisión y evaluación de los sistemas de información se detectaron las debilidades y se pusieron en conocimiento del administrador de la empresa y del Sr. Gerente para que de esa manera se tomen las medidas correctivas para una mejor operatividad de la organización.

5) Alcance de la auditoría

En la auditoría ejecutada se examinaron los aspectos de los sistemas de seguridades físicas y lógicas, procedimientos y documentación que forman parte de la actividad que realiza la empresa a diario.

De la misma manera la auditoría se realizará sobre los sistemas informáticos en computadoras personales que estén conectados a la red interna de la empresa.

6) Objetivos de la auditoría

- Determinar la vulnerabilidad, seguridad y confiabilidad de los sistemas informáticos de la empresa Calzacuba Cía. Ltda.
- Verificar la existencia de un panorama actualizado en cuanto a la seguridad física, las políticas de utilización, respaldo de datos y seguridad de los equipos.

7) Grupo de trabajo

- Ing. Luis Alfonzo Lema Cerda (Director del Proyecto de Investigación)
- Sr. Diego Fernando Pinsha Defaz (Investigador)
- Sr. Kleber Gonzalo Quevedo Zambonino (Investigador)

8) Periodo de ejecución

Nuestra auditoría comprende el período del 1 de enero del 2016 al 30 de junio del 2017, donde se realizó un examen especial al departamento/área de tecnología de información de la empresa Calzacuba Cía. Ltda.,

9) Marco de referencia

MARCO DE REFERENCIA UTILIZADO PARA LA AUDITORÍA INFORMÁTICA

COBIT es un Marco de referencia de procesos y objetivos de control de las tecnologías de información y comunicación que pueden ser implementados para controlar, auditar y administrar la organización. Este Marco de referencia está basado en las mejores prácticas y sistemas de información de auditoría y control de los sistemas informáticos.

Esto en particular aspira ayudar a los gerentes de las empresas a entender y administrar los riesgos relacionados con la tecnología de la Información y comunicación como también a conocer la relación entre los procesos de administración, las preguntas técnicas, la necesidad de controles y los riesgos que pueden sufrir las diversas organizaciones.

Por lo tanto es muy importante recordar que COBIT está estructurado por cuatro campos principales de administración, los cuales a su vez implican 34 procesos de administración asociados con la tecnología de la información y comunicación.

Los recursos de las TIC y los criterios de la información requeridos para asegurar el éxito son también identificados para cada proceso con los sistemas informativos de la empresa. Para soportar una auto-evaluación, COBIT incluye un modelo de madurez para cada proceso de las TIC. Por lo tanto se dice que COBIT cubre todos los aspectos de las tecnologías de información y comunicación, los modelos que pueden ser utilizados para soportar la evaluación de toda la organización, en lugar de especializarse en determinadas áreas. Como soporte a la medición del rendimiento operacional, factores críticos de éxito, indicadores clave de logro de objetivos, e indicadores clave de rendimiento son identificados en cada proceso.

COBIT ofrece un conjunto de herramientas para administrar los procesos de las tecnologías de información y comunicación, unificando los dos puntos

de vista, el de la administración y el del auditor. Las Guías de Administración TIC consideran los controles desde una perspectiva de la administración, mientras que las Guías de Auditoría proveen asistencia específica a los auditores en el diseño de programas adecuados de auditoría para cada dominio. COBIT también provee herramientas detalladas y personalizables de auto evaluación en forma de matrices y plantillas para asistir en la evaluación y medición de la organización comparada con los criterios de COBIT.

En resumen, COBIT, es una herramienta desarrollada para ayudar a los administradores de negocios a entender y administrar los riesgos asociados con la implementación de nuevas tecnologías de información y comunicación y demostrar a las entidades reguladoras e inversionistas, que tan efectiva es su tarea. Se ha definido a COBIT como: "Una estructura de relaciones y procesos para direccionar y controlar la compañía para lograr la consecución de los objetivos del negocio, entregando valor agregado mientras se administra el riesgo en función del ambiente de sistemas y sus procesos".

10) Hallazgos potenciales

- Inexistencia de cámaras de video vigilancia en la empresa.
- No posee un firewall para restricción de páginas indebidas y el acceso a redes sociales.
- No cuenta con una aplicación de notificaciones en el caso de acceso indebido a la información.
- El área de TIC no forma parte de la estructura organizacional de la empresa.
- No existen informes periódicos del rendimiento de los sistemas informáticos.

11) Conclusiones del Informe de Auditoría Informática

- La empresa Calzacuba Cía. Ltda., no cuenta con una guía de buenas prácticas para el uso de los equipos y sistemas que pose para la ejecución de sus actividades operativas.

- Como resultado de la investigación y con los datos recopilados y analizados, se proporcionan las respectivas directrices con la finalidad de aportar con información valiosa sobre las debilidades encontradas.
- Como equipo de auditores se considera que la empresa no realiza las tareas de actualización y mantenimiento necesarias de los equipos y sistemas informáticos, los cuales son esenciales para el normal funcionamiento de la misma y para el cumplimiento de los objetivos establecidos en las distintas áreas de la empresa.
- La empresa no cuente con firewall que impida el comportamiento errático y/o dañino para la operación de los sistemas computacionales en uso (Virus, sabotaje).

12) Recomendaciones al Informe de Auditoría Informática

- Como primera recomendación de este trabajo de investigación, se sugiere tomar en cuenta las recomendaciones planteadas en los diferentes controles auditados en el transcurso de la auditoría y que están debidamente documentados en este trabajo, recomendaciones que deben ser implementadas por el administrador de la empresa en conjunto con la alta gerencia.
- Se recomienda al administrador de la empresa instalar cámaras de video vigilancia en la parte interna y externa, con el objetivo de precautelar y resguardar los bienes de la misma.
- Se recomienda a la empresa implementar un firewall de seguridad de acuerdo a su condición económico, y a las necesidades de la empresa.
- Se recomienda al personal encargado de los ordenadores, que activen diferentes comandos para la protección de la información, en las herramientas que ofrece Microsoft.
- Se recomienda al administrador de la empresa establecer dentro de la estructura organizacional un área de TIC, que será de gran ayuda para el desarrollo de la misma y soporte a los diferentes departamentos.
- Se recomienda al administrador de la entidad que solicite a la empresa ADS (Administradora de la seguridad y soporte técnico de la

información), un reporte de la evaluación de sus sistemas el rendimiento y su funcionamiento.

- El administrador de la empresa, deberá mantener un servidor alterno con un sistema TCO (Costo Total de Propiedad o Costo Total de Operación), lo que permitirá en caso de fallo del servidor principal, la continuidad de las operaciones de la empresa y evaluar la inversión realizada.

CAPÍTULO IV

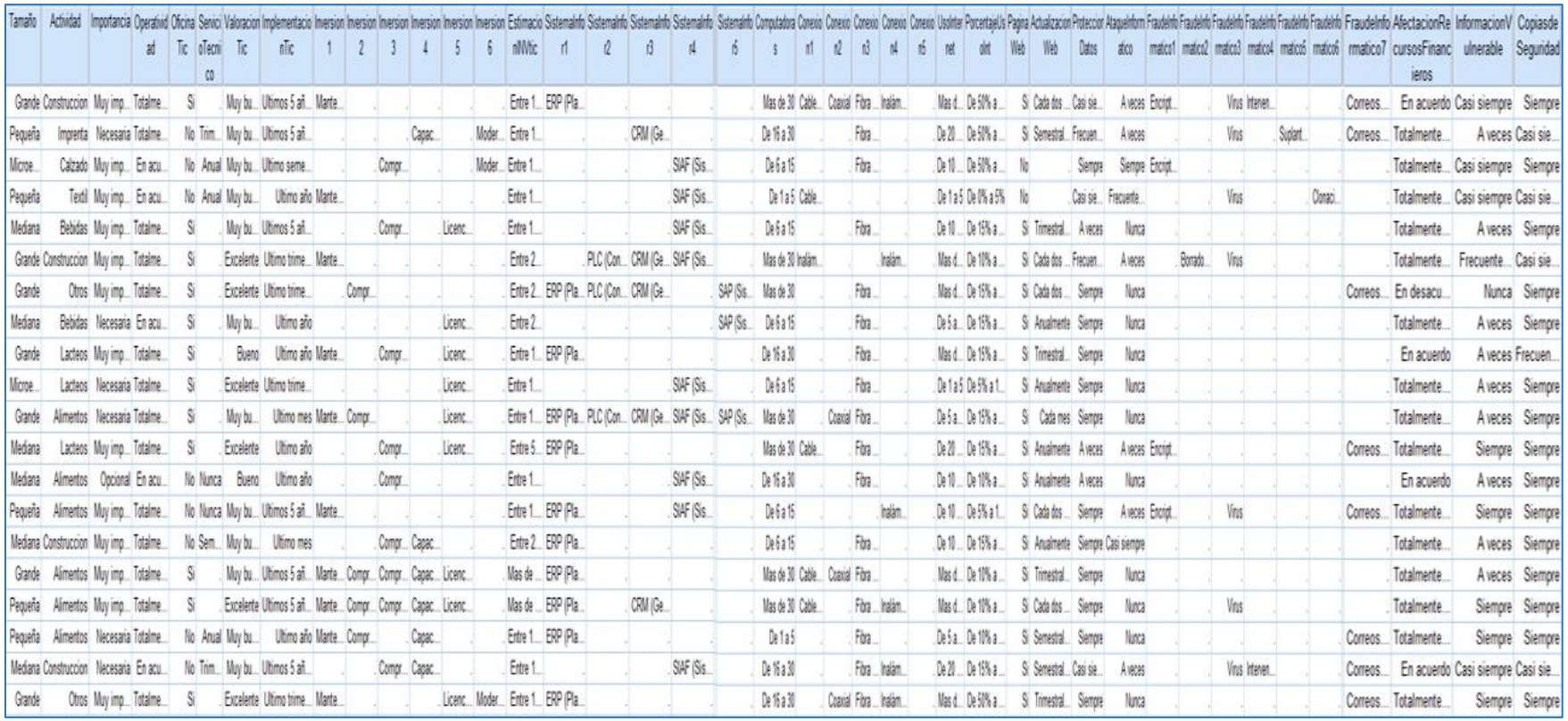
4. RESULTADOS DE LA INVESTIGACIÓN

4.1. Codificación de la Información

Nombre	Tipo	Anchura	Decimales	Etiqueta	Valores	Perdidos	Columnas	Alineación	Medida	Rol
Tamaño	Numérico	8	2	De que tamaño...	{1,00, Gran...	Ninguno	8	Derecha	Ordinal	Entrada
Actividad	Numérico	8	2	A que actividad...	{1,00, Const...	Ninguno	8	Derecha	Nominal	Entrada
Importancia	Numérico	8	2	Desde su persp...	{1,00, Muy i...	Ninguno	8	Derecha	Nominal	Entrada
Operatividad	Numérico	8	2	Considera uste...	{1,00, Total...	Ninguno	8	Derecha	Nominal	Entrada
OficinaTic	Numérico	8	2	La empresa cu...	{1,00, Si}...	Ninguno	8	Derecha	Nominal	Entrada
ServicioTec...	Numérico	8	2	Con que frecue...	{1,00, Mens...	Ninguno	10	Derecha	Escala	Entrada
ValoracionTic	Numérico	8	2	Cómo valora la ...	{1,00, Excel...	Ninguno	8	Derecha	Nominal	Entrada

Computador...	Numérico	8	2	Cuántas compu...	{1,00, Ningu...	Ninguno	8	Derecha	Escala	Entrada
Conexion1	Numérico	8	2	Qué tipo de co...	{1,00, Cable...	Ninguno	8	Derecha	Nominal	Entrada
Conexion2	Numérico	8	2	Qué tipo de co...	{1,00, Cable...	Ninguno	8	Derecha	Nominal	Entrada
Conexion3	Numérico	8	2	Qué tipo de co...	{1,00, Cable...	Ninguno	8	Derecha	Nominal	Entrada
Conexion4	Numérico	8	2	Qué tipo de co...	{1,00, Cable...	Ninguno	8	Derecha	Nominal	Entrada
Conexion5	Numérico	8	2	Qué tipo de co...	{1,00, Cable...	Ninguno	8	Derecha	Nominal	Entrada
UsoInternet	Numérico	8	2	Cuántas person...	{1,00, De 1 ...	Ninguno	8	Derecha	Escala	Entrada
PorcentajeU...	Numérico	8	2	Cuál es el porc...	{1,00, De 0...	Ninguno	8	Derecha	Escala	Entrada
PaginaWeb	Numérico	8	2	Dispone su em...	{1,00, Si}...	Ninguno	8	Derecha	Nominal	Entrada
Actualizacio...	Numérico	8	2	Con qué frecue...	{1,00, Cada ...	Ninguno	8	Derecha	Escala	Entrada
ProteccionD...	Numérico	8	2	Está su empre...	{1,00, Siem...	Ninguno	8	Derecha	Nominal	Entrada
AtaqueInfor...	Numérico	8	2	En los últimos ...	{1,00, Siem...	Ninguno	8	Derecha	Nominal	Entrada
FraudeInfor...	Numérico	8	2	Qué tipo de fra...	{1,00, Encri...	Ninguno	8	Derecha	Nominal	Entrada
FraudeInfor...	Numérico	8	2	Qué tipo de fra...	{1,00, Encri...	Ninguno	8	Derecha	Nominal	Entrada
FraudeInfor...	Numérico	8	2	Qué tipo de fra...	{1,00, Encri...	Ninguno	8	Derecha	Nominal	Entrada
FraudeInfor...	Numérico	8	2	Qué tipo de fra...	{1,00, Encri...	Ninguno	8	Derecha	Nominal	Entrada
FraudeInfor...	Numérico	8	2	Qué tipo de fra...	{1,00, Encri...	Ninguno	8	Derecha	Nominal	Entrada
FraudeInfor...	Numérico	8	2	Qué tipo de fra...	{1,00, Encri...	Ninguno	8	Derecha	Nominal	Entrada
FraudeInfor...	Numérico	8	2	Qué tipo de fra...	{1,00, Encri...	Ninguno	8	Derecha	Nominal	Entrada
AfectacionR...	Numérico	8	2	De acuerdo a la...	{1,00, Total...	Ninguno	8	Derecha	Nominal	Entrada
Informacion...	Numérico	8	2	Considera uste...	{1,00, Siem...	Ninguno	8	Derecha	Nominal	Entrada
CopiasdeSe...	Numérico	8	2	Realiza copias ...	{1,00, Siem...	Ninguno	8	Derecha	Nominal	Entrada

Figura 12 Ingreso de los datos de las variables



Tamaño	Actividad	Importancia	Operatividad	Oficina Tic	Servicio Tecnico	Valoracion Tic	Implementacion Tic	Inversion 1	Inversion 2	Inversion 3	Inversion 4	Inversion 5	Inversion 6	Estimacion Mantic	Sistemainfo r1	Sistemainfo r2	Sistemainfo r3	Sistemainfo r4	Sistemainfo r5	Computadora s	Conexion n1	Conexion n2	Conexion n3	Conexion n4	Conexion n5	Usointernet	PorcentajeUs ent	Pagina Web	Actualizacion Web	Proteccion Datos	Ataqueinformatico	Fraudeinformatico1	Fraudeinformatico2	Fraudeinformatico3	Fraudeinformatico4	Fraudeinformatico5	Fraudeinformatico6	Fraudeinformatico7	AfectacionRecursosFinancieros	InformacionVulnerable	Copiasde Seguridad
Grande	Construccion	Muy imp...	Totalme...	Si		Muy bu...	Ultimos 5 ait...	Mante...						Entre 1...	ERP (Pla...					Mas de 30	Cable...	Coaxial	Fibra ...	Inalám...		Mas d...	De 51% a ...	Si	Cada dos ...	Casi sie...	A veces	Encript...		Virus	Interven...			Correos...	En acuerdo	Casi siempre	Siempre
Pequeña	Imprenta	Necesaria	Totalme...	No	Trim...	Muy bu...	Ultimos 5 ait...				Capac...		Moder...	Entre 1...			CRM (Ge...			De 16 a 30			Fibra ...			De 20 ...	De 51% a ...	Si	Semestral...	Frecuen...	A veces			Virus		Suplant...		Correos...	Totalmente...	A veces	Casi sie...
Microe...	Calzado	Muy imp...	En acu...	No	Anual	Muy bu...	Ultimo seme...			Compr...			Moder...	Entre 1...				SIAF (Sis...		De 6 a 15			Fibra ...			De 10 ...	De 51% a ...	No		Siempre	Siempre	Encript...							Totalmente...	Casi siempre	Siempre
Pequeña	Textil	Muy imp...	En acu...	No	Anual	Muy bu...	Ultimo año	Mante...						Entre 1...				SIAF (Sis...		De 1 a 5	Cable...					De 1 a 5	De 0% a 5%	No		Casi sie...	Frecuente...			Virus			Conoci...		Totalmente...	Casi siempre	Casi sie...
Mediana	Bebidas	Muy imp...	Totalme...	Si		Muy bu...	Ultimos 5 ait...			Compr...		Licenc...		Entre 1...				SIAF (Sis...		De 6 a 15			Fibra ...			De 10 ...	De 15% a ...	Si	Trimestral...	A veces	Nunca								Totalmente...	A veces	Siempre
Grande	Construccion	Muy imp...	Totalme...	Si		Excelente	Ultimo trime...	Mante...						Entre 2...		PLC (Con...	CRM (Ge...	SIAF (Sis...		Mas de 30	Inalám...			Inalám...		Mas d...	De 10% a ...	Si	Cada dos ...	Frecuen...	A veces		Borrado...	Virus					Totalmente...	Frecuente...	Casi sie...
Grande	Otros	Muy imp...	Totalme...	Si		Excelente	Ultimo trime...		Compr...					Entre 2...	ERP (Pla...	PLC (Con...	CRM (Ge...		SAP (Sis...	Mas de 30			Fibra ...			Mas d...	De 15% a ...	Si	Cada dos ...	Siempre	Nunca						Correos...	En desacu...	Nunca	Siempre
Mediana	Bebidas	Necesaria	En acu...	Si		Muy bu...	Ultimo año					Licenc...		Entre 2...					SAP (Sis...	De 6 a 15			Fibra ...			De 5 a...	De 15% a ...	Si	Anualmente	Siempre	Nunca								Totalmente...	A veces	Siempre
Grande	Lacteos	Muy imp...	Totalme...	Si		Bueno	Ultimo año	Mante...		Compr...		Licenc...		Entre 1...	ERP (Pla...					De 16 a 30			Fibra ...			Mas d...	De 15% a ...	Si	Trimestral...	Siempre	Nunca							En acuerdo	A veces	Frecuen...
Microe...	Lacteos	Necesaria	Totalme...	Si		Excelente	Ultimo trime...					Licenc...		Entre 1...				SIAF (Sis...		De 6 a 15			Fibra ...			De 1 a 5	De 5% a 1...	Si	Anualmente	Siempre	Nunca								Totalmente...	A veces	Siempre
Grande	Alimentos	Necesaria	Totalme...	Si		Muy bu...	Ultimo mes	Mante...	Compr...			Licenc...		Entre 1...	ERP (Pla...	PLC (Con...	CRM (Ge...	SIAF (Sis...	SAP (Sis...	Mas de 30		Coaxial	Fibra ...			De 5 a...	De 15% a ...	Si	Cada mes	Siempre	Nunca								Totalmente...	A veces	Siempre
Mediana	Lacteos	Muy imp...	Totalme...	Si		Excelente	Ultimo año			Compr...		Licenc...		Entre 5...	ERP (Pla...					Mas de 30	Cable...		Fibra ...			De 20 ...	De 15% a ...	Si	Anualmente	A veces	A veces	Encript...					Correos...	Totalmente...	Siempre	Siempre
Mediana	Alimentos	Opcional	En acu...	No	Nunca	Bueno	Ultimo año			Compr...				Entre 1...				SIAF (Sis...		De 16 a 30			Fibra ...			De 10 ...	De 10% a ...	Si	Anualmente	A veces	Nunca							En acuerdo	A veces	Siempre
Pequeña	Alimentos	Muy imp...	Totalme...	No	Nunca	Muy bu...	Ultimos 5 ait...	Mante...						Entre 1...	ERP (Pla...			SIAF (Sis...		De 6 a 15				Inalám...		De 10 ...	De 5% a 1...	Si	Cada dos ...	Siempre	A veces	Encript...		Virus			Correos...	Totalmente...	Siempre	Siempre
Mediana	Construccion	Muy imp...	Totalme...	No	Sem...	Muy bu...	Ultimo mes			Compr...	Capac...			Entre 2...	ERP (Pla...					De 6 a 15			Fibra ...			De 10 ...	De 15% a ...	Si	Anualmente	Siempre	Casi siempre							Totalmente...	A veces	Siempre
Grande	Alimentos	Muy imp...	Totalme...	Si		Muy bu...	Ultimos 5 ait...	Mante...	Compr...	Compr...	Capac...	Licenc...		Mas de ...	ERP (Pla...					Mas de 30	Cable...	Coaxial	Fibra ...			Mas d...	De 10% a ...	Si	Trimestral...	Siempre	Nunca								Totalmente...	A veces	Siempre
Pequeña	Alimentos	Muy imp...	Totalme...	Si		Excelente	Ultimos 5 ait...	Mante...	Compr...	Compr...	Capac...	Licenc...		Mas de ...	ERP (Pla...		CRM (Ge...			Mas de 30	Cable...		Fibra ...	Inalám...		Mas d...	De 10% a ...	Si	Cada dos ...	Siempre	Nunca			Virus					Totalmente...	Siempre	Siempre
Pequeña	Alimentos	Necesaria	Totalme...	No	Anual	Muy bu...	Ultimo año	Mante...	Compr...		Capac...			Entre 1...	ERP (Pla...					De 1 a 5			Fibra ...			De 5 a...	De 10% a ...	Si	Semestral...	Siempre	Nunca						Correos...	Totalmente...	Siempre	Siempre
Mediana	Construccion	Necesaria	En acu...	No	Trim...	Muy bu...	Ultimos 5 ait...			Compr...	Capac...			Entre 1...				SIAF (Sis...		De 16 a 30			Fibra ...	Inalám...		De 20 ...	De 15% a ...	Si	Semestral...	Casi sie...	A veces			Virus	Interven...			Correos...	En acuerdo	Casi siempre	Casi sie...
Grande	Otros	Muy imp...	Totalme...	Si		Excelente	Ultimo trime...	Mante...				Licenc...	Moder...	Entre 1...	ERP (Pla...					De 16 a 30		Coaxial	Fibra ...	Inalám...		Mas d...	De 51% a ...	Si	Trimestral...	Siempre	Nunca							Correos...	Totalmente...	Siempre	Siempre

Figura 13 Ingreso de los resultados de la encuesta

La codificación y agrupamiento de los datos, variables y resultados obtenidos se lo ha realizado mediante el programa de estadística SPSS, de esa manera se optimizo tiempo y esfuerzo en la tabulación de las encuestas, cruce de variables y demás herramientas que nos proporciona el programa.

4.2. Análisis de los Resultados

TABULACIÓN DE ENCUESTAS

Pregunta Nº 1

1. ¿De qué tamaño es su empresa?

Tabla 15

Tamaño de las empresas

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Grande	7	35,0	35,0	35,0
Mediana	6	30,0	30,0	65,0
Pequeña	5	25,0	25,0	90,0
Microempresa	2	10,0	10,0	100,0
Total	20	100,0	100,0	

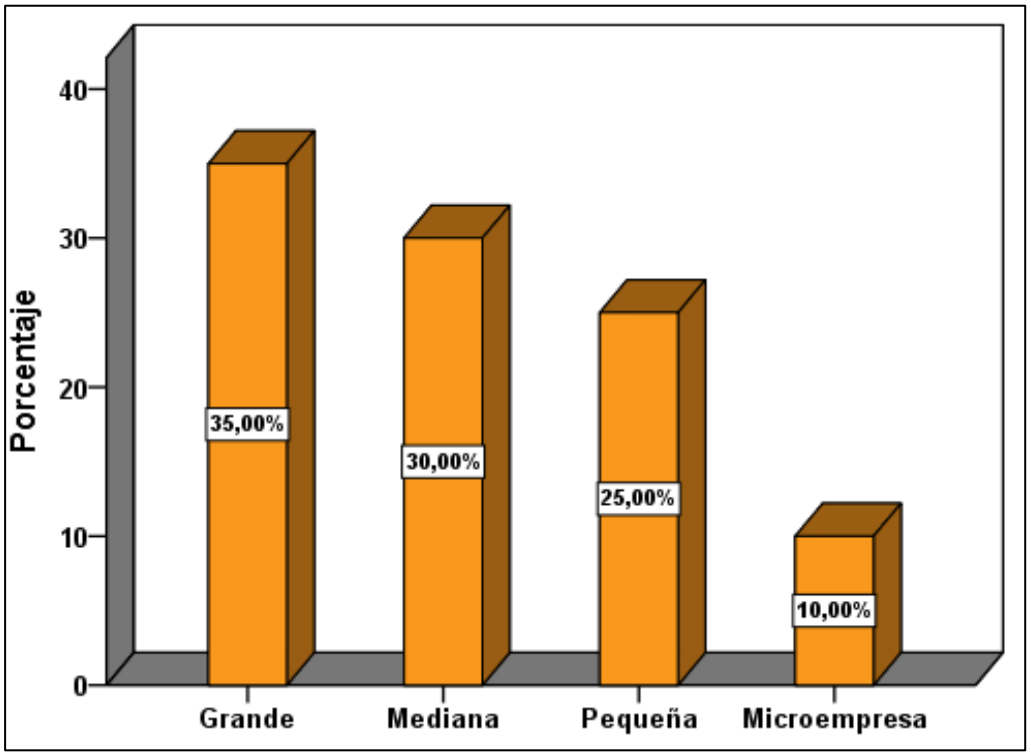


Figura 14 Tamaño de las empresas

Interpretación

De acuerdo a las encuestas realizadas a las empresas del sector industrial de la Provincia de Cotopaxi, se pudo evidenciar que del total de las empresas que se realizó el respectivo estudio el 35% corresponde a empresas grandes, el 30% a empresas medianas, el 25% a empresas pequeñas y el 10% a microempresas, teniendo en cuenta que dentro de las empresas grandes encontramos a: Familia Sancela del Ecuador, Parmalat, Novacero S.A., Cedal S.A., Molinos Poultier, entre otras. Por lo cual se dice que son las que más aportan al desarrollo económico-financiero y productivo de la Provincia y como referente a la investigación se deberían poner énfasis en las mismas por considerarse un nicho de exploración a fraudes informáticos debido al gran volumen de información que poseen, obviamente sin dejar de lado a las demás empresas que son también muy importantes en el crecimiento del país.

Pregunta Nº 2

2. ¿A qué actividad manufacturera se dedica su empresa?

Tabla 16

Actividad Manufacturera de las empresas

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Construcción	4	20,0	20,0	20,0
Calzado	1	5,0	5,0	25,0
Imprenta	1	5,0	5,0	30,0
Lácteos	3	15,0	15,0	45,0
Textil	1	5,0	5,0	50,0
Bebidas	2	10,0	10,0	60,0
Alimentos	6	30,0	30,0	90,0
Otros	2	10,0	10,0	100,0
Total	20	100,0	100,0	

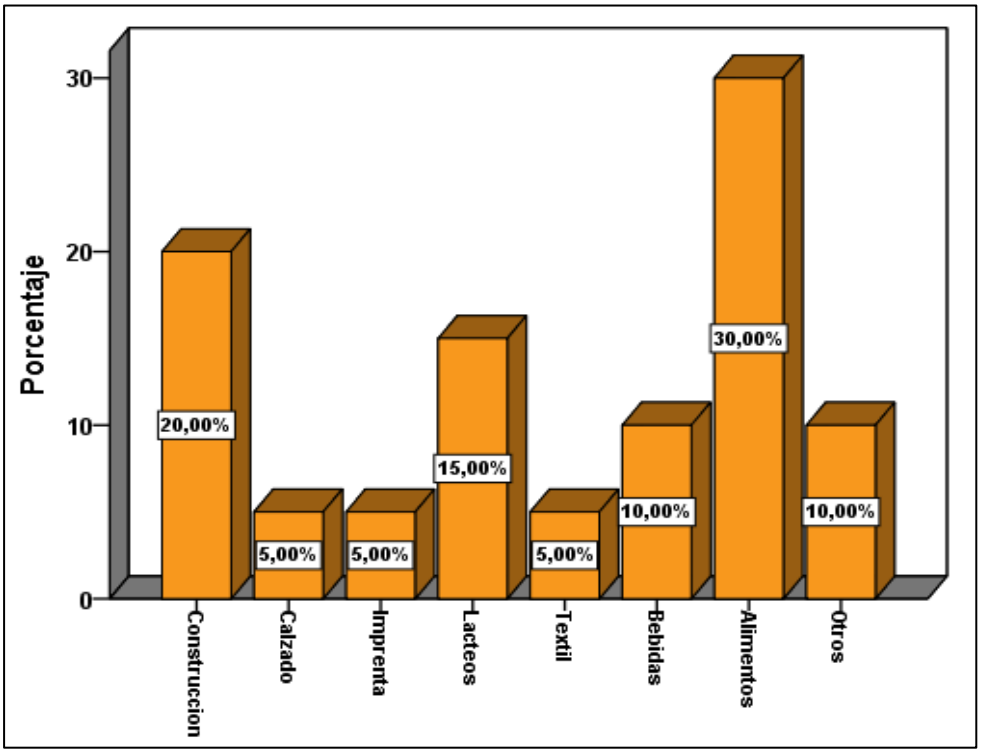


Figura 15 Actividad Manufacturera de las empresas

Interpretación

Dentro de las empresas industriales de la provincia de Cotopaxi, la actividad primordial a la que se dedican son a la línea de los alimentos con un porcentaje del 30%,y por esta razón se puede señalar que las empresas de esta provincia se dedican al sector agrícola y la producción de alimentos que se distribuyen dentro del mismo y para otras regiones, seguido de la actividad de la construcción con un valor significativo del 20%,acotanto que tenemos empresas que ayudan y aportan de manera significativa a este sector como

es el caso de Novacero, Cedal, con un 15% dedicándose a la elaboración de lácteos, atribuyendo a la existencia de actividad ganadera dentro de la localidad y sabiendo aprovechar la producción de leche para la elaboración de lácteos y demás productos derivados para ser comercializados, continuando con las bebidas, con un 10% tenemos como referente a Fuentes San Felipe una empresa posicionada en el mercado, este dato lo comparten con actividades de madera caso específico de Aglomerados Cotopaxi de y elaboración de papel y sus derivados mencionando a Familia Sancela y finalmente las actividades de calzado, imprenta y textil con un 5%, sectores muy importantes dentro de la economía de la provincia.

Pregunta Nº 3

3. **¿Desde su perspectiva, que importancia merece la utilización de recursos tecnológicos como apoyo operativo en los procesos de industrialización dentro de su empresa?**

Tabla 17

Recursos tecnológicos de las empresas

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Muy importante	13	65,0	65,0	65,0
Necesaria	6	30,0	30,0	95,0
Opcional	1	5,0	5,0	100,0
Total	20	100,0	100,0	

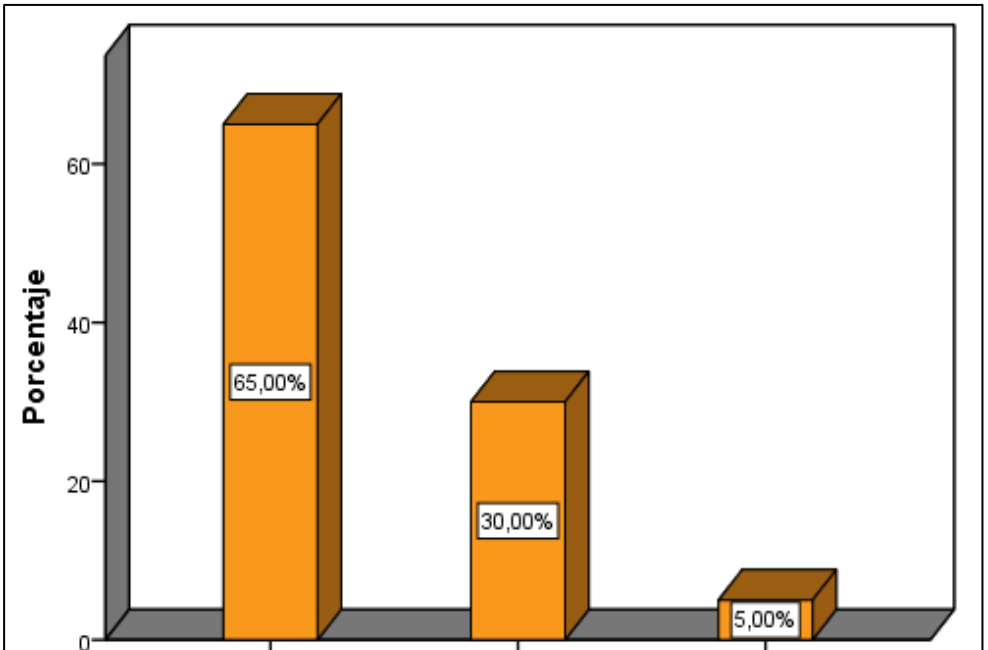


Figura 16 Recursos tecnológicos de las empresas

Interpretación:

Un 65% de las empresas del sector productivo industrial consideran que es muy importante la utilización de los recursos tecnológicos, ya que con el avance de la tecnología de información y comunicación constantemente surgen nuevos avances en máquinas, equipos, software y herramientas tecnológicas que ayudan a tener un mejor desempeño de las organizaciones y más aún si son del sector industrial porque tienen que basarse en procesos estandarizados y con un mejor control de calidad, donde se podría suponer que posean una oficina de TIC que sirvan de soporte a las empresas como una unidad fundamental de las entidades, seguido de un 30% considera que es necesario conjeturando que se puede mencionar a las pequeñas empresas y con un porcentaje muy bajo pero menos importante tiene la opinión de que es opcional con un 5%, refiriéndonos a las microempresas que por la infraestructura limitada o la actividad a la que se dedica no es tan importante a diferencia de las grandes industrias.

Pregunta Nº 4

4. **¿Considera usted que los recursos tecnológicos favorecen la operatividad de la empresa, como un medio para optimizar recursos?**

Tabla 18

Recursos Tecnológicos en la operatividad de las empresas

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en acuerdo	15	75,0	75,0	75,0
En acuerdo	5	25,0	25,0	100,0
Total	20	100,0	100,0	

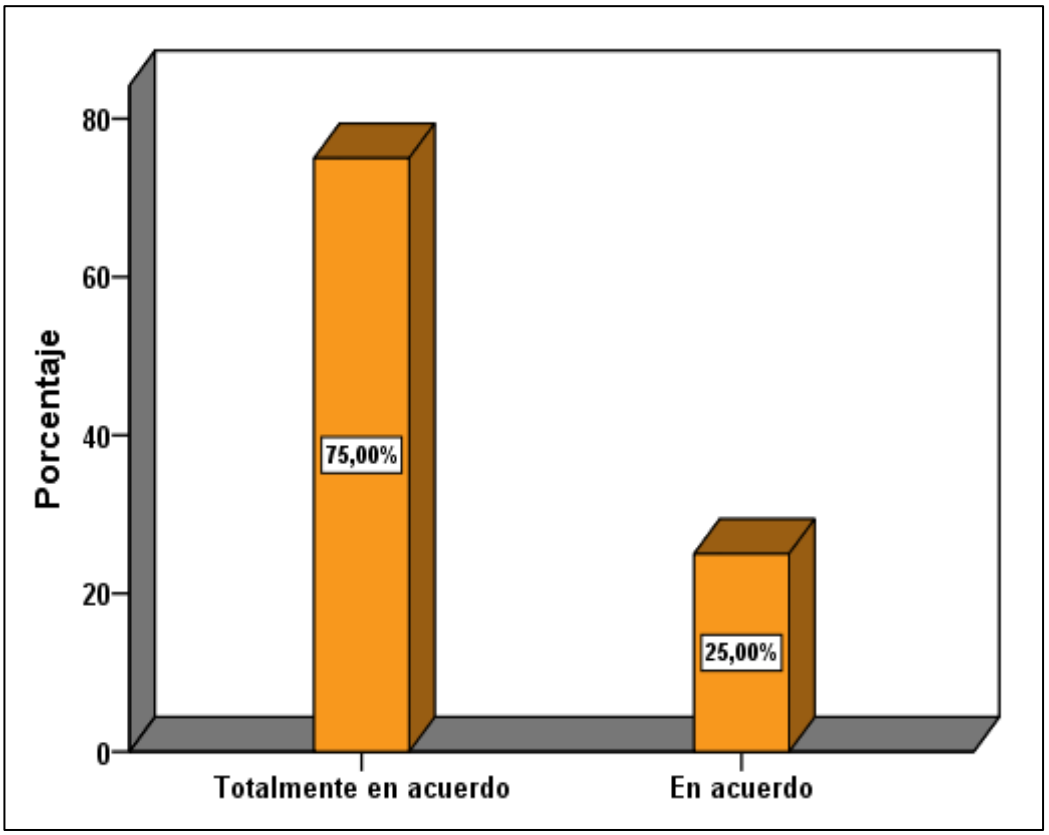


Figura 17 Recursos Tecnológicos en la operatividad de las empresas

Interpretación:

El 75% las empresas del sector industrial de la Provincia de Cotopaxi, están totalmente en acuerdo que los recursos tecnológicos ayudan a la optimización y minimización de recursos, como ya se mencionó anteriormente cada industria requiere de equipos automatizados, maquinarias de última

tecnología que les ayuden a hacer más eficaces y eficientes dentro de la operatividad de la empresa siendo generadores de riqueza para la empresa, pero siempre y cuando se tenga aún protección y seguridad de la información de las actividades de la empresas que en la actualidad se vuelven vulnerables a ataques informáticos, mientras que en acuerdo nos arroja un 25%, que es muy importante dentro de la opinión que tienen cada gerente de las medianas, pequeña y microempresas.

Pregunta Nº 5

5. **¿La empresa cuenta con una oficina administrativa de TIC (Tecnologías de Información y Comunicación)?**

Tabla 19

Poseen unidad de TIC

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	12	60,0	60,0	60,0
No	8	40,0	40,0	100,0
Total	20	100,0	100,0	

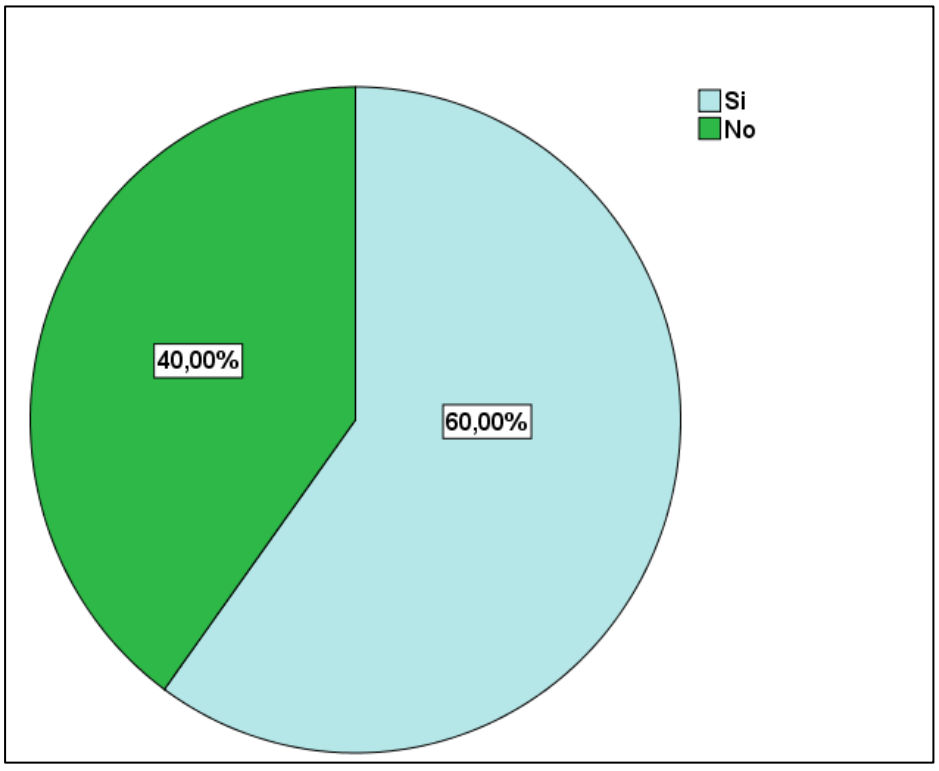


Figura 18 Poseen unidad de TIC

Interpretación

Un 60% de las empresas encuestadas si poseen unidad de TIC (Tecnologías de Información y Comunicación),dentro de este porcentaje están incluidas la empresas que utilizan mayores recursos tecnológicos para la operatividad de las empresas caso principal de la grandes empresas que poseen un gran volumen de información importante o Big Data dentro de las grandes organizaciones, y como apoyo fundamental para el desarrollo organizacional y económico deben poseer la oficina de Tecnologías de información y comunicación que en gran medida ayudan a la dinamización de los datos y la información, desde luego con una gran inversión a este medio operativo , a diferencia que, el 40% no posee departamento de TIC, ya que todos estos datos dependen y varía de acuerdo a la actividad de la empresa y su tamaño para que se pueda configurar en cada organización, donde quizá no poseen información no tan relevante y que los mismos gerentes no ven necesario tener una unidad de Tic, que quizá ellos lo pueden manejar de otra manera adecuándose a sus necesidades y costos.

Pregunta Nº 5.1

5.1. ¿Con que frecuencia la empresa contrata de un servicio técnico especializado en TIC?

Tabla 20

Contrata servicio técnico especializado en TIC

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Trimestral	2	10,0	25,0	25,0
Semestral	1	5,0	12,5	37,5
Anual	3	15,0	37,5	75,0

Nunca	2	10,0	25,0	100,0
Total	8	40,0	100,0	
Sistema	12	60,0		
	20	100,0		

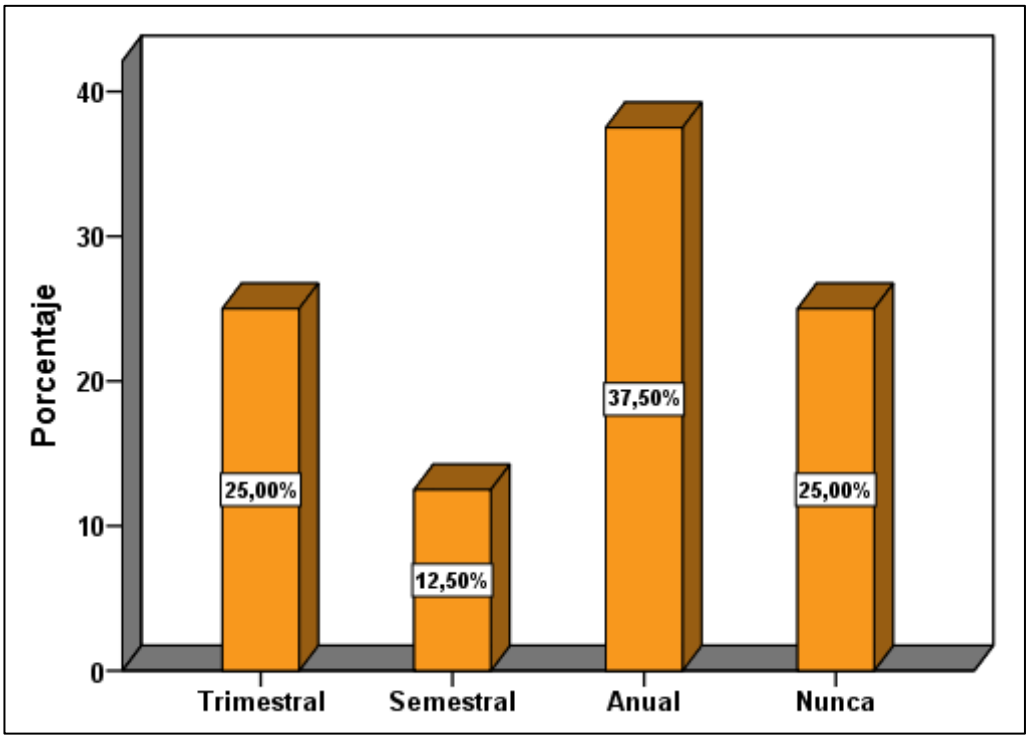


Figura 19 Contrata servicio técnico especializado en TIC

Interpretación

Con relación a la pregunta anterior de las empresas que no tienen un departamento de TIC, en esta pregunta se puede ver que el 25% nunca contrata un servicio técnico especializado, algo que es significativo y que se debería poner énfasis dentro de las organizaciones que no hacen mención a una oficina de Tic o un servicio especializado o que quizá no lo necesitan en el caso de un microempresa que está abriendo al mercado a diferencia que un 37,5% lo hace de forma anual, que como ya se dijo que depende de la

actividad que se dedique la empresa, o del volumen de información que posean y no menos importante del costo de inversión que se requiera, por lo cual sería importante evaluar en qué condiciones se encuentran sus datos, ya que si se lo mantiene de esta manera puede ser vulnerable a cualquier fuga de información debido a que no existe un monitoreo constante que permita evidenciar el buen manejo de las operaciones en materia de seguridad informática, seguido por un 25% que contratan de forma trimestralmente algo adecuado para algunas empresas, y finalmente un 12,5% que lo realiza de manera semestral, algo que se debería evaluar y por lo menos sugerir que se lo haga de manera trimestral.

Pregunta Nº 6

6. ¿Cómo valora la importancia que tienen las TIC en su Empresa?

Tabla 21

Importancia de TIC dentro de las empresas

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Excelente	6	30,0	30,0	30,0
Muy bueno	12	60,0	60,0	90,0
Bueno	2	10,0	10,0	100,0
Total	20	100,0	100,0	

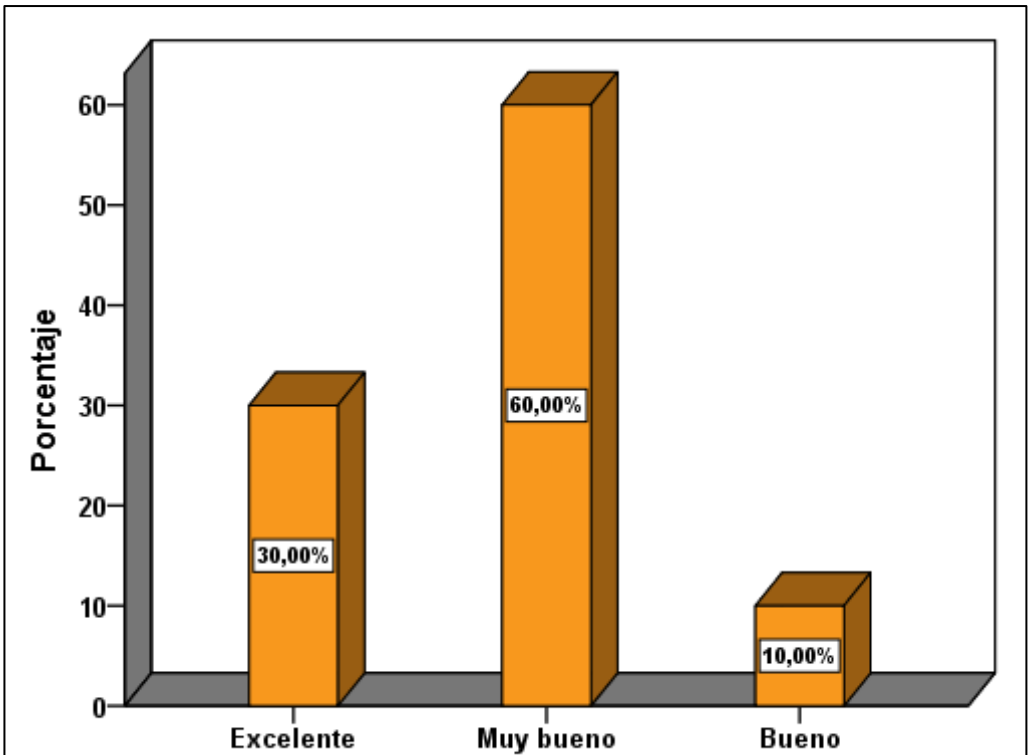


Figura 20 Importancia de TIC dentro de las empresas

Interpretación:

Un 60% de las empresas estudiadas consideran que un departamento de Tic es muy bueno, seguido de un 30% que consideran que es excelente que una organización posea un departamento de TIC, por lo que se puede mencionar que las grandes empresas utilizan de mejor manera sus herramientas dentro de los procesos de industrialización y un 10% considera que sería bueno, todo eso ajustado a la realidad y las condiciones de las entidades ya que cada una tiene diferente actividad. También podemos expresar que no existe una adecuada utilización de los recursos tecnológicos por parte de las empresas, ya que sería muy importante que el 100% de las empresas valoren al departamento de TIC de forma excelente, lo cual ayudaría en el control de sus actividades cotidianas y en el desarrollo de las mismas.

Pregunta Nº 7

7. **¿Ha implementado tecnología o sistemas de información y comunicación dentro de la empresa en?**

Tabla 22

Implementación de Tic o sistemas información

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Último mes	2	10,0	10,0	10,0

Último trimestre	4	20,0	20,0	30,0
Último semestre	1	5,0	5,0	35,0
Último año	6	30,0	30,0	65,0
Últimos 5 años	7	35,0	35,0	100,0
Total	20	100,0	100,0	

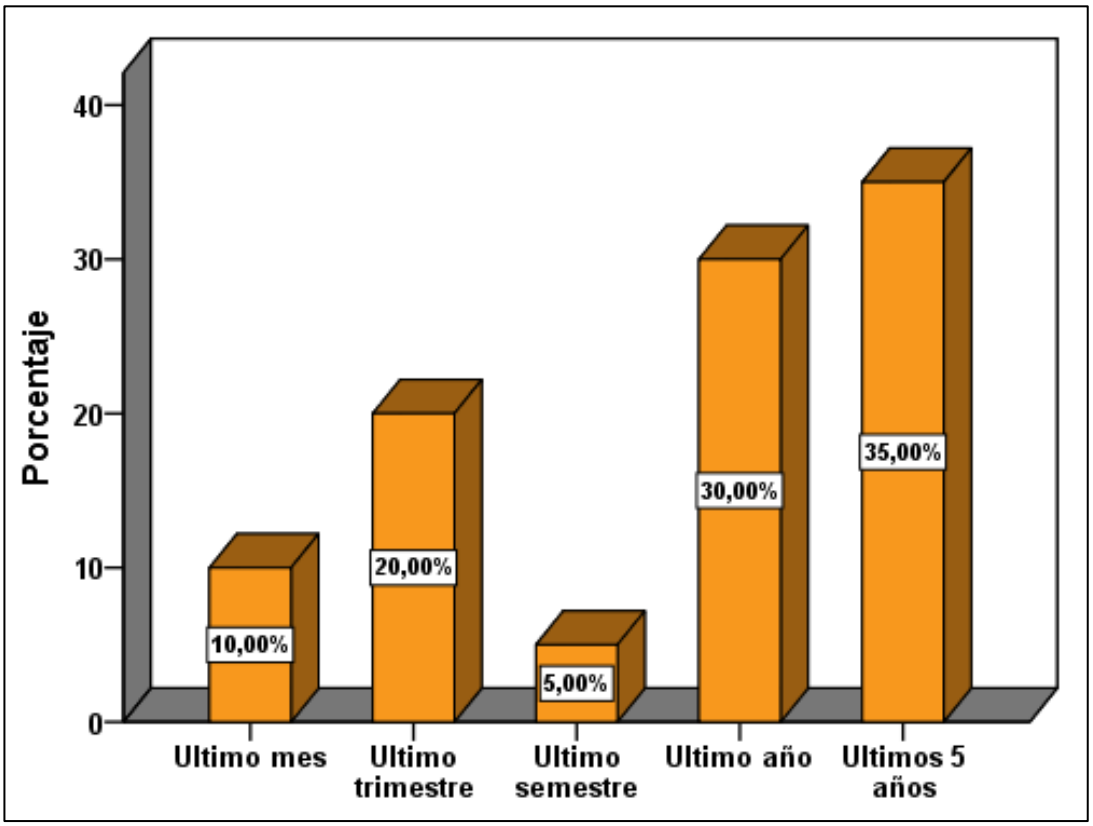


Figura 21 Implementación de Tic o sistemas información

Interpretación:

El 35% de las empresas dedicadas a la manufactura aluden que durante los últimos 5 años han implementación de tecnología o sistemas de información, todo esto acumulándose a las inversiones como pueden ser compra de equipos de alta tecnología, compra de software, licencias que lo deben adquirir de manera anual o semestral dependiendo del tipo de licencia,

mantenimiento y capacitación en el manejo de TIC, que son muy importantes para un adecuado manejo de recursos de TI, seguido de un 30% que ha implementado en el último año y tan solo un 20% que ha implementado el último trimestre, un 10 % en el último mes y con un 5% de manera semestral, como ya se dijo de acuerdo a la necesidad de la empresa y su presupuesto se realiza la implementación de sistemas tecnológicos.

Pregunta Nº 8

8. **¿De acuerdo a la respuesta de la pregunta anterior qué tipo de inversión es más representativa para la empresa en tecnología de información y comunicación seleccione una de ellas?**

Tabla 23

Inversión más representativa

	Respuestas		Porcentaje de casos
	N	Porcentaje	
Mantenimiento de equipo	10	23,8%	50,0%
Compra de equipo	5	11,9%	25,0%
Compra de software	9	21,4%	45,0%
Capacitación de personal	6	14,3%	30,0%
Licencias y patentes informáticas	9	21,4%	45,0%
Modernización de equipos	3	7,1%	15,0%
Total	42	100,0%	210,0%

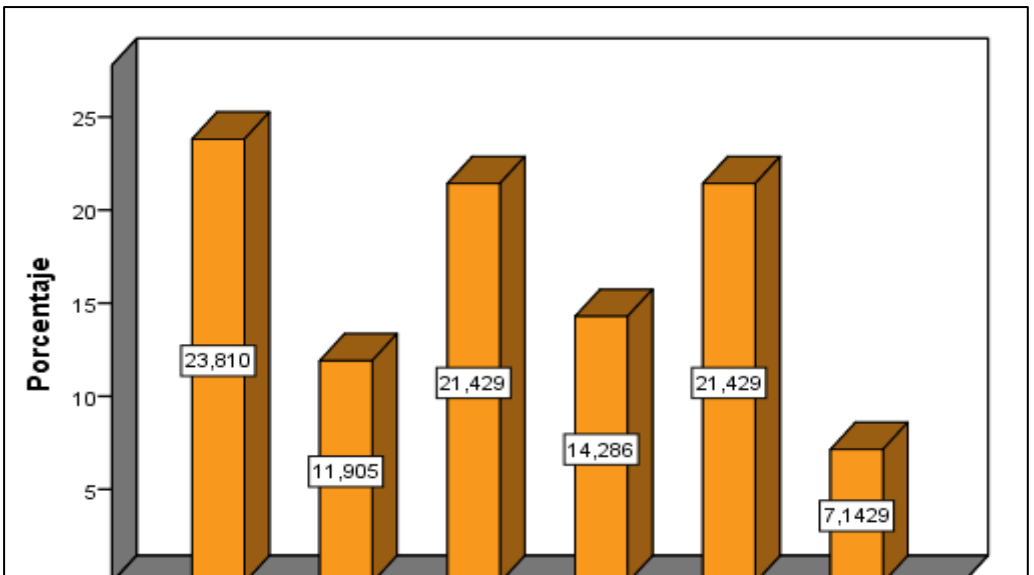


Figura 22 Inversión más representativa

Interpretación:

Dentro de la inversiones más representativas y de acuerdo al estudio realizado tenemos que el 23,80% de las empresas industriales invierten en mantenimiento de equipos, ya que dentro de la actividad manufacturera se requiere equipos que tengan un adecuado funcionamiento para de esa manera alcanzar una operatividad máxima de producción y cumplir las metas y objetivos planteados a corto y largo plazo y en caso de presentar alguna anomalía en los equipos o maquinaria se requiera prestar énfasis, o quizá la renovación de equipos nuevos, seguido de igual forma con un porcentaje alto del 21,40% son aquellas que han contratado licencias y patentes informáticas que lo comparten con la inversión de compra de software, continuando con un 14,30% que han invertido en capacitación de personal, la compra de equipo alcanza un 11,90% y finalmente la modernización de equipos en un 7,10%, ya que eso incurre un costo de inversión y quizá no todas la empresas puedan realizarlo o adquirir equipos modernos o de última tecnología.

Pregunta Nº 9

9. ¿Cuánto estima usted que ha invertido en TIC durante el periodo 2012 - 2016?

Tabla 24

Estimación de inversión en TIC

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado

Entre 1.000 a 10.000 dólares	8	40,0	40,0	40,0
Entre 10.000 a 25.000 dólares	5	25,0	25,0	65,0
Entre 25.000 a 50.000 dólares	4	20,0	20,0	85,0
Entre 50.000 a 100.000 dólares	1	5,0	5,0	90,0
Más de 100.000 dólares	2	10,0	10,0	100,0
Total	20	100,0	100,0	

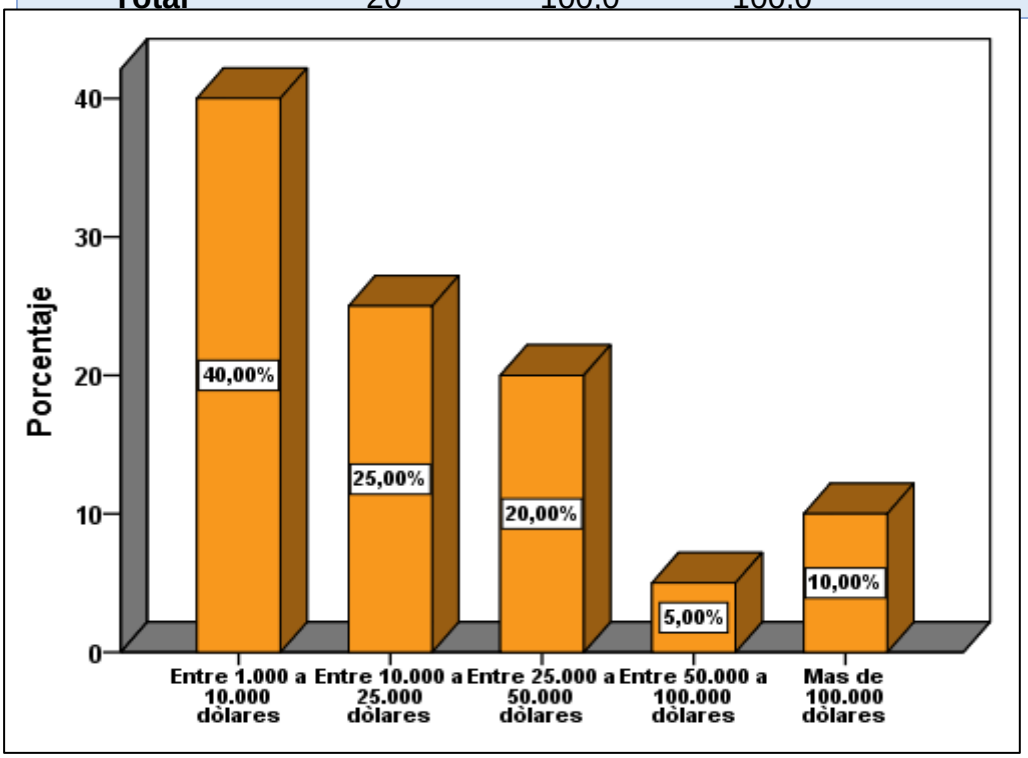


Figura 23 Estimación de inversión en TIC

Interpretación:

De acuerdo al estudio realizado y a las encuestas realizadas a las empresas industriales se pudo evidenciar que existe un porcentaje del 40% de las empresas que invierte entre 1000 a 10.000 dólares en tecnologías de información y comunicación dentro de esta se encuentran las pequeñas y las microempresas debido al volumen de operación de las mismas, para lo cual se evalúa y se recomienda realizar un incremento en inversión en tecnologías de información y comunicación, seguido de un 25% que invierten entre 10.000 a 25.000 dólares, sin mucha diferencia del 20% que invierten entre 25.000 a

50.000 dólares, en lo cual se concentran empresas medianas y pequeñas tales como El Ranchito, Prodicereal, CorpIce-Cream, lo que demuestra que si habido una inversión significativa, de igual manera hay una dato significativo que un 10% ha invertido más de 100.000 dólares dentro de estas se encuentran un empresa grande como lo es Provefrut S.A. en la renovación e implementación de sus sistemas de información y la Dlip-Industrial una empresa pequeña dedicada a la fabricación de suplementos alimenticios que de igual manera su inversión era para la implementación de equipos de procesamiento modernos, finalmente un 5% entre los valores de inversión de 50.000 a 100.000 dólares, que lo conforman Novacero, Familia Sancela, Parmalat, etc.

Pregunta Nº 10

10. ¿Qué sistema informático dispone la empresa?

Tabla 25

Sistemas Informáticos de las empresas

	Respuestas		Porcentaje de casos
	N	Porcentaje	
ERP (Planificación de Recursos Empresariales)	11	35,5%	55,0%
PLC (Controlador Lógico Programado)	3	9,7%	15,0%
CRM (Gestión de Servicio al Cliente)	5	16,1%	25,0%
SIAF (Sistema de Información y Administración Financiera)	9	29,0%	45,0%
SAP (Sistemas, Aplicaciones y Productos)	3	9,7%	15,0%
Total	31	100,0%	155,0%

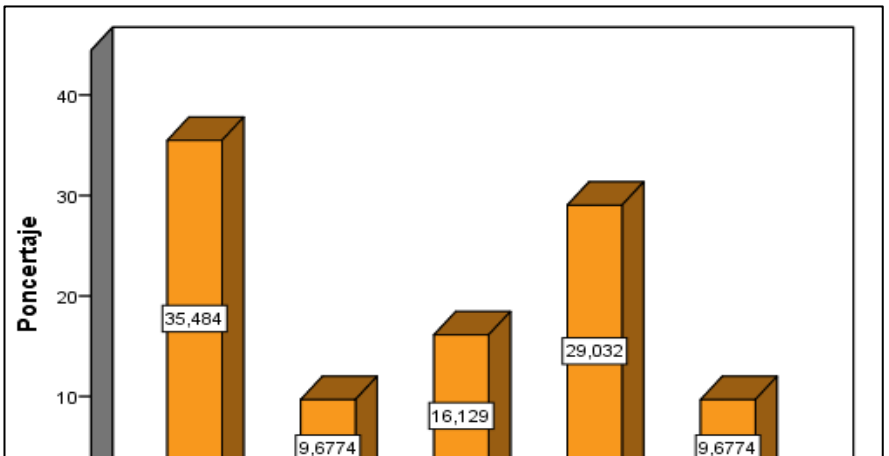


Figura 24 Sistemas Informáticos de las empresas

Interpretación:

De acuerdo a las encuestas realizadas a las empresas del sector industrial sobre los sistemas informáticos que disponen para la ejecución de sus actividades manufactureras y poniendo a su disposición una lista de los principales sistemas tenemos que con un 35% utilizan el ERP (Planificación de Recursos Empresariales), ya que muchas de la investigación tienes este sistemas que ayuda a optimizar tiempo y dinero, seguido con un 29,00% del SIAF, este sistema es muy necesario dentro de cada organización ya que ayuda a manejar y a controlar los recursos financieros y económicos a continuación de con un16,10% utilizan el CRM , casi la mitad de las empresas utilizan como un apoyo para una mejor atención al cliente y compartiendo un 9,70% utilizan los sistemas de PLC Y SAP, quizá muy pocos conocidos por las organizaciones pero no menos importantes, para las grandes que son muy necesarios, cabe mencionar que la empresa que utiliza todo los sistemas de una manera integral es Molinos Poultier que de manera integral posee todos los sistemas en un solo sistema especializado, cabe destacar que es una buena inversión para el desarrollo de su operaciones y protección de datos.

Pregunta Nº 11

11. ¿Cuántas computadoras posee su empresa?

Tabla 26

Computadoras en las empresas

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
De 1 a 5	2	10,0	10,0	10,0
De 6 a 15	6	30,0	30,0	40,0
De 16 a 30	5	25,0	25,0	65,0
Más de 30	7	35,0	35,0	100,0
Total	20	100,0	100,0	

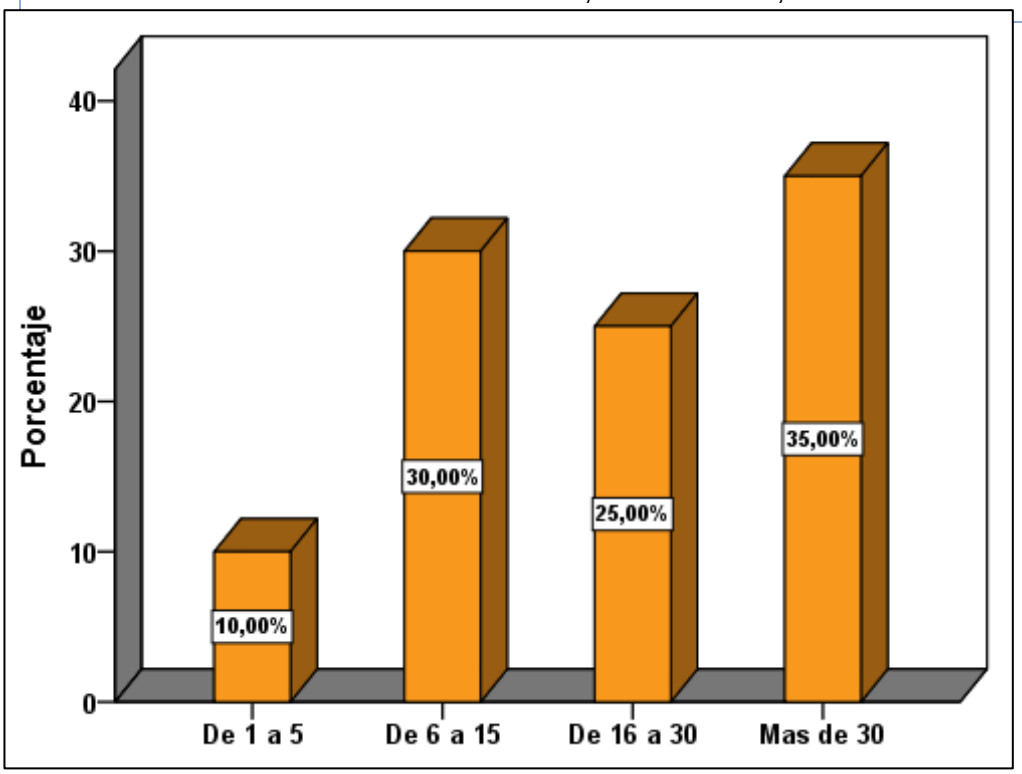


Figura 25 Computadoras en las empresas

Interpretación:

El 35% de las empresas industriales poseen más de 30 computadoras debido a las actividades que lo realizan como es el caso de las empresas Cedal, Dlip-Industrial, Novacero entre otras, aunque esto también incurre un gran riesgo de fuga de información, y vulneración de sus datos al no contar con un buen sistema de seguridad y protección de datos, seguido de un 30% que poseen entre 6 a 15 computadoras esto es el caso de las empresas medianas que tienen un riesgo de fuga de información bajo, continuando con un 25% que poseen entre 16 a 30 computadoras con un riesgo de fuga de

información medio, finalmente con un 10% que poseen de 1 a 5 computadoras con un riesgo de fuga de información nulo, se podría decir que en realidad sucede lo contrario ya que empresas pequeñas quizá porque no cuentan con seguridad en datos en su información y se han visto vulneradas, todo esto de acuerdo a la necesidad de las empresas y su actividad relacionada, para la adecuación de una seguridad adecuada.

Pregunta Nº 12

12. ¿Qué tipo de conexión utiliza la empresa para acceder a su red local?

Tabla 27

Tipo de conexión a la Red

	Respuestas		Porcentaje de casos
	N	Porcentaje	
Cableado	5	15,2%	25,0%
Coaxial	4	12, 12%	20,0%
Fibra Óptica	17	51,5%	85,0%
Inalámbrica	7	21,2%	35,0%
Total	33	100,0%	165,0%

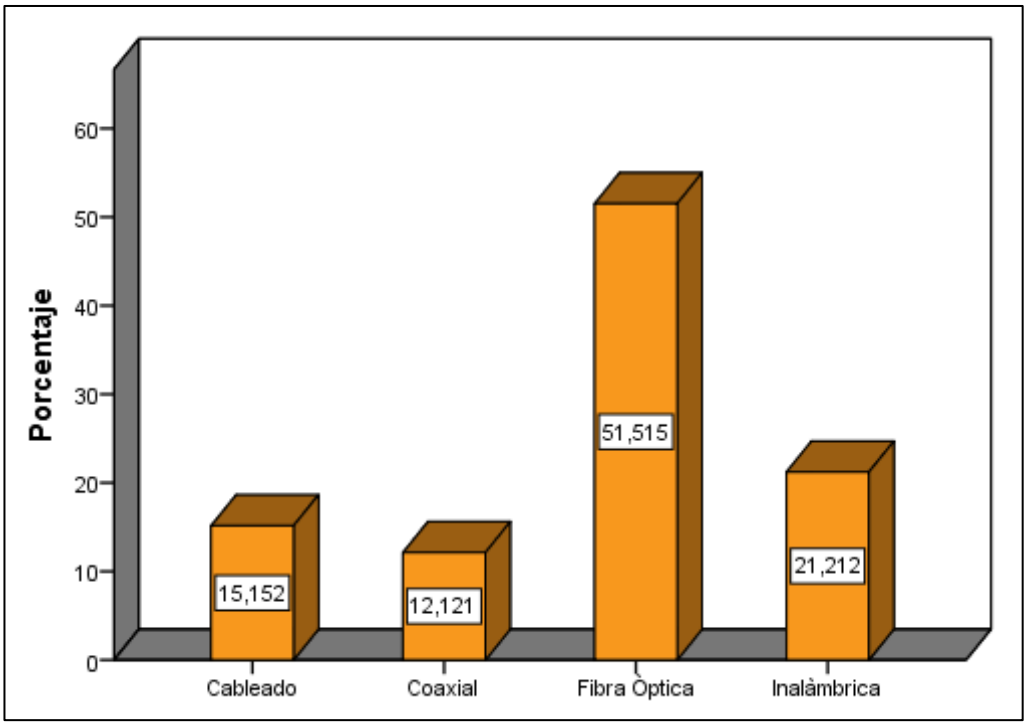


Figura 26 Tipo de conexión a la Red

Interpretación:

En lo que se refiere a la conexión a la red o internet dentro de las empresas tenemos un porcentaje representativo de 51,50% que utiliza conexión por fibra óptica, por cada tipo de empresas sea desde la grande hasta la microempresa, seguido de un 21,20% con una conexión de tipo inalámbrica o wifi como comúnmente se le conoce, continuando con un 15,20% de cableado o trenzado y finalmente con un 12,10% con una conexión de tipo coaxial, cabe mencionar que dentro de la información recopilada muchas de las empresas poseen dos o tres tipos de conexiones, eso podría representar un medio de fuga de información o vulneración de datos masivo, aunque en la actualidad los dispositivos móviles son la vía principal para el robo de información por la conexión a internet o a una red wifi pública, las mismas cámaras de seguridad de las empresas sirven como medio de fuga o espionaje a través de aplicaciones web como Shodan.

Pregunta Nº 13

13. ¿Cuántas personas empleadas en su empresa utilizan habitualmente Internet durante su trabajo?

Tabla 28

Uso de Internet

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
De 1 a 5	2	10,0	10,0	10,0

De 5 a 10	3	15,0	15,0	25,0
De 10 a 20	5	25,0	25,0	50,0
De 20 a 30	3	15,0	15,0	65,0
Más de 30	7	35,0	35,0	100,0
Total	20	100,0	100,0	

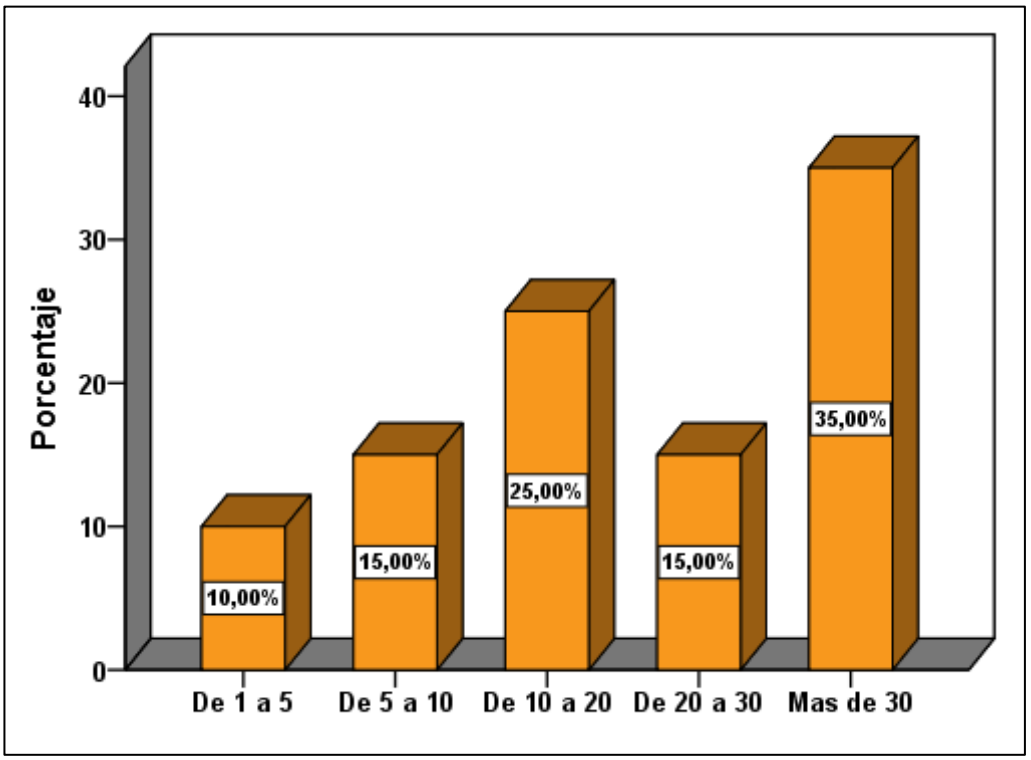


Figura 27 Uso de Internet

Interpretación

Mediante las encuestas realizadas a las empresas del sector industrial sobre el número de empleados que utilizan habitualmente internet durante su trabajo, se puedo constatar que en el rango de 1 a 5 personas, el 10% de las empresas utilizan habitualmente Internet durante el trabajo de sus empleados, en el rango de 5 a 10 personas, utilizan el 15%, en el rango de 10 a 20, utilizan el 25%, en el rango de 20 a 30 utilizan el 15% y en el rango de más de 30 personas utilizan el 35%, por lo que se evidencia que la mayoría de empresas

trabajan a diario mediante el internet, por lo cual están expuestas a diversos ataques informáticos por parte de ciberdelincuente quienes realizan este tipo de actividad que es el robo de información o clonación de datos de las empresas más vulnerables con la finalidad de tener un beneficio mutuo y personal.

Pregunta N° 14

14. ¿Cuál es el porcentaje del total de empleados que utiliza computador en su rutina normal de trabajo?

Tabla 29

Uso de computadoras en su rutina de trabajo

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
De 0% a 5%	1	5,0	5,0	5,0
De 5% a 10%	2	10,0	10,0	15,0
De 10% a 15%	5	25,0	25,0	40,0
De 15% a 50%	8	40,0	40,0	80,0
De 50% a 100%	4	20,0	20,0	100,0
Total	20	100,0	100,0	

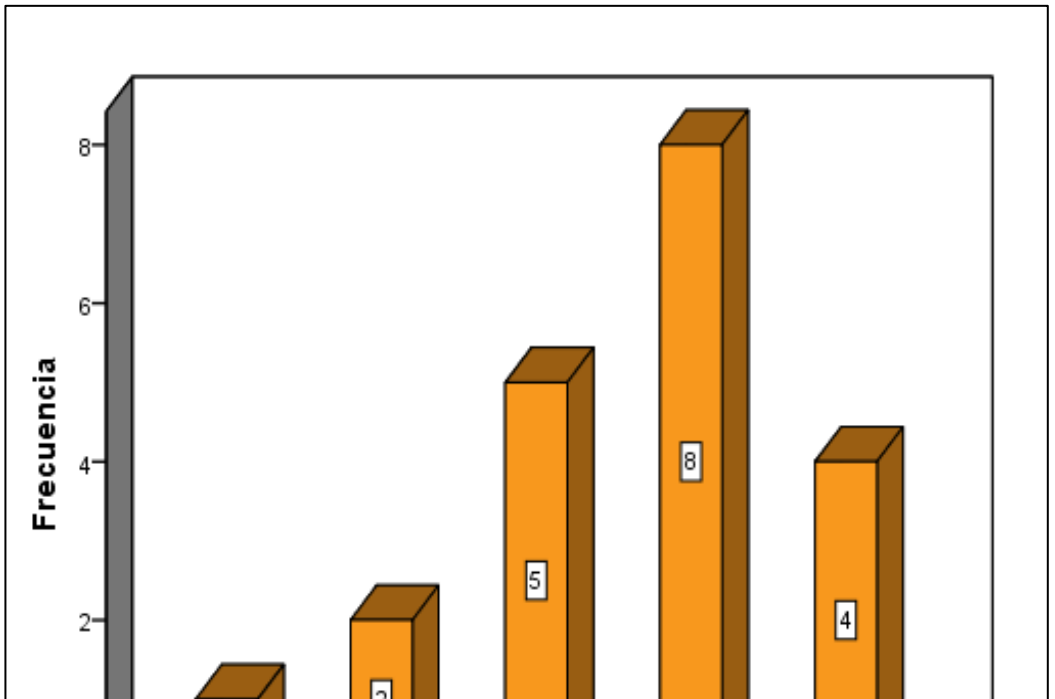


Figura 28 Porcentaje de Uso de Internet

Interpretación:

En la realización de las encuestas se obtuvo los siguientes datos donde, 8 de las empresas encuestadas evidencian que el 50% de sus empleados utiliza un computador, seguido de 4 empresas que más del 50% de sus trabajadores manipula un ordenador en su rutina de diaria, 5 empresas se ubican en el rango del 15 a 50% de sus empleados que utiliza un computador, ya reduciéndose el rango de 5 al 10% se hallan dos empresas y una empresa en el rango inferior del 0 al 5% de empleados en la utilización de computadoras pudiéndose suponer que es una microempresa.

Pregunta N° 15

15. ¿Dispone su empresa de Página Web?

Tabla 30

Disponen de Pagina Web

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	18	90,0	90,0	90,0
No	2	10,0	10,0	100,0
Total	20	100,0	100,0	

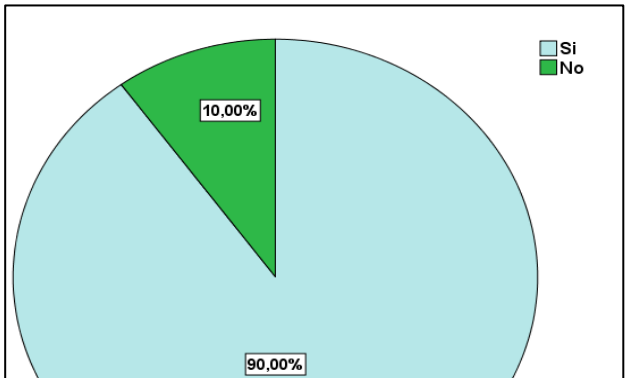


Figura 29 Disponen de Pagina Web

Interpretación:

Con respecto a las encuestas realizadas a las empresas del sector industrial se puede evidenciar que el 90% de las de las mismas mencionan que disponen de una página web lo cual es muy importante ya que de esta manera pueden propagandas de publicidad y promocionar sus productos que cada una lo elabora, pero también al poseer la mayoría de empresas de una página web este medio puede ser un agujero para el robo de información por parte de los intrusos o mafias internacionales, a diferencia de un 10% del total no poseen una página web, quizá por la actividad que lo realizan o el poco interés por parte de la administradores.

Pregunta N° 15.1

15.1 ¿Con qué frecuencia se actualiza la Página Web de su empresa?

Tabla 31

Frecuencia de Actualización de página web

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Cada dos semanas	5	25,0	27,8	27,8
Cada mes	1	5,0	5,6	33,3

Trimestralmente	4	20,0	22,2	55,6
Semestralmente	3	15,0	16,7	72,2
Anualmente	5	25,0	27,8	100,0
Total	18	90,0	100,0	
Sistema	2	10,0		
	20	100,0		

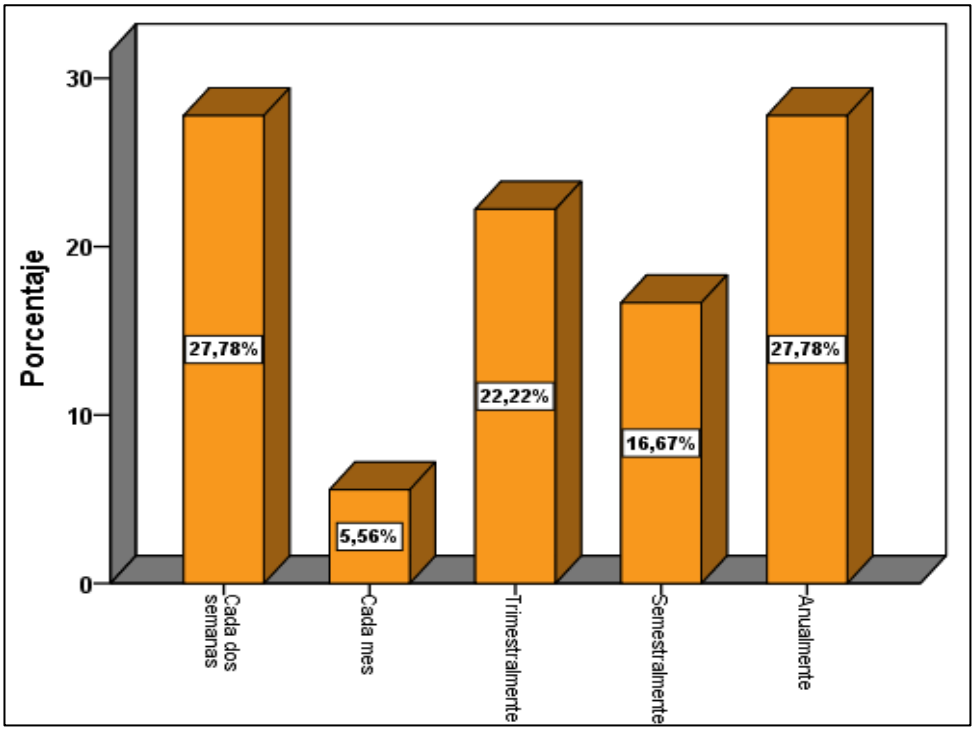


Figura 30 Frecuencia de Actualización de página web

Interpretación

De acuerdo a las encuestas realizadas a las empresas del sector industrial se ha podido constatar que el 27,78% mencionan que actualizan su página web cada dos semanas, lo cual muestran que están constantemente controlando su página web y de esta manera proteger su información lo cual es muy importante para el desarrollo de las mismas económicamente mientras que el 5,56% lo realizan cada mes, el 22,22% lo hacen trimestralmente, el 16,67% semestralmente y el 27,78% lo realizan de manera anual, y tan solo un 10% de las empresas que no poseen página web no lo realizan, en ninguno de los periodos mencionados o analizados mediante la ejecución de las encuestas.

Pregunta N° 16

16. ¿Está su empresa interesada en poner en marcha un sistema informático de protección de datos o actualizarlos?

Tabla 32

Protección de Datos

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Siempre	12	60,0	60,0	60,0
Casi siempre	3	15,0	15,0	75,0
Frecuentemente	2	10,0	10,0	85,0
A veces	3	15,0	15,0	100,0
Total	20	100,0	100,0	

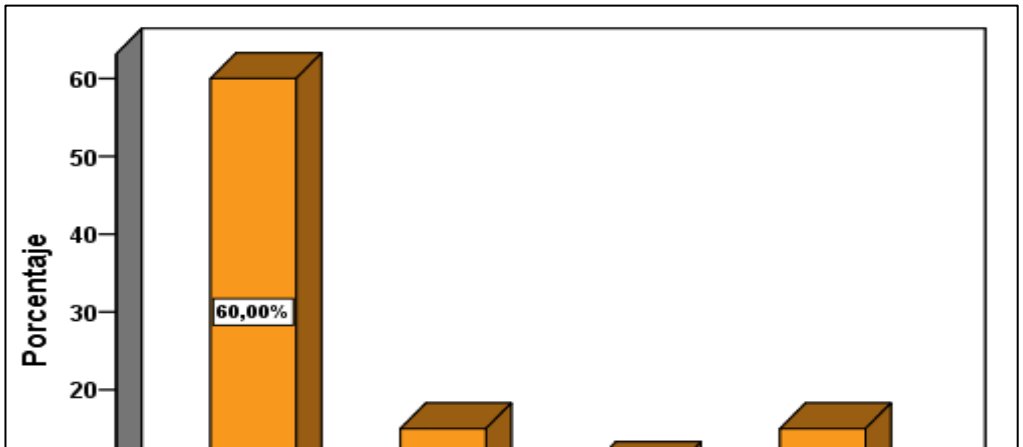


Figura 31 Protección de Datos

Interpretación:

Con respecto a las encuestas realizadas se puedo evidenciar que el 60% de las empresas del sector industrial están siempre interesadas en poner en marcha un sistema informático de protección de datos o actualizarlos de manera constante, lo cual es un porcentaje bastante alto a diferencia que un 15% mencionan que casi siempre lo realizan, un 10% lo realizan frecuentemente, y un 15% mencionan que lo ejecutan a veces, con respecto a estos datos se podría decir que la mayoría de empresas hoy en día sin importar su actividad o volumen de ventas que lo realicen están en la disposición proteger su información, para de esta manera evitar fraudes informáticos o que su información sea vulnerable a diversos ataques o robos por parte de mafias internacionales.

Pregunta N° 17

17. ¿En los últimos 5 años ha sufrido alguna fuga de información o ataque informático la empresa?

Tabla 33

Fuga de información últimos años

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Siempre	1	5,0	5,0	5,0
Casi siempre	1	5,0	5,0	10,0
Frecuentemente	1	5,0	5,0	15,0
A veces	6	30,0	30,0	45,0

Nunca	11	55,0	55,0	100,0
Total	20	100,0	100,0	

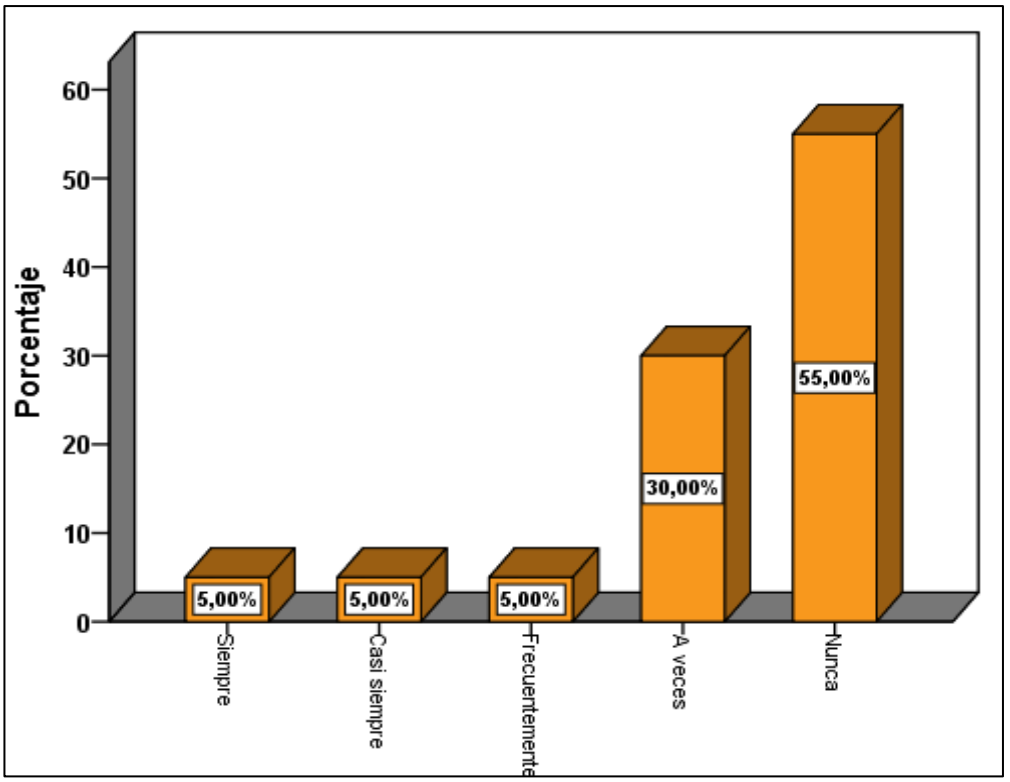


Figura 32 Fuga de información últimos años

Interpretación:

Un 5% de las empresas del sector industrial manifiestan que durante los últimos 5 años han sufrido siempre fuga de información o ataques cibernéticos por pate de mafias internacionales, ya que no existo un control total de los sistemas tecnológicos para evitar fraudes informáticos, otro 5% mencionan que casi siempre sufren fugas de información o ataques por parte de intrusos, otro 5% manifiestan que son atacados de manera frecuentemente, y un 30% a veces, a diferencia de un 55% que es la mayoría manifiestan que nunca han sufrido fraudes informáticos debido a la actualización de sus páginas web o a su alto inversión en TIC, pero esto no quiere decir que estas empresa no están expuestas a alguna fuga de información o ataque cibernético.

Pregunta N° 18

18. ¿Qué tipo de fraude informático ha sufrido su empresa?

Tabla 34

Fraudes informáticos sufridos

	Respuestas		Porcentaje de casos
	N	Porcentaje	
Encriptación de información	4	16,7%	33,3%
Borrado de datos	1	4,2%	8,3%
Virus	7	29,2%	58,3%
Intervención de páginas maliciosas	2	8,3%	16,7%
Suplantación de identidad (Phishing)	1	4,2%	8,3%
Clonación de páginas en redes sociales	1	4,2%	8,3%
Correos maliciosos	8	33,3%	66,7%
Total	24	100,0%	200,0%

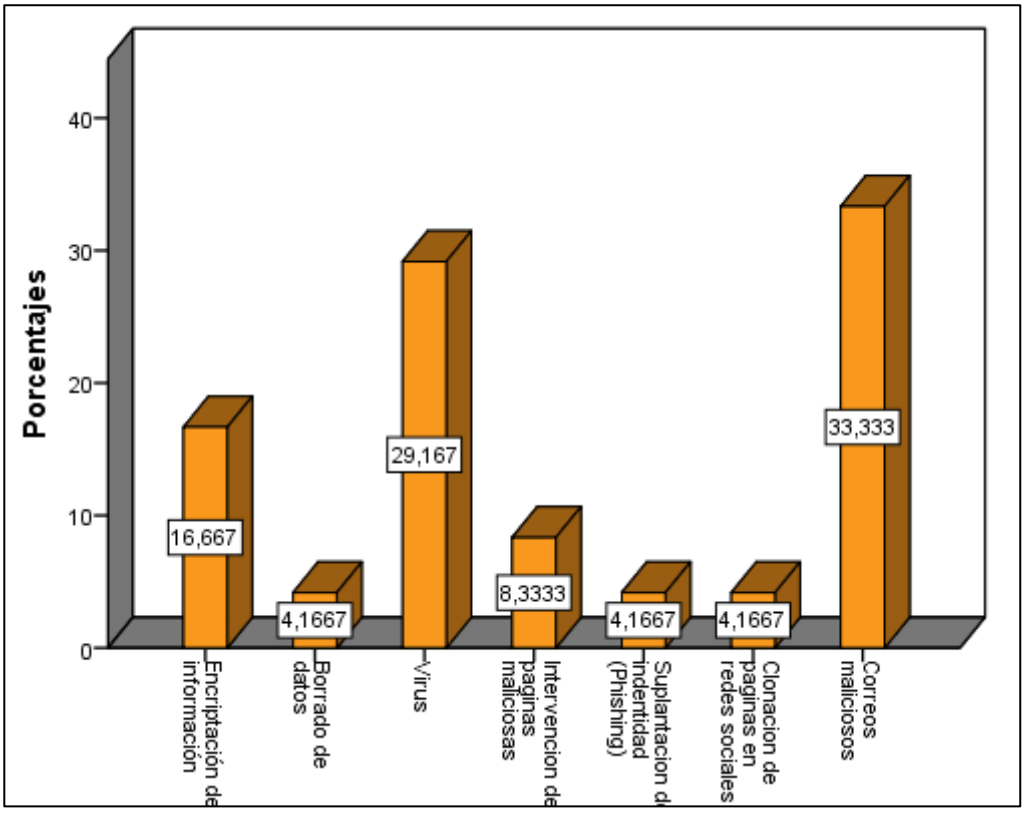


Figura 33 Fraudes informáticos sufridos

Interpretación:

Mediante las encuestas realizadas se ha podido verificar que el 33,30% de las empresas del sector industrial han sufrido fraudes informáticos mediante correo maliciosos quizá estos utilizados o provocados por mafias internacionales que realizan como trampa de engaño o agujero para filtrar a la información de una persona o una organización, seguido del 29, 20% sufren fraudes informáticos mediante virus, el 16,70% mediante encriptación de Información, el 8,30% mediante intervención de páginas maliciosas, el 4,20% mediante borrado de datos, el 4,20% mediante suplantación de información (Phishing), y el 4,20% mediante clonación de páginas en redes sociales, por lo que se puede decir que la mayoría de fraudes informáticos que han sufrido las empresas son mediante correo maliciosos y virus, que con el simple hecho de abrirlos para recabar su información se crean puertas traseras para el acceso a la información confidencial de una persona u empresa.

Pregunta N° 19

19. ¿De acuerdo a la respuesta de la pregunta anterior, usted cree que los fraudes informáticos, afectan a los recursos económicos financieros de la empresa?

Tabla 35

Afectación de Recursos Financieros

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en acuerdo	14	70,0	73,7	73,7
En acuerdo	4	20,0	21,1	94,7
En desacuerdo	1	5,0	5,3	100,0
Total	19	95,0	100,0	
Sistema	1	5,0		

	20	100,0

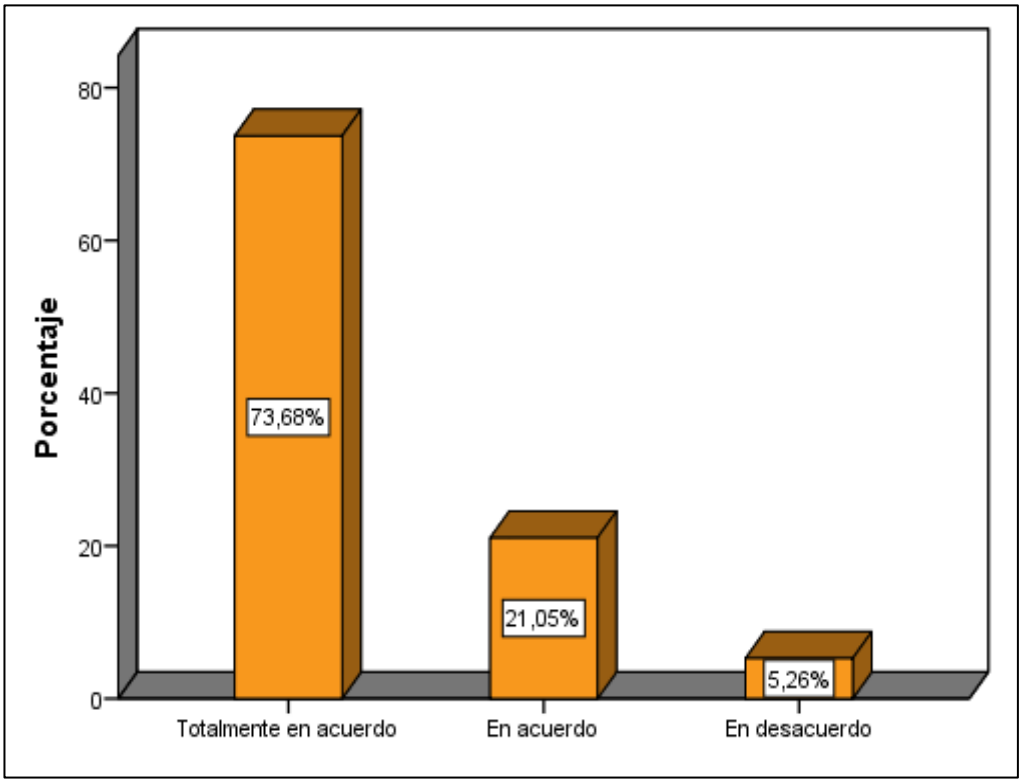


Figura 34 Afectación de Recursos Financieros

Interpretación:

El 73.68 % de las empresas del sector industrial están totalmente de acuerdo que los fraudes informáticos afectan a los recursos económicos financieros de las empresas, ya que muy independiente de que si son afectados por un ataque o no, tienen una percepción de que cualquier vulnerabilidad pueda afectar en menor o mayor medida de acuerdo a su actividad que lo realicen, de acuerdo a este porcentaje obtenido podemos decir que a nivel mundial los fraudes informáticos afectan al desarrollo de las empresas , también un 20% manifiestan estar en acuerdo de la afectación de los ataques y tan solo el 5% están en desacuerdo. Por lo tanto se establece que muchas empresas sin importar su movimiento económico han sufrido fraudes informáticos o fuga de información, aunque se puede decir que las afectaciones también se dan de manera indirecta como efecto de ataque de

gran magnitud en algunas ocasiones llevándoles a la ruina y quizá hasta su desaparición del mercado.

Pregunta N° 20

20. ¿Considera usted que la información de la empresa es vulnerable a fraudes Informáticos?

Tabla 36

Empresa es vulnerable a fraudes informáticos

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Siempre	5	25,0	25,0	25,0
Casi siempre	4	20,0	20,0	45,0
Frecuentemente	1	5,0	5,0	50,0
A veces	9	45,0	45,0	95,0
Nunca	1	5,0	5,0	100,0
Total	20	100,0	100,0	

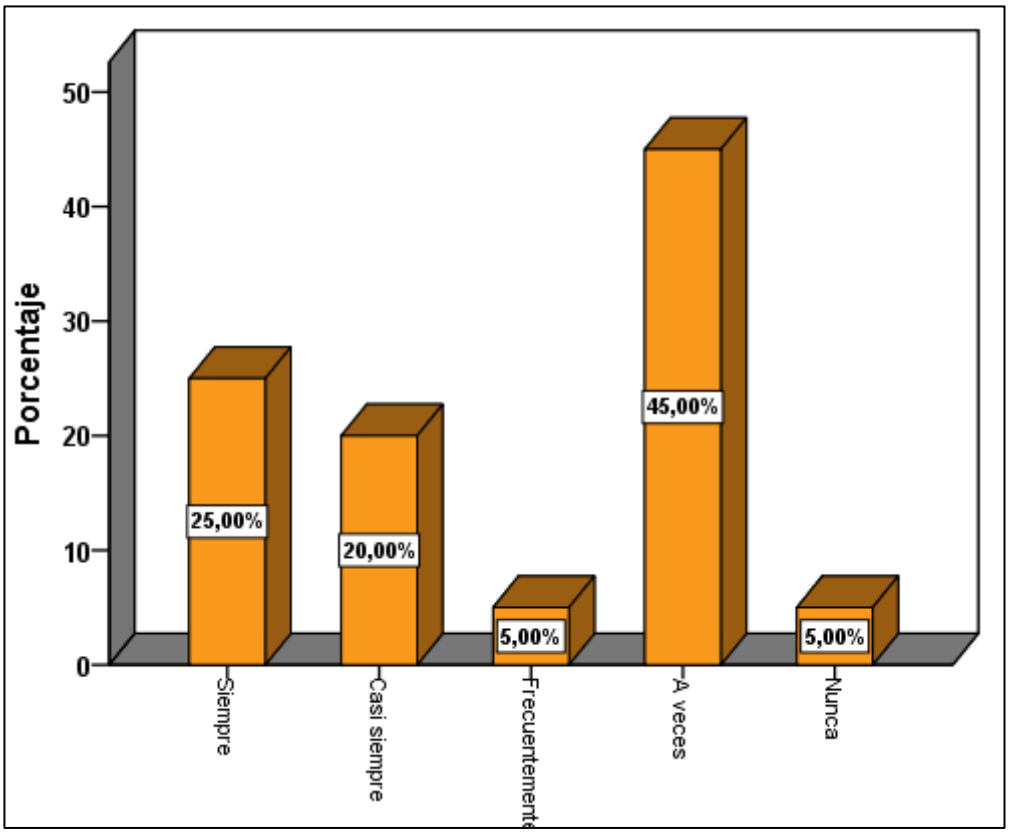


Figura 35 La información de la Empresa es vulnerable a fraudes informáticos

Interpretación:

De acuerdo a las encuestas realizadas se pudo constatar que el 25% de las empresas del sector industrial consideran que la información de la empresa es siempre vulnerable a fraudes Informáticos debido a que no existe un control específico para la protección de la información, el 20% consideran que casi siempre son vulnerables, el 5% consideran que frecuentemente, el 45% consideran que a veces la información es vulnerable y tan solo el 5% cree que nunca la información de la empresa es vulnerable a fraudes Informáticos, específicamente se da en las empresas grandes donde poseen sistemas de seguridad más especializados en protección de datos. En consideración a estos datos se podría decir que si existe un control adecuado en la información de cada una de las empresas, ya que actualizan de manera constante su página web y poseen de adecuados sistemas informáticos que ayudan a controlar la fuga de información.

Pregunta N° 21

¿Realiza copias de seguridad de forma planificada y oportuna?

Tabla 37

Copias de seguridad

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Siempre	15	75,0	75,0	75,0
Casi siempre	4	20,0	20,0	95,0
Frecuentemente	1	5,0	5,0	100,0
Total	20	100,0	100,0	

Figura 36 Copias de seguridad

Interpretación

De acuerdo a la información obtenida y a los datos tabulados se puede evidenciar que el 75% de las empresas del sector Industrial realizan siempre copias de seguridad de forma planificada y oportuna, un 20% casi siempre, y tan solo un 5% de manera frecuentemente, con respecto a esto se podría decir que la mayoría de las empresas tienen copias de su información de cada una de las actividades que se va realizando a diario.

4.1. Discusión de los Resultados

En la obtención de los resultados de las empresas involucradas del sector industrial de la Provincia de Cotopaxi, se puede evidenciar que la información proporcionada es veraz de acuerdo a la información recabada por la Superintendencia de Compañías, Cámara de Comercio de Latacunga, Cámara de industrias de Cotopaxi y el cruce con todas la empresas de este sector, para de esa forma realizar la comprobación de la hipótesis, correlación de las variables e interpretación.

Dentro de la comprobación de hipótesis los resultados obtenidos, se afirma que los fraudes informáticos no afectan a los resultados económicos de la empresas del sector manufacturero de la provincia, cabe recalcar que las grandes empresas tienen contratado sistemas eficientes de protección de

datos, a lo contrario de las pequeñas que por la actividad o el giro del negocio no aseguran de manera completa o integral sus datos, lo hacen manera básica protegiendo la información medianamente y es ahí donde existen espacios, o puertas traseras para el acceso indebido y manipulación maliciosa de los sistemas de datos.

La encriptación de la información es uno de los fraudes o delitos cibernéticos que se pudieron evidenciar dentro de nuestra investigación tanto en empresas pequeñas y medianas, de igual manera los virus son un medio de acceso para los ciberdelincuentes ya que es la manera habitual y fácil para enviar correos electrónicos como punto de entrada de información maliciosa o con el simple de la apertura de los mismos correos o el hecho de dar un clip a los enlaces que vienen consigo.

En relación a la evaluación que se tomó de las encuestas realizadas a las empresas industriales, se adoptó realizar una herramienta de ayuda de manera general en la protección de los datos y sistemas de información, ya que muchas organizaciones no le dan prioridad al buen uso y manejo de las tecnologías de información para el resguardo de sus datos.

4.3. Evaluación de los Resultados

a) Cruce de Variables de la Investigación

El cruce de variables se lo realiza de un grupo de preguntas seleccionadas de la encuesta denominada como fuente de recolección de la información en la presente investigación, para de esa manera determinar la correlación que existe entre las interrogantes seleccionadas.

Tabla 38
Cruce de Variable N° 1

		¿Cuánto estima usted que ha invertido en TIC durante el periodo 2012 – 2016?					
		Entre 1.000 a 10.000 dólares	Entre 10.000 a 25.000 dólares	Entre 25.000 a 50.000 dólares	Entre 50.000 a 100.000 dólares	Más de 100.000 dólares	Total
		%	%	%	%	%	%
¿De qué tamaño es su Empresa?	Grande	14,30%	42,90%	28,60%	0,00%	14,30%	100,00%
	Mediana	33,30%	16,70%	33,30%	16,70%	0,00%	100,00%
	Pequeña	60,00%	20,00%	0,00%	0,00%	20,00%	100,00%
	Microempresa	100,00%	0,00%	0,00%	0,00%	0,00%	100,00%

Interpretación

Con respecto a las preguntas cogidas para el cruce de la primera variable se puede evidenciar que depende mucho el tamaño de la empresa para realizar una inversión alta o baja en tecnología de información, con la finalidad de prevenir posibles ataques informáticos o vulnerabilidades a sus sistemas de información, dando como resultado en el primer cruce de variables que las empresas grandes invierten un 42,90% entre 10.000 y 25.000 dólares, esto debido a que concentran una cantidad mayor en sus activos dentro de sus estados financieros en el periodo 2012-2016, y que cada año existe una inversión proporcional, por lo tanto se determinó que las empresas pequeñas tienen una inversión del 60% entre el rango de 1.000 a 10.000 dólares, y como dato significativo que el 100% de las microempresas tienen de inversión entre 1.000 a 10.000 dólares.

Tabla 39
Cruce de Variable N° 2

		Qué sistema dispone su Empresa					
		ERP (Planificación de Recursos Empresariales)	PLC (Controlador Lógico Programado)	CRM (Gestión de Servicio al Cliente)	SIAF (Sistema de Información y Administración Financiera)	SAP (Sistemas, Aplicaciones y Productos)	**Total**
A qué actividad manufacturera se dedica su Empresa	Construcción %	10,00%	5,00%	5,00%	10,00%	0,00%	20,00%
	Calzado %	0,00%	0,00%	0,00%	5,00%	0,00%	5,00%
	Imprenta %	0,00%	0,00%	5,00%	0,00%	0,00%	5,00%
	Lácteos %	10,00%	0,00%	0,00%	5,00%	0,00%	15,00%
	Textil %	0,00%	0,00%	0,00%	5,00%	0,00%	5,00%
	Bebidas %	0,00%	0,00%	0,00%	5,00%	5,00%	10,00%
	Alimentos %	25,00%	5,00%	10,00%	15,00%	5,00%	30,00%
	Otros %	10,00%	5,00%	5,00%	0,00%	5,00%	10,00%
Total		55,00%	15,00%	25,00%	45,00%	15,00%	100,00%

Interpretación:

Para el siguiente cruce de variables y su relación con la investigación del fraude informático y las vulnerabilidades que pueden tener las empresas del sector industrial, se ha dispuesto una combinación de acuerdo a la actividad de la empresa y el tipo de sistema informático que posee, dando como resultado que un 10% de utiliza el ERP (Planificación

de Recursos Empresariales) y SIAF (Sistema de Información y Administración Financiera) dentro del sector de la construcción, seguido del sector de alimentos que de igual manera un 15% y 25% maneja los sistemas ERP y SIAF, y como no menos importante un 5% abarcan los sistemas de CRM, SAP y PLC, todo de acuerdo a la actividad de las organizaciones.

Poniendo de manera general y abarcando a todo el sector manufacturero y cada sistema que disponen, obtenemos que el 55% de las industrias poseen el sistema ERP (Planificación de Recursos Empresariales) que ayuda a la integración de operaciones en una empresa en especial de la que tienen que ver con las actividades de producción, logística, inventarios y contabilidad para de esa manera dar tiempos rápidos de respuesta a sus problemas, minimizando los costos y con capacidad suficiente para la toma de decisiones.

En segundo lugar el sistema informático que disponen las empresas con un notable 45% es el SIAF (Sistema de Información y Administración Financiera), herramienta muy importante y complementaria a cada una de las operaciones en lo que se refiere al registro de ingresos y egresos, pero sobre todo llevar un control de su contabilidad, presupuestos y fondos económicos de las organizaciones.

Y como un tercer sistema no menos importante dentro de las operaciones de las empresas del sector industrial tenemos a CRM (Gestión de Servicio al Cliente) con un 25%, algo importante ya que esta herramienta ayuda a ofrecer una mejor atención y servicio al cliente, como un medio de respuesta y capacidad de resolver cualquier problema dentro de las entidades.

Tabla 40
Cruce de Variable N° 3

			Tipo de Fraude							
			Encriptación de información	Borrado de datos	Virus	Intervención de páginas maliciosas	Suplantación de identidad (Phising)	Clonación de páginas en redes sociales	Correos maliciosos	**Total**
A qué actividad manufacturera se dedica su empresa	Construcción	Recuento	1	1	3	2	0	0	2	3
		% del total	8,30%	8,30%	25,00%	16,70%	0,00%	0,00%	16,70%	25,00%
	Calzado	Recuento	1	0	0	0	0	0	0	1
		% del total	8,30%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	8,30%
	Imprenta	Recuento	0	0	1	0	1	0	1	1
		% del total	0,00%	0,00%	8,30%	0,00%	8,30%	0,00%	8,30%	8,30%
	Lácteos	Recuento	1	0	0	0	0	0	1	1
		% del total	8,30%	0,00%	0,00%	0,00%	0,00%	0,00%	8,30%	8,30%
	Textil	Recuento	0	0	1	0	0	1	0	1
		% del total	0,00%	0,00%	8,30%	0,00%	0,00%	8,30%	0,00%	8,30%
	Alimentos	Recuento	1	0	2	0	0	0	2	3
		% del total	8,30%	0,00%	16,70%	0,00%	0,00%	0,00%	16,70%	25,00%
	Otros	Recuento	0	0	0	0	0	0	2	2
		% del total	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	16,70%	16,70%
Total		Recuento	4	1	7	2	1	1	8	12
		% del total	33,30%	8,30%	58,30%	16,70%	8,30%	8,30%	66,70%	100,00%

Interpretación:

Luego de haber analizado cada una de las preguntas de las encuestas realizadas a las empresas del sector industrial se procedió a un cruce de variables para identificar que tan vulnerables son las empresas del sector industrial a fraudes informáticos, donde se tomó como preguntas claves el tipo de fraude y la actividad manufacturera que se dedica la empresa, por lo tanto se puede observar que el 25% de las empresas dedicadas a la construcción son atacadas mediante virus siendo este el porcentaje más representativo en esta actividad, el 8,30% de las industrias de calzado, Lácteos, alimentos son atacadas mediante encriptación de información, el 16,70% de las industrias de Construcción alimentos y otros son atacados mediante correos maliciosos.

Con estos últimos datos siendo los más representativos, y de acuerdo a las tendencias actuales que ha sucedido en el último semestre de 2016 e iniciando el primer semestre del 2017, como espacios de tiempo que se ha generado noticias, hechos, sucesos importantes dentro de las Tecnologías de Información y Comunicación dentro de las empresas a nivel mundial y sus sistemas de protección de datos y de la información, dentro de estudios importantes que realizan empresas de tecnología como es el caso de IBM y que determina como principal actividad fraudulenta a la intervención de virus y correos maliciosos.

Tabla 41
Cruce de Variable Nº 4

		Está su empresa interesada en poner en marcha un sistema informático de protección de datos o actualizarlos					
		Siempre	Casi Siempre	Frecuentemente	A veces	Nunca	Total
		%	%	%	%	%	%
Considera usted que la información de la empresa es vulnerable a fraudes Informáticos	Siempre	20,00%	0,00%	0,00%	5,00%	0,00%	25,00%
	Casi siempre	5,00%	15,00%	0,00%	0,00%	0,00%	20,00%
	Frecuentemente	0,00%	0,00%	5,00%	0,00%	0,00%	5,00%
	A veces	30,00%	0,00%	5,00%	10,00%	0,00%	45,00%
	Nunca	5,00%	0,00%	0,00%	0,00%	0,00%	5,00%
	Total	60,00%	15,00%	10,00%	15,00%	0,00%	100,00%

Interpretación:

Con respecto a la investigación realizada a las empresas del sector industrial se toma como referencia dos preguntas de la encuesta realizada con la finalidad de conocer que tanta importancia le dan cada una de las industrias a los sistemas informáticos, por lo que se puede decir que el 20% de las empresas del sector industrial siempre están interesadas en poner en marcha un sistema informático de protección de datos o actualizarlos para de esta manera evitar que la información de la empresa sea vulnerable a fraudes informáticos, el 15% menciona que casi siempre, el 30% a veces y tan solo un 5% nunca está de acuerdo en proteger o resguardar su información.

4.4. Comprobación de Hipótesis

PRUEBA DE HIPÓTESIS

En nuestro proyecto necesitamos saber si el Fraude Informático influye en resultados económicos financieros de las empresas del sector industrial de la Provincia de Cotopaxi para ello se utiliza el estadístico chi-cuadrado, debido a que las variables son de tipo cualitativas con nivel de medición nominal y ordinal.

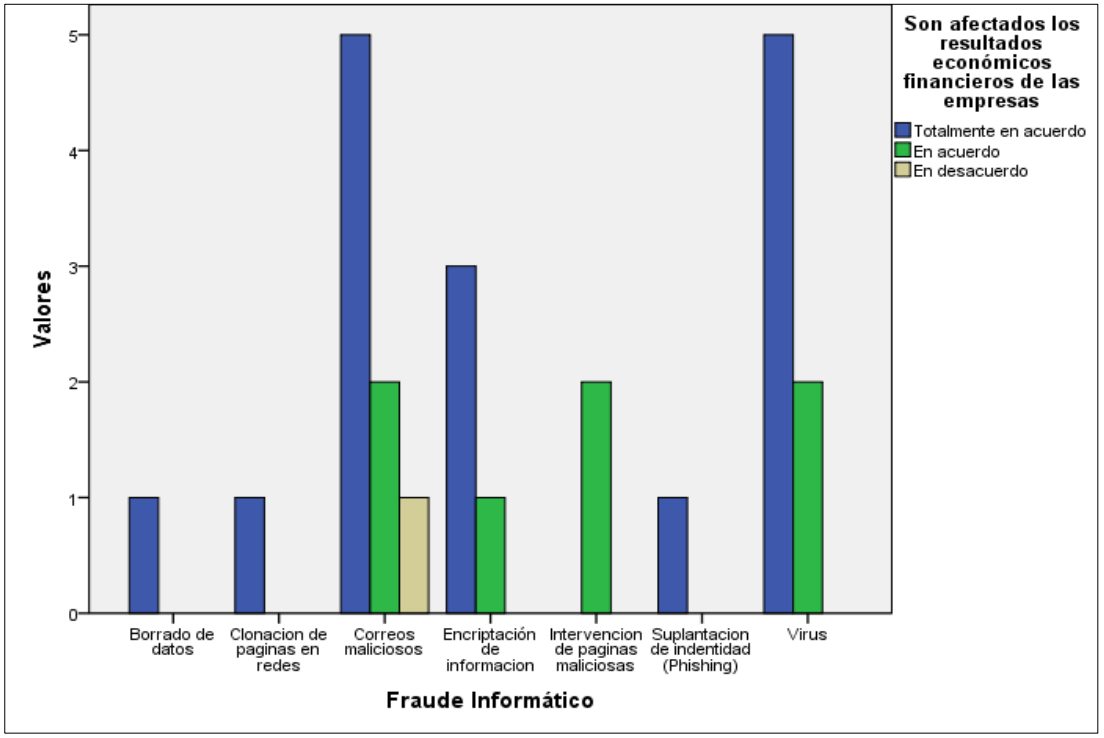


Figura 37 Prueba de Hipótesis

a) Planteamiento de hipótesis:

(H0) = Los fraudes informáticos no inciden en los resultados económicos financieros de las empresas del sector industrial de la Provincia de Cotopaxi.

(H1) = Los fraudes informáticos inciden en los resultados económicos financieros de las empresas del sector industrial de la Provincia de Cotopaxi.

b) Nivel de significación alfa=0,05 de cometer Error tipo I

Se elige un nivel de significancia del 5% para lo que es necesario indicar que tener un 5% de significancia es tener una probabilidad del 5% de cometer un error tipo I “rechazar la hipótesis alternativa siendo esta verdadera”. Como la probabilidad es del 0,05 es muy difícil de cometer este error tipo I, que es lo que tratamos de evitar en nuestro estudio.

Grados de libertad: (número de columnas -1) (número de filas -1)

Grados de libertad: (3-1) (7-1) = **12**

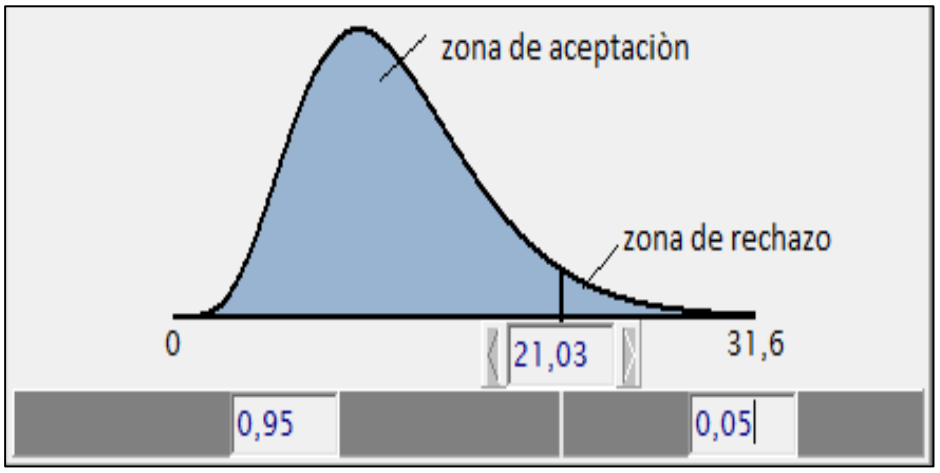


Figura 38 Campana de Gauss-Comprobación de Hipótesis

c) Determinación del estadístico mediante SPSS

Tabla 42
Cruce de variables para comprobación de hipótesis

			Son afectados los resultados económicos financieros de las empresas			
			Totalmente en acuerdo	En acuerdo	En desacuerdo	**Total**
Fraude Informático	Borrado de datos	Recuento	1	0	0	1
		Recuento esperado	0,7	0,3	0	1
	Clonación de páginas en redes	Recuento	1	0	0	1
		Recuento esperado	0,7	0,3	0	1
	Correos maliciosos	Recuento	5	2	1	8
		Recuento esperado	5,3	2,3	0,3	8
	Encriptación de información	Recuento	3	1	0	4
		Recuento esperado	2,7	1,2	0,2	4
	Intervención de páginas maliciosas	Recuento	0	2	0	2
		Recuento esperado	1,3	0,6	0,1	2
	Suplantación de identidad	Recuento	1	0	0	1
		Recuento esperado	0,7	0,3	0	1
	Virus	Recuento	5	2	0	7
		Recuento esperado	4,7	2	0,3	7
Total		Recuento	16	7	1	24
		Recuento esperado	16	7	1	24

Pruebas de chi-cuadrado			
	Valor	gl	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	8,307	12	0,761
Razón de verosimilitud	9,302	12	0,677
N° de casos válidos	**24**		

d) Decisión

Como el valor es de 8,307 < 21,03 zona de aceptación, por tanto se rechaza la hipótesis alternativa y se acepta la hipótesis nula.

e) Conclusión

Al nivel de significancia del 5% hay evidencia para concluir que Los fraudes informáticos no inciden en los resultados económicos financieros de las empresas del sector industrial de la Provincia de Cotopaxi.

4.5. Tendencia a fraudes informáticos en el Ecuador.

Según Diario la Hora en una investigación realizada sobre los delitos Informáticos manifiesta que “En Ecuador se empezó a hablar de delitos informáticos en 2009 ya que desde entonces, las autoridades han registrado 3.143 casos de robos y denuncias en los últimos años. Pero existiría un su registro de aquellas personas que no reportaron la pérdida de su información” (La Hora, 2011) .

Según El Observatorio Iberoamericano de Protección de Datos en un estudio realizado sobre los Delitos informáticos y comercio electrónico en Ecuador menciona que: “El constante progreso tecnológico que experimenta la sociedad, supone una evolución en las formas de delinquir, dando lugar, a los delitos tradicionales como a la aparición de nuevos ilícitos. Esta realidad ha originado los llamados delitos informáticos” (Observatorio Iberamericano de Protección de Datos, 2013).

> El primer delito informático que se cometió en el Ecuador fue en el año 1996 en un caso conocido, que fue denunciado pero que nunca obtuvo sentencia y es sobre el redondeo que se realizaba en las planillas realizadas por el antiguo EMETEL, y que no se sabía a donde se dirigían estas cantidades que muchas veces eran demasiado pequeñas para que cause discusión, pero ya en grandes cantidades era una cantidad de dinero muy apreciable, en esto se puede decir que se utilizó la técnica del salami o roundingdown. (Observatorio Iberamericano de Protección de Datos, 2013).

a) Tendencia de Inversión de TIC en las Empresas del Sector Industrial de la Provincia de Cotopaxi dentro del periodo (2012-2016).

Con la información obtenida de la Superintendencia de Compañías se pudo establecer una línea tendencial de las inversiones que realizan en tecnologías de información y comunicación como base primordial para la protección de información y datos que posee cada organización del sector industrial de la Provincia de Cotopaxi objeto de estudio, donde el establecimiento de tendencia se focalizo dentro de dos grupos esenciales como son las grandes empresas como eje principal en el desarrollo productivo

de la provincia y de las Pymes como el complemento dentro del impulso económico de la sociedad.

a.1 Tendencia – de Inversión de las empresas de la Provincia de Cotopaxi

Tabla 43

Tendencia – Grupo Nº 1

EMPRESAS INDUSTRIALES	AÑO 2012	AÑO 2013	AÑO 2014	AÑO 2015	AÑO 2016
FAMILIA SANCELA S.A.	$ 1.517.161,71	$ 1.678.753,33	$ 1.691.732,59	$ 1.908.739,98	$ 2.064.542,26
AGLOMERADOS COTOPAXI S.A.	$ 689.987,28	$ 688.072,15	$ 727.387,03	$ 830.868,94	$ 847.522,57
NOVACERO S.A.	$ 604.135,02	$ 802.620,57	$ 911.608,06	$ 1.018.895,08	$ 1.120.705,28
CEDAL S.A.	$ 397.106,04	$ 527.798,29	$ 604.077,93	$ 637.329,69	$ 638.071,29
MOLINOS POULTIER S.A.	$ 161.131,45	$ 172.011,05	$ 172.544,17	$ 183.064,20	$ 183.064,20

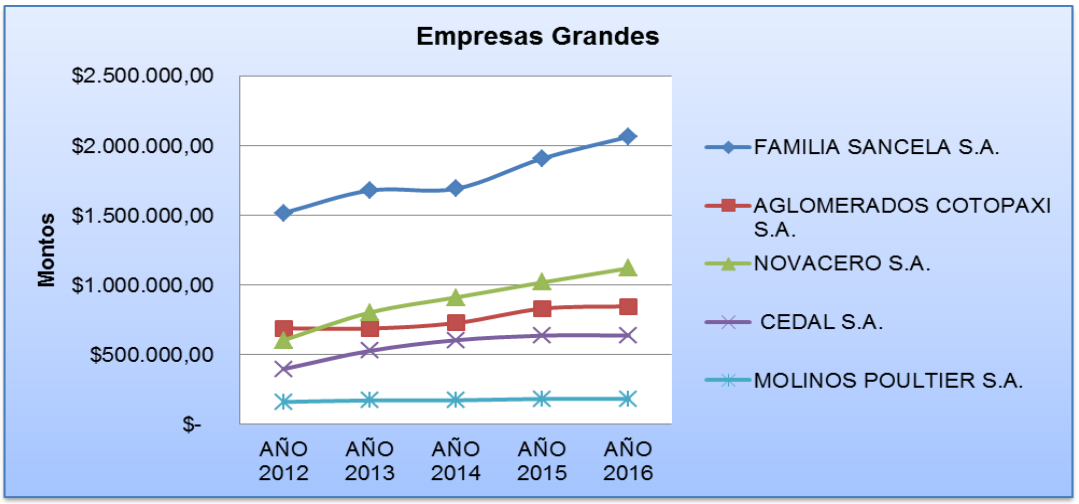


Figura 39 Tendencia - Grandes Empresas de la Provincia de Cotopaxi

Interpretación

Dentro del grupo de las grandes empresas dentro del periodo comprendido se da a notar un incremento considerable y muy importante en algunas empresas como es el caso de Familia Sancela que su inversión ha incrementado en un 25% del 2012 al 2016, caso similar de la empresa Novacero S.A, caso particular de la empresa Molinos Poultier S.A. que ha mantenido una regularidad e inversión en el lapso de tiempo analizado.

b.1 Tendencia – de Inversión de las empresas de la Provincia de Cotopaxi

Tabla 44

Tendencia – Grupo Nº 2

EMPRESAS INDUSTRIALES	AÑO 2012	AÑO 2013	AÑO 2014	AÑO 2015	AÑO 2016
FUENTES SAN FELIPE S.A.	$ 45.142,30	$ 49.429,68	$ 57.006,32	$ 64.499,32	$ 68.555,72
CALZACUBA CIA. LTDA.	$ 4.375,03	$ 4.571,46	$ 4.571,46	$ 7.010,74	$ 7.260,74
EDITORIAL LA GACETA S.A.	$ 17.245,85	$ 24.290,85	$ 25.440,85	$ 25.440,85	$ 25.440,85
INDUSTRIA LICOREC S.A.	$ 2.103,15	$ 72.898,82	$ 85.723,41	$ 97.493,21	$ 97.493,21
PARMALAT DEL ECUADOR S.A.	$ 39.596,71	$ 54.078,16	$ 84.582,16	$ 116.818,72	$ 114.719,36

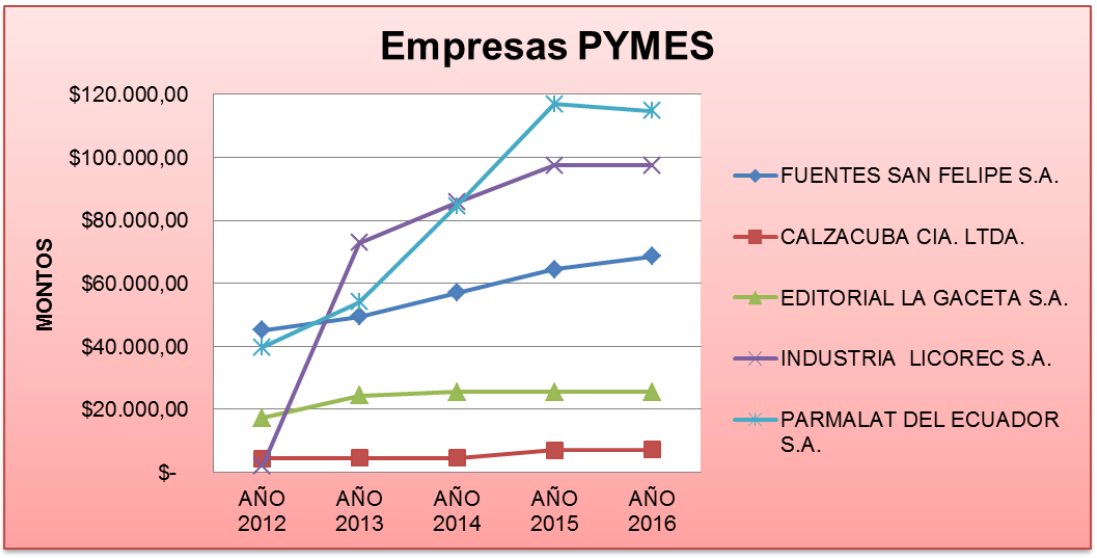


Figura 40 Tendencia - PYMES de la Provincia de Cotopaxi

Interpretación

En el grupo de las Pymes, similar periodo comprendido se verifica un incremento con variaciones importantes en las empresas como Parmalat S.A., Licorec S.A, caso similar de la empresa Novacero S.A, caso particular de la empresa Calzacuba S.A. que ha mantenido una regularidad e inversión debido a que es una pequeña empresa.

CAPÍTULO V

5. PROPUESTA DE LA INVESTIGACIÓN

5.1. Diagnóstico de los fraudes informáticos o ataques cibernéticos en el Ecuador.

La tecnología informática hoy en día está presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los grandes avances de la tecnología, y comienzan a utilizar los sistemas de información más sofisticados para ejecutar cualquier tipo de actividad que en otros tiempos se realizaban manualmente.

En el Ecuador el fenómeno de los llamados delitos informáticos o ataques cibernéticos han alcanzado una tendencia creciente debido a que se ha constatado la vulneración de información y datos a empresas multinacionales, privadas y públicas.

Según (El Comercio, 2015) menciona que el 19 de enero pasado, el país registró el primer ataque masivo de las cibermafias ya que 17 empresas de Quito, Guayaquil y Cuenca fueron afectadas de manera directa a sus sistemas informáticos. En Ecuador están registradas más de 67000 empresas, pero el ataque a 17 empresas llamó la atención, porque se consideró que la difusión del virus fue sostenida y masiva.

Según el diario el Telégrafo en un estudio realizado sobre los fraudes Delitos Informáticos en el Ecuador menciona que “La Fiscalía General del Estado registró 530 delitos informáticos en los primeros cinco meses de 2016, en el mismo período del año anterior se presentaron 635 denuncias. Las cifras evidencian una disminución notable entre los dos años” (El Telégrafo, 2016)

Según el diario el Telégrafo en un estudio realizado sobre los fraudes Delitos Informáticos en el Ecuador menciona que “En Guayas hubo 18 casos; Pichincha, 145; Manabí, 24; El Oro, 22; en el resto de provincias se registró

una cantidad menor e la cual está incluida la Provincia de Cotopaxi. La mayoría de denuncias (368) corresponde al delito de “apropiación fraudulenta por medios electrónicos” (El Telégrafo, 2016).

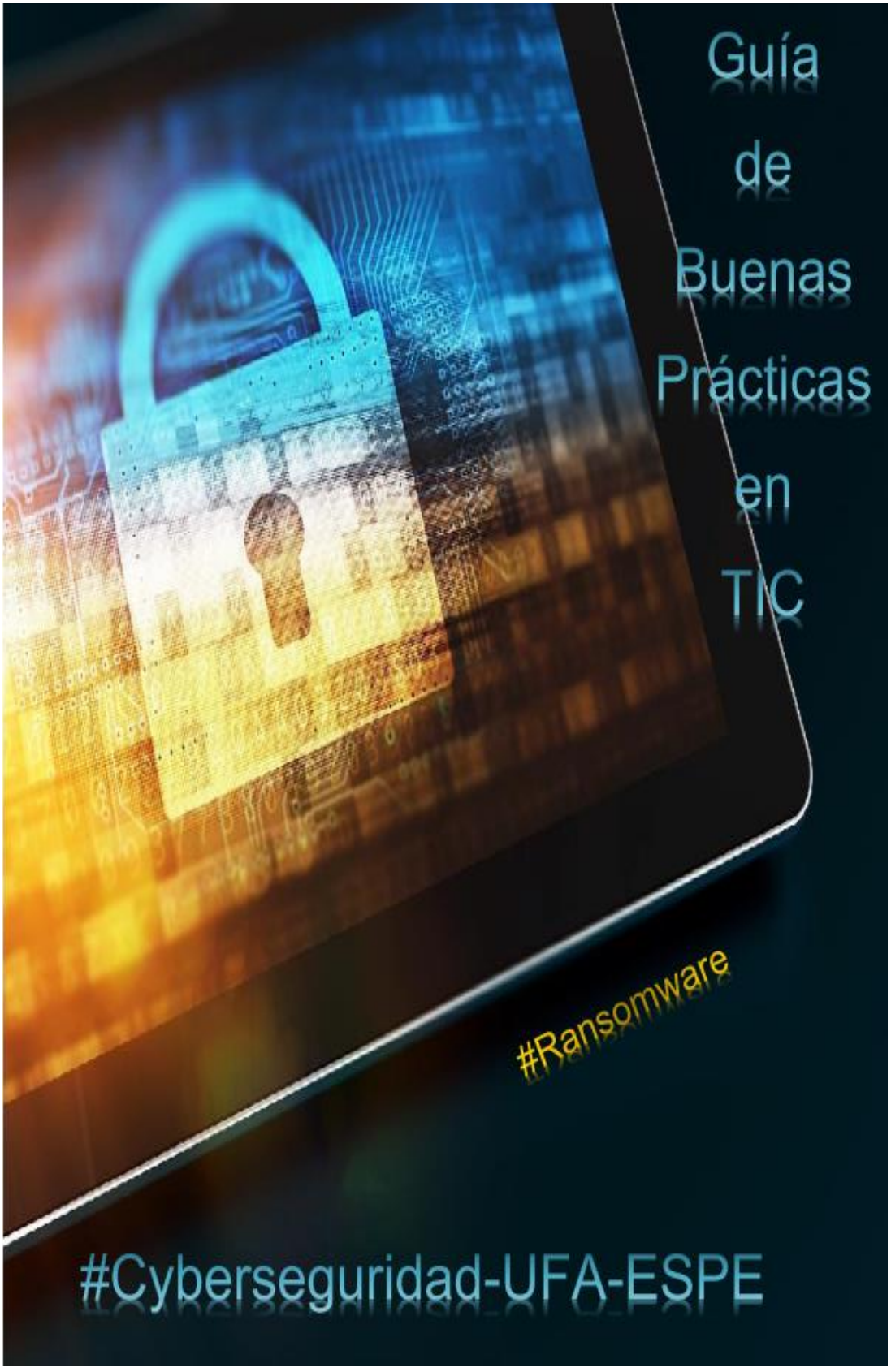
Un estudio elaborado por la Policía Nacional, Interpol, el centro de respuesta a Incidentes Informáticos del Ecuador (Ecucert), con el soporte de organismos similares de América Latina, indica que:

- El 85% de los ataques a los sistemas informáticos son causados por errores de los usuarios, quienes no toman precauciones al acceder a las redes sociales.
- El 35% ha realizado clics en correos recibidos por emisores desconocidos.
- El 80% de las amenazas en redes sociales se debe a la curiosidad de los usuarios por ver quienes observan su perfil.
- Tan solo el 59% de los usuarios almacenan información de trabajo en las nubes. (El Telégrafo, 2016).

Los delincuentes informáticos en la actualidad son tan diversos como sus delitos que se presen en diferentes lugares del mundo y puede tratarse de terroristas, estudiantes o figuras del de mafias internacionales. Por esta razón se puede decir que el mayor porcentaje de fraudes o robo de información lo realizan los empleados de empresas, que son responsables del 90% de los ataques cibernéticos.

Los intrusos o llamados hackers pueden pasar desapercibidos a través de las fronteras ocultas de los sistemas informáticos o también pueden ocultarse tras incontables “enlaces” o simplemente desvanecerse sin dejar ninguna huella o rastro. Pueden despachar directamente las comunicaciones o esconder pruebas delictivas en (paraísos informáticos) -o sea, en países que carecen de leyes o experiencia para seguirles la pista del robo de información.

5.2. Elaboración de una Guía de Buenas Prácticas de control de vulnerabilidades en Fraudes Informáticos para las empresas de la Provincia de Cotopaxi.


Guía
de
Buenas
Prácticas
en
TIC
#Ransomware
#Cyberseguridad-UFA-ESPE

Guía de Buenas Prácticas en TIC

(Tecnologías de Información y Comunicación)

a) Prólogo

El propósito de la presente Guía de Buenas Practicas en Tecnologías de Información y Comunicación (TIC), es proporcionar un conjunto de herramientas consejos y soluciones, para la prevención y detección de fraudes informáticos o delitos cibernéticos que en la actualidad se encuentran en auge en la industria global, debido al gran avance de la tecnología y el acceso fluido al internet, servirá de gran aporte a todas las empresas del sector industrial de la Provincia de Cotopaxi, ilustrando con métodos fáciles y comprensibles, de esta manera facilitar la resolución de diversos problemas que se pueden suscitar dentro de los sistemas del área de tecnologías de las organizaciones y así evitar fugas de información que serían de vital importancia en el desarrollo de sus actividades diarias.

Lo que se presenta son diferentes hechos, casos, datos significativos, información relevante de acuerdo a la problemática que se ha originado en los últimos años con respecto a la Ciberseguridad.

Por último, la principal característica de esta guía es el enfoque al gerente y cada uno de los empleados dentro del área de tecnologías de información y comunicación de la empresa en general, y de esa forma orientar a promover la buena práctica empresarial dentro de los sistemas de información.

b) Introducción

Las empresas del sector industrial de la Provincia de Cotopaxi, juegan un papel muy importante en la economía de nuestro país y poco a poco se suman y se van adaptando a la era digital y tecnológica. Muchas de ellas están utilizando dispositivos móviles, acceso a Internet y las tecnologías de la comunicación e información (TIC) para potenciar su actividad manufacturera para llegar a nuevos mercados e incrementar las ventas y productividad, así como para almacenar, procesar y transmitir información que podría ser sensible o confidencial. Ante tal situación, las empresas deben de tomar en consideración los riesgos asociados e implementar políticas, mejores prácticas y mecanismos de seguridad para la protección de redes y sistemas, ya que los ataques cibernéticos van en aumento y cada vez son más sofisticados y persistentes.

En el Ecuador existe escasa estadística porcentual de empresas que han sido víctimas de ataques cibernéticos, a diferencia que en Estados Unidos y España más del 50% de las organizaciones empresariales han sido vulneradas, lo cual nos hace suponer que nuestras empresas también están siendo foco de posibles intervenciones externas, solo que sus capacidades no permiten prevenir ni mucho menos identificar ese tipo de intromisiones.

Debido a la falta de difusión, conocimiento, educación, asesoría e inclusión tecnológica, la gran mayoría de las empresas del sector industrial, desconocen de los riesgos y/o consideran que no son objeto de ataques cibernéticos, pues tienen información importante que es atractiva para los cibercriminales, tales como información de empleados, proveedores, clientes y socios comerciales, información bancaria, contable y financiera, plan y estrategia de negocios, e incluso propiedad intelectual (fórmulas, secretos comerciales, investigaciones, etc.). Considerando que no importa el tamaño de la empresa y su giro comercial, siempre existe un riesgo y si los propietarios y/o administradores deciden no invertir en seguridad, el riesgo es más alto.

c) Secciones que constan en la Guía de Buenas Practicas en TIC

La Guía de Buenas Practicas consta de las siguientes secciones:

- Sección 1: Fundamentos teóricos
- Sección 2: Gestión de los activos
- Sección 3: Medidas de seguridad básica
- Sección 4: Seguridad de las operaciones
- Sección 5: Herramientas de cifrado
- Sección 6: Gestión del riesgo de TI
- Sección 7: Detección de intrusos
- Sección 8: Procesos, técnicas y normativa para la ciberseguridad dentro de las empresas
- Sección 9: Nube de datos
- Sección 10: Estudios, datos e información
- Sección 11: Instrumento de evaluación
- Sección 12: Representación gráfica de los diagramas de flujo

La Guía de Buenas Prácticas

Se

Encuentra Anexada a la Investigación.

CONCLUSIONES

- Durante la investigación realizada lo primordial fue indagar a profundidad que tan vulnerables se encuentran las empresas del sector industrial a fraudes Informáticos, determinando que las pequeñas empresas son más propensas a ataques cibernéticos, esto se da debido a que las mismas no cuentan en su estructura organizacional con un departamento de tecnologías de información y comunicación que sirva de apoyo en el desarrollo de sus operaciones de manera sistemática y confiable.
- Para la ejecución del presente estudio se utilizaron diversas herramientas como encuestas, cédulas sumarias, diagnóstico financiero y cuestionario de control Interno para la obtención de información específica y relevante sobre la perspectiva general que tienen las empresas del sector industrial con respecto a la gestión en TIC y de esta manera se pudo identificar que las medianas y grandes empresas tienen una inversión significativa en seguridad informática, a diferencia que las microempresas que por su misma condición no cuentan con estructuras organizacionales sólidas que le permitan mitigar posibles fraudes y ataques informáticos.
- Para la ejecución de la presente investigación se inició con un diagnostico financiero obteniendo que del total de las empresas el 80% tienen una inversión significativa en propiedad planta y equipo en sus estados de situación financiera y de esta manera aplicar los instrumentos de recopilación de información en las entidades del sector manufacturero que se dedican a las siguientes actividades como es: construcción, metal mecánica, alimentos, bebidas, imprenta, calzado, lácteos, textiles y entre otros.
- Del estudio se determinó que la empresa Calzacuba fue víctima de Fraude Informático, por tanto mediante la aplicación de un cuestionario de Control Interno, herramienta de evaluación basada en los componentes del COSO, se demostró que las actividades de control; información y comunicación, tienen un nivel de confianza bajo de 26,67%, frente a un nivel de riesgo alto de 73,73% con respecto al

ambiente de control, evaluación de riesgo, supervisión y monitoreo, constatando que no existe un control eficiente de los sistemas de información y por ende se deriva en una deficiente gestión en TIC.

- Para la comprobación de la hipótesis planteada se aplicó el test de Chi-Cuadrado donde se obtuvo un coeficiente de 8,31 zona de aceptación, por tanto se acepta la hipótesis nula se rechaza la hipótesis alternativa, estableciendo que los fraudes informáticos no inciden sustancialmente en los resultados económicos financieros de las empresas, ya que la mayoría de estas cuentan con sistemas de protección de datos e información eficientes y controlables, y la afectación se da en pequeñas y medianas empresas, debido a la falta de interés e inversión en recursos de tecnología de información.
- Se obtuvo la información necesaria con respecto a los fraudes informáticos más significativos que afectan a las empresas como son encriptación de información, borrado de datos, virus y correos maliciosos, siendo estos un foco de infección a los sistemas de información y datos sensibles, de la misma forma se pudo constatar que ciberdelincuentes atentan principalmente vía email como medio de intromisión.
- Mediante la ejecución de un examen especial forense realizado a la empresa Calzacuba Cía. Ltda. se pudo identificar que sus sistemas de seguridad son poco confiables y vulnerables a ataques informáticos, debido a que la empresa no posee un firewall adecuado, lo cual es de vital importancia para un control eficiente en torno a la protección de la información de la empresa.
- Se determina que existe una tendencia al alza con respecto a fraudes informáticos en las pequeñas y medianas empresas del sector industrial, debido a que no se invierte lo suficiente en la gestión de herramientas de TI, para satisfacer las necesidades de la empresa de manera integral con un método de evaluación integrado tanto individual como colectivamente acorde a las necesidades de la organización que ayuden en el respaldo de la información y protección de datos.
- Una vez finalizada la investigación a las empresas del sector industrial se pudo concluir que la mayoría no poseen un manual o guía de buenas

prácticas con referente al manejo de las equipos de seguridad y protección de datos de información, con el propósito de facilitar el uso de herramientas de seguridad que permitan adoptar una buena gestión de riesgos de TIC.

RECOMENDACIONES

- Realizar más inversión en medios de protección de datos, aplicaciones y parches de seguridad con la finalidad de proteger intromisiones a los sistemas de información y comunicación de cada una de las áreas y departamentos; muy independiente de su actividad, logrando satisfacer las necesidades de ambas partes como son los trabajadores y los clientes creando un clima organizacional confiable.
- Estructurar planes estratégicos de TI acorde a los requerimientos del negocio de acuerdo al tamaño y a la actividad que se dediquen, ejecutando una buena gestión en la adopción de recursos de TI, lo cual permite a la organización ofrecer productos de calidad que satisfagan las necesidades de un mercado globalizado.
- A la comunidad científica, se propone ampliar los estudios de investigación sobre fraudes, delitos informáticos y vulnerabilidades que se presentan actualmente en las organizaciones públicas, privadas y mixtas, proponer políticas públicas que permitan tomar acciones preventivas y contribuir al desarrollo de las actividades empresariales, dado al elevado crecimiento de ataques cibernéticos en el mundo entero.
- En el diagnóstico realizado se pudo constatar que la mayoría de las empresas del sector industrial desconocen la terminología de la problemática en delitos informáticos y cibernéticos, por lo cual se recomienda a la Universidad de las Fuerzas Armadas ESPE conjuntamente con los administradores y personal encargado de seguridad de TIC, fomentar la vinculación a través de campañas o talleres de concientización en materia de seguridad informática, creando una cultura tecnológica empresarial, previniendo posibles intromisiones y la detección de intrusos.

- Realizar revisiones periódicas a sus equipos, sistemas de protección de datos de información, disponer de un antivirus que realice chequeos de las aplicaciones instaladas en los equipos informáticos y establecer una política de contraseñas seguras, por medio de métodos de autenticación fuertes a través de cifrados adicionales para poder acceder a la información, evitando la fuga y la encriptación de la misma.
- Las empresas del sector industrial deben utilizar una aplicación de constatación de correos electrónicos donde se identifique cuáles son los de naturaleza propia de la empresa, detectando y desechando correos maliciosos que con el simple hecho de ser abiertos se pueden crear medios de acceso e intromisión, vulnerando e inhabilitando los programas de las entidades, provocando la suspensión de las actividades y generando la perdida de grandes montos de dinero o cobros para la devolución de los sistemas encriptados, implicando un alto riesgo de recuperación de la información que es vital para el funcionamiento de las organizaciones.
- A los administradores, contratar cualquier tipo de mecanismo en seguridad de los sistemas de protección de información, como son firewalls o cortafuegos de manera continua, ya que ayudarán a mantener a los ciberdelincuentes alejados de la información, prevenir ataques externos en las redes locales, todo esto dependiendo del volumen de operaciones y su actividad industrial.
- Se recomienda la adopción de la guía de buenas de prácticas en Tecnología de Información y Comunicación propuesta por los investigadores del proyecto, ya que al hacer uso de este instrumento ayudará en gran medida y de manera íntegra a la gestión de tecnologías, implementación de herramientas de seguridad informática, mitigación de riesgos cibernéticos y fraudes informáticos.

REFERENCIAS BIBLIOGRÁFICAS

Accountants, I. F. (2008). *Auditoría Financiera de Pymes.* Bogota: Ecoe Ediciones.

Arens, A., & Loebbecke, J. (1996). *Auditoría un Enfoque Integral* (Sexta ed.). Mexico: Pearson Educacion.

Arens, A., Elder, R., & Beasley, M. (2007). *Auditoría,Un enfoque integral* (Decimo Primera ed.). Mexico, DF, Mexico: Pearson Educacion.

Auditool. (04 de 2011). *Auditool*. Obtenido de Red Global de Conociemientos en Auditoría y Control Interno: https://www.auditool.org/blog/auditoría-externa/866-auditor-forense

Auditores & Gerentes. Contadores Publicos Ltda. (2017). *ContabilidadParaTodos.com.* Recuperado el 05 de 05 de 2017, de http://contabilidadparatodos.com/libro-auditoría-y-normas-internacionales/

Badillo, J. (2008). *Auditoría Forense/ Mas que una especialidad profesional una mision: prevenir y detectar el fraude financiero.* Quito.

Baena, G. P. (2014). *Metodologia de la Investigaciòn.* Mexico: Grupo Editorial Patria.

Ballester, M. (sf). *IsacaMTY.* Obtenido de IsacaMTY: http://www.isacamty.org.mx/archivo/Standard_ISO38500.pdf

Batthyány, K., & Cabrera, M. (2011). *Metodología de la Investigacion en Ciencias Sociales.* Montevideo.

Beas, A. (1993). *Organización y Administración de Empresas.* Madrid España: McGraw-Hill.

Benavides, I; Acosta, Carla,. (s.f.).

Bermejo, R. (2005). *La gran Transición hacia la Sostenibilidad.* Recuperado el 19 de Abril de 2017, de La gran Transición hacia la Sostenibilidad:

https://books.google.es/books?hl=es&lr=&id=f7KLkWtFy74C&oi=fnd&pg=PA15&dq=econom%C3%ADa+sostenible&ots=fA3-1Jhwri&sig=oGUDF9cm12BwApRTBLUlZW_vntA#v=onepage&q=econom%C3%ADa%20sostenible&f=false

Bernal, C. (2010). *Metodologia de la Investigación.* Bogota: Pearson.

Betancourt, V. (Abril de 2004). *La Cumbre mundial sobre la sociedad de la Informacion.* Obtenido de https://www.apc.org/sites/default/files/wsis_process_ES.pdf

Bonilla, E., Hurtado, J., & Jaramillo, C. (2009). *La Investigación (Aproximaciones a la construcción del conocimiento Científico).* Bogota: Alfaomega.

Canaves, I. (24 de 04 de 2002). *Gestiopolis.* Obtenido de https://www.gestiopolis.com/auditoría-informatica/#pf8

Cano, M., & Lugo, D. (2008). *Auditoría Financiera Forense.* Bogota: Ecoe.

Cardona,D. (2010). *Evaluacion de la amenaza, la vulnerabilidad y el Riesgo.* Ecuador.

Chungata, A. (Marzo de 2015). *Repositorio Digital de la Universidad de Cuenca.* Obtenido de Repositorio Digital de la Universidad de Cuenca: http://dspace.ucuenca.edu.ec/bitstream/123456789/21321/1/TESIS.pdf

COBIT. (2007). Recursos de TI. *GOVERNACE INSTITUTE*, 209.

COIP, M. d.-S. (2014). *Codigo Organico Integral Penal.* Quito: Ayerve C.A.

Contraloria General del Estado. (2016). *Contraloria General del Estado*. Obtenido de Contraloria General del Estado: http://www.contraloria.gob.ec/Informativo/NuestrosServicios

Del Aguila, A., Padilla, A., Serarols, C., & Veciana, J. (15 de 10 de 2001). *Revista ICE.* Recuperado el 27 de Abril de 2017, de Revista ICE: http://www.revistasice.info/cachepdf/BICE_2705_07-24__0540D1E3A161DBFDD6A4B2982CC756BD.pdf

Deloitte. (2015). *DELOITTE.* Obtenido de DELOITTE: https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/COSO-Sesion1.pdf

Diario El Telégrafo. (16 de Agosto de 2016). *Diario El Telégrafo*. Obtenido de Diario El Telégrafo: http://www.eltelegrafo.com.ec/noticias/judicial/13/en-ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario

Díaz, M., Escalona, M., Ricalde, D., León, A., & Ramírez, M. (2015). *Metodología de Investigación.* Mexico: Trillas.

Díaz, Martha; Escalona,Maria; Ricalde, Diana; León, Alejandra & Ramírez, Marissa (2015) en su libo de . (2015). *Metodología de Investigación.* Mexico: Trillas.

Díaz, N., García, Y., Hernández, M., Ruiz, M., Santana, D., & Verona, M. (2009). *Finanzas Corporativas en la Práctica.* Madrid España: Garcia Tome.

Echenique, J. (2001). *Auditoría en Informatica.* Mexico: Interamericana Mc Graw Hill.

ECUCERT. (2017). *Centro de respuesta a incidentes informáticos en el Ecuador*. Recuperado el 19 de 05 de 2017, de Centro de respuesta a incidentes informáticos en el Ecuador: https://www.ecucert.gob.ec/incidente.html

El Comercio. (24 de 07 de 2015). *El Comercio.* Recuperado el 05 de 10 de 2017, de El Comercio: http://www.elcomercio.com/actualidad/cibermafias-ciberataque-17empresas-ecuador-seguridadinformatica.html

El Telégrafo. (16 de 08 de 2016). *El Telégrafo*. Recuperado el 05 de 10 de 2017, de El Telégrafo: http://www.eltelegrafo.com.ec/noticias/judicial/13/en-ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario

Estupiñan, R. (2006). *Control Interno y Fraudes.* Bogota Colombia: Eco Ediciones.

Fassio, A., Pascual, L., & Suarez, F. (2006). *Introducción a la Metodología de la Investigación.* Buenos Aires: Macchi.

FLACSO. (08 de 2013). *Ministerio de Industrias y Productividad.* Obtenido de Ministerio de Industrias y Productividad: http://www.industrias.gob.ec/wp-content/uploads/downloads/2013/08/ESTUDIOS_INDUSTRIALES_MIPYMES.pdf

Frett, N. (24 de Septiembre de 2014). *Auditool*. Obtenido de https://auditool.org/blog/fraude/2981-14-tipos-de-fraudes

García, V. (2014). *Introduccion a las Finazas.* Mexico: Callejas Javier Enrique.

Gómez, A. (2011). *Enciclopedia de la Seguridad Informática.* Mexico: S.A.

Guerrero. (2012). *Fraude en la Red.* Bogota: Ediciones de la U.

Guerrero, D. (2012). *Fraude en la Red.* Bogota: Ediciones de la U.

Gutiérrez, L. (1991). *Fraude Informático y Estafa.* Bogota.

Hernández, R., Fernández, C., & Baptista, P. (2006). *Metodología de la Investigación.* Mexico: Graw Hill.

Hurtado de Barrera, J. (2000). *Metodología de Investigación Holística.* Caracas: Funadacion Sypal.

Infovia.Ar. (24 de 04 de 2002). *GestioPolis*. Recuperado el 2017 de 05 de 11, de GestioPolis: https://www.gestiopolis.com/auditoría-informatica/

ISACA. (2007). *ISACA.* Obtenido de ISACA: http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT_4.1.pdf?regnum=405605

Joven Club de Computacion. (2010). *EcuRed- Conocimiento con todos y para todos*. Obtenido de https://www.ecured.cu/Auditoría_Inform%C3%A1tica

Kotler, P. (2010). *Dirección de Mercadotecnia.* Espana: Prentice Hall.

La Hora. (11 de 08 de 2011). *La Hora.* Recuperado el 05 de 10 de 2017, de La Hora: https://lahora.com.ec/noticia/1101191943/se-disparan-los-delitos-informc3a1ticos-

Laudon, K., & Laudon, J. (1996). *Administración de los Sistemas de Información.* New York: Pearson.

Leiva, F. (2002). *Nociones de Metodología de Investigacion Cientifia.* Quito: Grupo Leer.

Lugo, Danilo; Cano, Donaliza,. (2008). *Auditoría Financiera Forense.* Bogota: Ecoe-ediciones.

Mantilla, A., & Cante, S. (2005). *Auditoría de Control Interno.* Bogota: Ecoe Ediciones.

Mantilla, S. (2005). *Control Interno Informe COSO* (Cuarta ed.). Bogota, Colombia : Eco Ediciones.

Méndez, J. (2011). *Economía de la Empresa.* Santa Fe de Mexico: Mc. Graw Hill.

Miller, R. (2002). *Economía Hoy.* Bogota: Pearson.

Ministerio de Coordinacion de la Produccion, Empleo y Competitividad. (Mayo de 2011). *Ministerio de Coordinacion de la Produccion, Empleo y Competitividad.* Obtenido de Ministerio de Coordinacion de la Produccion, Empleo y Competitividad: https://es.scribd.com/document/245008250/Agenda-Territorial-Cotopaxi

Ministerio de Telecomunicaciones y Sociedad de la Informacion. (2015). *MINTEL*. Obtenido de MINTEL: https://www.telecomunicaciones.gob.ec/ecuador-cuenta-con-una-propuesta-de-plan-estrategico-de-investigacion-desarrollo-e-innovacion-de-las-tic/

Ministerio de Telecomunicaciones y Sociedad de la Informacion. (sf). *MINTEL*. Obtenido de MINTEL: https://www.telecomunicaciones.gob.ec/ecuador-cuenta-con-una-

propuesta-de-plan-estrategico-de-investigacion-desarrollo-e-innovacion-de-las-tic/

Moran, S. (24 de Julio de 2017). *Revista Digital PLAN V*. Obtenido de Revista Digital PLAN V: http://www.planv.com.ec/historias/politica/ecuador-el-mapa-mundial-tropas-ciberneticas

Moreno, A. (2000). *Metodos de Investigacion y Exposicion: para el trabajo de acdemicos y estudiantes.* Quito: Corporacion Editora Nacional.

Naranjo Marcelo, Naranjo Joselito. (2000). *Contabilidad Comercial y de Servicios.* Quito, Ecuador.

Naranjo, M., & Naranjo, J. (2000). *Contabilidad Comercial y de Servicios.* Quito Ecuador: Imprenta Don Bosco.

Nicuesa, M. (5 de Abril de 2016). *Empresariados*. Recuperado el 19 de Abril de 2017, de Empresariados: https://empresariados.com/cuatro-tipos-de-empresa-segun-su-tamano/

Observatorio de Delitos Informaticos de Latinoamèrica (ODILA). (2016). *Observatorio de Delitos Informaticos de Latinoamèrica.* Obtenido de Observatorio de Delitos Informaticos de Latinoamèrica: https://www.odila.org/pdf/Informe_ODILA_2016.pdf

Observatorio Iberamericano de Protección de Datos. (6 de 03 de 2013). *Delitos informáticos y comercio electrónico en Ecuador.* Recuperado el 09 de 10 de 2017, de Delitos informáticos y comercio electrónico en Ecuador: http://oiprodat.com/2013/03/06/delitos-informaticos-y-comercio-electronico-ecuador/

Organizacion de las Naciones Unidas. (sf). *Naciones Unidas.* Obtenido de Naciones Unidas: http://www.un.org/sustainabledevelopment/es/la-agenda-de-desarrollo-sostenible/

Ortiz, J. (2013). *Principios de estadística aplicada.* Bogota: Ediciones de la U.

Pallerola, J., & Monfort, E. (2013). *Auditoría, Enfoque Teorico - Pràctico.* Bogota: Ediciones de la U.

Paradinas, J. (sf). *Fundacion Canaria Orotava de Historia de la Ciencia.* Obtenido de Fundacion Canaria Orotava de Historia de la Ciencia: http://profesorjoserojas.weebly.com/uploads/4/2/3/5/42358921/fundamentos_de_la_econom%C3%8Da_pol%C3%8Dtica_de_a_smith.pdf

Piattini, M. (2001). *Auditoría Informatica Un enfoque practico.* Madrid: Alfaomega.

Pilmayquen, I. (2013). *Pensamiento Penal.* Obtenido de Pensamiento Penal: http://www.pensamientopenal.com.ar/system/files/2015/03/doctrina40720.pdf

Plan Nacional del Buen Vivir. (2013). *Plan Nacional del Buen Vivir.* Obtenido de Plan Nacional del Buen Vivir: http://www.buenvivir.gob.ec/objetivo-11.-asegurar-la-soberania-y-eficiencia-de-los-sectores-estrategicos-para-la-transformacion-industrial-y-tecnologica#tabs1

Quezada, N. (2010). *Metodologia de la Investigacion.* Lima-Peru: Macro E.I.R.L.

Santillana, J. R. (2004). *Auditoría Fundamentos .* Mexico: Thompson .

Scheel, C. (2011). *Las TICs un Nuevo Modelo de Negocios.* Distrito Federal de Mexico: Camara Nacional de la Industria.

Superintencia de Compañias, Valores y Seguros. (2015). *Superintencia de Compañias, Valores y Seguros*. Obtenido de Superintencia de Compañias, Valores y Seguros: http://appscvs.supercias.gob.ec/portalInformacion/sector_societario.zul

Superintendencia de Compañias y Valores. (20 de Mayo de 2014). *Bolsa de Valores Quito.* Obtenido de Bolsa de Valores Quito: http://www.bolsadequito.info/uploads/normativa/normativa-relacionada/ley-de-companias/141027193407-b61798b4923c4f24dff12632e81c7ef5_leycompanias.pdf

Temperini, M. (2013). *CONICET*. Recuperado el 2017 de 03 de 01, de CONICET: http://conaiisi.unsl.edu.ar/2013/82-553-1-DR.pdf

Terán, D. (2014). *Administración Estratégica de la Función Informática.* Mexico: Alfaomega.

Thompson, I. (2012). *PromonegocioS.net*. Recuperado el 19 de Abril de 2017, de PromonegocioS.net: https://www.promonegocios.net/mercadotecnia/empresa-definicion-concepto.html

Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation. (24 de 07 de 2017). *Politicas Historias.* Recuperado el 09 de 10 de 2017, de Politicas Historias: http://www.planv.com.ec/historias/politica/ecuador-el-mapa-mundial-tropas-ciberneticas

ANEXOS

DEPARTAMENTO DE CIENCIAS ECONÓMICAS, ADMINISTRATIVAS Y DEL COMERCIO

CARRERA DE INGENIERÍA EN FINANZAS Y AUDITORÍA

CERTIFICACIÓN

Se certifica que el presente trabajo fue desarrollado por el Sr. Diego Fernando Pinsha Defaz y el Sr. Kleber Gonzalo Quevedo Zambonino en la cuidad de Latacunga a los 07 días del mes de diciembre del 2017.

Ing. Luis Alfonso Lema Cerda

DIRECTOR

Aprobado por:

Ing. Julio César Tapia León

DIRECTOR DE LA CARRERA

Dr. Juan Carlos Díaz Álvarez

SECRETARIO ACADÉMICO