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 DE SERVICIOS REGULADAS POR LA SUPERINTENDENCIA DE COMPAÑÍA EN LA PROVINCIA DE COTOPAXI"

AUTORES:

ROSERO CHAVES, ÁNGEL ALEJANDRO

VALVERDE SOTO, ERICA MARIBEL

DIRECTOR ING. LEMA CERDA, LUIS

LATACUNGA

2018

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

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 SERVICIOS REGULADAS POR LA SUPERINTENDENCIA DE COMPAÑIAS EN LA PROVINCIA DE COTOPAXI",** realizado por el señor **ANGEL ALEJANDRO ROSERO CHAVES** y la señorita **ERICA MARIBEL VALVERDE SOTO,** 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 al señor **ANGEL ALEJANDRO ROSERO CHAVES** y la señorita **ERICA MARIBEL VALVERDE SOTO** para que lo sustente públicamente.

Latacunga, Agosto de 2018

Ing. Luis Alfonso Lema Cerda
DIRECTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS ECONÓMICAS, ADMINISTRATIVAS Y DEL COMERCIO

CARRERA DE INGENIERA EN FINANZAS Y AUDITORÍA

AUTORÍA DE RESPONSABILIDAD

Nosotros, **ANGEL ALEJANDRO ROSERO CHAVES,** con cedula de identidad Nº050343629-7 y **ERICA MARIBEL VALVERDE SOTO,** con cedula de identidad Nº 050357927-8 declaramos que el presente trabajo de investigación titulado **"FRAUDE INFORMÁTICO, ANÁLISIS DE VULNERABILIDAD EN LAS EMPRESAS DEL SECTOR SERVICIOS REGULADAS POR LA SUPERINTENDENCIA DE COMPAÑIAS EN 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 ello nos declaramos responsables del contenido, veracidad y alcance de investigación mencionada.

Latacunga, Agosto de 2018

ANGEL ALEJANDRO
ROSERO CHAVES
C.C.: 050343629-7

ERICA MARIBEL
VALVERDE SOTO
C.C.:050357927-8

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, **ANGEL ALEJANDRO ROSERO CHAVES, Y ERICA MARIBEL VALVERDE SOTO,** 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 SERVICIOS REGULADAS POR LA SUPERINTENDENCIA DE COMPAÑIAS EN LA PROVINCIA DE COTOPAXI",** cuyo contenido, ideas y criterios son de nuestra autoría y responsabilidad.

Latacunga, Agosto de 2018

ANGEL ALEJANDRO
ROSERO CHAVES
C.C.: 050343629-7

ERICA MARIBEL
VALVERDE SOTO
C.C.:050357927-8

DEDICATORIA

La educación es el arma más poderosa que puedes usar para cambiar el mundo.

Nelson Mandela.

Agradezco primero a Dios todo poderoso por darme la oportunidad de venir a este mundo y mantenerme día a día con mi hermosa familia, cuidarme y protegerme en cada momento y guiarme por el camino del bien gracias Dios mío.

A mi Madre

A la persona más importante en mi vida la que me dio la oportunidad de venir a este mundo a ese ser querido que me enseñó a vivir desde que estaba en su vientre, la que siempre me cuido, me protegió y la que está conmigo en los buenos y malos momentos todo se lo debo a mi hermosa madre, gracias al esfuerzo de ella logre terminar mi carrera como Ing. Finanzas y Auditoria, esto se lo dedico a mi AMADA MADRE TE AMO MADRE MIO.

A mis Hermanos

Les agradezco por todo el apoyo que me brindaron a los largo de mi carrera universitaria, y decirles que son lo más importante para mí siempre estaremos unidos hermanos.

Y a todas las personas que estuvieron apoyándome día a día muchas gracias.

Ángel A. Rosero Ch.

DEDICATORIA

A Dios.

Por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

A mi padre Manuel.

Por los ejemplos de perseverancia y constancia que lo caracterizan y que me ha infundado siempre, por el valor mostrado para salir adelante y por su amor.

A mi madre Mirian.

Por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.

A mis hermanos Cristhian, David.

Por lo que representan para mí y por ser parte importante de una hermosa familia unida.

Erica Maribel Valverde S.

AGRADECIMIENTO

Primeramente agradecer a Dios por haber permitido vivir hasta este día, haberme guiado a lo largo de mi vida, por ser mi apoyo, mi luz y mi camino. Por haberme dado la fortaleza para seguir adelante en aquellos momentos de debilidad y por brindarme una vida llena de aprendizajes y sobre todo de felicidad.

Al macro proyecto de investigación "Tecnologías de Información y Comunicación: Impacto en la Economía de las empresas en la provincia de Cotopaxi" aprobado por el Consejo de Departamento de Ciencias Económicas Administrativas y de Comercio mediante resolución Nº003-2017-ESPE-DECEAC efectuado el 28 de marzo de 2017, que fue la base para iniciar con el trabajo de investigación, aportando finalmente un gran instrumento para el sector de estudio.

A mi compañero de tesis: Ángel Rosero Chaves, por su confianza, apoyo, por haber formado un equipo de trabajo compartiendo conocimientos y valores como la amistad, la perseverancia, la humildad, por haberme tenido la paciencia necesaria y motivarme a seguir adelante en este proceso para poder concluir de manera satisfactoria con este sueño.

Mi agradecimiento infinito a mi Director de Tesis Ing. Luis Lema Cerna por la confianza que deposito en mí, su constante apoyo, sus indicaciones y orientaciones indispensables en el desarrollo de este trabajo. Quisiera destacar la seriedad profesional que le caracteriza.

Agradezco a mi querida y prestigiosa institución que me dio la oportunidad de formarme como profesional Universidad de las Fuerzas Armadas "ESPE".

AGRADECIMIENTO

Primero agradecer a Dios todo poderoso que nos cuida, protege y nos da su bendición para tenernos con vida día a día, por la salud que nos brinda y darnos la oportunidad de seguir en pie a lo largo de nuestro camino con todos los objetivos que tenemos en mente cumplir GRACIAS DIOS MIO por no dejarnos caer y apoyándonos y entregándonos fuerzas y ganas de seguir adelante, y por toda la felicidad que nos permites tener.

Al macro proyecto de investigación "Tecnologías de Información y Comunicación: Impacto en la Economía de las empresas en la provincia de Cotopaxi" aprobado por el Consejo de Departamento de Ciencias Económicas Administrativas y de Comercio mediante resolución N°003-2017-ESPE-DECEAC efectuado el 28 de marzo de 2017, que fue la base para iniciar con el trabajo de investigación, aportando finalmente un gran instrumento para el sector de estudio.

A mi compañera de investigación Erica V. te agradezco por ser una persona humilde, sencilla y comprensiva en todo el camino universitario y al final ser una compañera que me brindo apoyo a no dejarnos vencer en los momentos buenos y malos que supimos llevar juntos salir adelante y poder concluir con nuestra investigación, te deseo muchos éxitos a lo largo de tu vida profesional.

Mi agradecimiento a la prestigiosa Universidad de las Fuerzas Armadas ESPE, con la que empecé formándome como profesional gracias a sus docentes de excelente calidad que aportaron sus enseñanzas que me servirán de mucho a lo largo de mi vida laboral a toda la familia ESPE muchas gracias.

Mi agradecimiento al Director de Tesis Ing. Luis Alfonso Lema Cerda que fue mi docente desde que inicie la Universidad, por permitirme desarrollar y ser parte de su macro proyecto, y guiarme

a lo largo de mi investigación gracias por su tiempo que compartió con nosotros y su excelente profesionalidad como persona y docente.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente proyecto de investigación está encaminado a realizar un análisis de fraude informático y la vulnerabilidad de las empresas del sector servicios reguladas por la Superintendencia de Compañías y la Superintendencia de Economía Popular y Solidaria (SEPS) de la provincia de Cotopaxi durante el periodo 2012-2016.

En este trabajo se efectuó una investigación exploratoria de datos de las empresas del sector servicios de la provincia de Cotopaxi, 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, la utilización de la metodología a utilizar es de campo, descriptiva y exploratoria, cualitativa y cuantitativa, la aplicación de control interno, aplicación de encuestas, realización de la auditoria informática, examen especial y análisis forense digital, para dar solución a los fraudes informáticos. Se detalla el análisis y evaluación de resultados de la investigación realizando la comprobación de hipótesis y la tendencia de los fraudes informáticos de las empresas de servicios. Y por último una guía de buenas prácticas para la protección y seguridad de la información en las empresas, finalizando con las conclusiones y recomendaciones orientadas a la investigación.

PALABRAS CLAVES

- **PROVINCIA DE COTOPAXI**
- **EMPRESAS DE SERVICIOS**
- **FRAUDE INFORMATICO**
- **SEGURIDAD INFORMÁTICA**
- **CONTROL INTERNO**

ABSTRACT

This research project is aimed at conducting an analysis of computer fraud and the vulnerability of companies in the services sector regulated by the Superintendency of companies and the Superintendency of Popular and Solidarity Economy (SEPS) of the Cotopaxi province during the period 2012-2016.

In this work an exploratory investigation of data of the companies of the services sector of the province was carried out, initiating with the problematic of the investigation and its evaluation of the systems of information and vulnerability that these can suffer, Contextualizing The variables of study, defining the theoretical basis with respect to the topic raised, the use of the methodology to use is field, descriptive and exploratory, qualitative and quantitative, the application of internal control, application of surveys, execution of the computer audit, special examination and digital forensic analysis, to give solution to the computer frauds. It details the analysis and evaluation of the results of the investigation performing the test of hypothesis and the trend of computer frauds of service companies. And finally, a guide to good practices for the protection and security of information in companies, ending with research-oriented conclusions and recommendations.

KEY WORDS

- **COTOPAXI PROVINCE**
- **SERVICE COMPANIES**
- **COMPUTER FRAUD**
- **COMPUTER SECURITY**
- **INTERNAL CONTROL**

CAPÍTULO I

PROBLEMA DE LA INVESTIGACIÓN

1.1. Tema de Investigación

Fraude Informático, análisis de vulnerabilidad en las empresas del sector de servicios reguladas por la Superintendencia de Compañías en 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 de servicios reguladas por la Superintendencia de Compañías y Superintendencia de Economía Popular y Solidaria en la Provincia de Cotopaxi.

1.2.3. Área de Influencia Indirecta.

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

1.3. Planteamiento del problema

1.3.1. Contextualización

a. Macro.

La globalización y los avances tecnológicos han revolucionado la forma de vida del ser humano. Con la aparición de la informática y en particular de las nuevas tecnologías

llámese internet, correo electrónico, celulares, redes sociales, etc., ha implantado no solo nuevas formas de realizar tareas cotidianas, sino que las “personas y organizaciones han quedado expuestas por las vulnerabilidades de los sistemas de intercomunicación y manejo de la información y por la falta de preparación y de cuidado en su uso, al progresivo y peligroso impacto de la ciberdelincuencia” manifiestan los autores (Ojeda Pérez Jorge Eliécer: Arias Flórez Miguel Eugenio, 2010)

La globalización es de suma importancia por lo que nos permite tener muchos beneficios en la cual tenemos un potencial tecnológico que nos sirve de mucho en nuestro tiempo ya que nos integra a una sociedad virtual en la que se puede interactuar de muchas formas a nivel mundial realizando negocios internacionales, conexiones entre países para el desarrollo de las necesidades que tiene el ser humano en diferentes partes del planeta. El internet es una herramienta necesaria en todo hogar ya que la misma nos perite tener un acceso directo para la conexión a cualquier destino que uno desea acceder como resultado positivo tenemos una tecnología de avance y algo negativo del acceso a internet es el mal uso que se le da al mismo, ya que se obtiene sin número de problemas como por ejemplo el fraude y delito informático.

En este sentido Fayad indica que:

> En un estudio realizado por la Unión Internacional de Telecomunicaciones (UIT), en el mundo existen alrededor de 3,000 millones de cibernautas (40% de la población mundial) con una tasa de crecimiento anual aproximada de 14%. Un estudio realizado por la firma de software Symantec señala que la cifra de víctimas es de aproximadamente 12 víctimas por segundo: 1 millón diarias y 378 millones al año. El reporte indica que las pérdidas económicas anuales oscilan entre los 375 y 575 mil millones de dólares. (Fayad Omar, 2015)

Presenta un riesgo el mal uso que se da al Internet ya que existen personas a nivel global que se dedican atentar contra los cibernautas y como resultado tenemos grandes pérdidas diarias como nos indican en el párrafo anterior por lo que estamos expuestos a ser víctimas.

A medida que se ha extendido el uso del internet, las herramientas de los ciberdelincuentes han ido evolucionando paralelamente al desarrollo tecnológico. Prueba de ello son los distintos ataques cibernéticos que ha sufrido, la banca electrónica, comercios electrónicos, empresas, personas, instituciones gubernamentales a través de la historia. Entre los casos más importantes reportados en los últimos años, tomando en cuenta la cantidad de dinero que se movió; así como la magnitud de la información, varios son los que llaman la atención, y se resumen en el siguiente cuadro:

Tabla 1

Principales delitos informáticos a nivel mundial.

Año	Empresa	Estrategia	Monto
1988	First National Bank	Acceso a los equipos informáticos y telefónicos Autor: Armand Devon Moore	70 Millones
1994	Citibank	Acceso a las cuentas de cientos de clientes y realizar transferencias electrónicas. Autor: Vladimir Levin	3,7 millones
1994	40 Compañías estadounidenses	Saqueo de tarjetas de crédito de alcance internacional. Autor: Maxim Kovalchuk,	Sustracción de sus bases de datos en línea más de un millón de números de tarjetas
2008	Empresas Norteamericanas	Utilización de técnicas de inyección SQL Autor: Albert González	Entre 130 y 170 millones 5
2006	Supermercados Schnucks	El sistema que procesa los pagos de 69 establecimientos fueron hackeados.	2,4 millones de datos de tarjetas.
2004	Microsoft y Symantec	Un grupo de delincuentes montaron un enorme botnet, tomando el control de miles de ordenadores iposteriormente se ejecutava el fraude en las maquinas o computadores.	1 millón de dólares al año.
1998	Agencias gubernamentales, militares y empresas de Estados Unidos, Japón y otros países	Robo de información Autores: Markus Hess, Karl Koch, Hans Huebne, Dirk Brezinski y Peter Carl	Sustracción de material diverso del Pentágono, NASA, Laboratorio Nacional de Los Álamos, CERN, ESA
2005	Paris Hilton	Acceso a la cuenta de Paris Hilton en los servidores de T-Mobile asociados a sus terminales Sidekick Autor: Cameron Lacroix	Robo de infomacíon pesonal. (agenda de contactos, videos,etc.)

CONTINÚA

2010	Google, Microsoft Internet Explorer	Robo de información protegida Autor:Chema Alonso	Robos de propiedad intelectual, obtención de acceso a cuentas de correo y un conflicto serio entre los del buscador, el gobierno de EE.UU y el de China.
2010	Académicas JSTOR	Robo de informaión protegido a través de las redes del MIT. Autor: Aaron Swartz	4 millones de documentos y aplicaciones bajo copyright del repositorio digital de publicaciones académicas JSTOR
2012	PlayStation Network	Ciberataque durante 3 dias Autor:Sebastián Bortnik	Sustracción de datos personales de 77 millones de usuarios.
2011-2012	Foxconn	Incautación de los servidores del fabricante tecnológico chino Foxconn. Autor: Swagg Security	1GB de datos (MasterCard, Farmers Ins., instituciones gubernamentales etc) repartidos por diferentes partes del globo.

Fuente: (El diario. es, 2013)

Desde décadas pasadas los delitos informáticos aparecen siendo así con el pasar de los años han ido evolucionando de forma impresionante que en los últimos años nos dejaron grandes pérdidas económicas.

Los robos informáticos tanto económicos y de información, expuestos son únicamente los más importantes de los publicados en diferentes fuentes. Lo que verdaderamente preocupa es que este tipo de delitos (robos) no solamente han sobrevivido hasta la actualidad, sino que ahora son mucho más masivos y sofisticados que los de hace años.

En este sentido, el Director de la multinacional de seguridad de la información Etek Manuel Bustos manifiesta que: “la industria en general, el sector gobierno y las Pyme son los menos preocupados por la seguridad de la información, porque requiere inversiones y normalmente no le dedican lo suficiente para lograr un nivel adecuado de seguridad” (Rincón Rodríguez, Ojeda Pérez, Arias Flórez, & Daza Martínez, 2010)

Como resultado de no tener un buen sistema de información seguro y no contar con inversión alguna las empresas que han sido victimas de delitos informáticos son las que no se preocupan de contar con un servicio de seguridad por lo que se convierten en vulnerables para ser atentados ante un delito.

Un factor critico en el impacto de los delitos informaticos en la sociedad en general; es la falta de una cultura informatica, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan orientar posibles respuestas, formas de prevención y el manejo de dichas situaciones.

b. Meso.

En el informe denominado “Ciberseguridad 2016” denominado ¿Estamos preparados en América Latina y el Caribe? Revela que:

> Cuatro de cada cinco países de la región no tienen estrategias de Ciberseguridad o planes de protección de infraestructura crítica. Dos de cada tres no cuentan con un centro de comando y control de seguridad cibernética. La gran mayoría de las fiscalías carece de capacidad para perseguir los delitos cibernéticos, entre otras carencias. (Banco Interamericano de Desarrollo, 2016)

La falta de importancia que tienen algunos países para enfrentar los diversos problemas que conllevan los delitos de información es un tema de mucha importancia para la empresa al momento de manejar una base de datos, porque al no contar con un manual, guía de buenas prácticas de esta manera estaremos disminuyendo la vulnerabilidad ante estos sucesos que presentan un problema para las organizaciones.

En este sentido el Secretario de la Organización de Estados Americanos (OEA) enfatizó que en la mayoría de los países de la región no han alcanzado madurez de las políticas de seguridad cibernética. En tanto a medida que América Latina y el Caribe se incorporan a la revolución digital, los riesgos de vulnerabilidad aumentan, considerando que hay países en América Latina que procesan el 100% de sus compras gubernamentales vía electrónica, donde ya no es solo computadoras interconectadas sino un universo de máquinas controlando virtualmente todo lo que usamos a diario. Las capacidades de sancionar este tipo de delitos a nivel de la región se muestran

desalentadores puesto que “el 81% de los países analizados poseen sanción penal para menos del 40% de este tipo de delitos. Los países con mayor nivel de regularización se encuentran Puerto Rico, República Dominicana y Costa Rico” (Temperini Marcelo, 2014)

En América Latina y el Caribe se convierten en vulnerables ya que todas sus operaciones en lo que concierne a adquisición por parte del Estado lo hacen a través de acceso mediante un computador que esta interconectado a una infinidad de máquinas, como resultado a este tipo de delitos cada región cuenta con su código penal y son sancionados de acuerdo a la Ley.

Tabla 2

Ranking de delitos informáticos menos sancionados penalmente en Latinoamérica.

Delitos Informátiicos	**%**
Espionaje Informático	86%
Captación o venta ilegítima de datos	86%
Suplantación de Identidad Digital	86%
Carding	81%
Violación a la Intimidad	71%
Grooming	67%
Hurto Informático	62%
Difusión de Malware	62%
Violación de Datos Personales	62%
Difucsión maliciosa de información	48%

Fuente: (Temperini Marcelo, 2014, pág. 137)

La mayoría de países cuentan con Leyes y Políticas para sancionar de acuerdo a lo que estipula la misma Ley, a diferencia de otros países que no cuentan con las mismas

Leyes y Políticas para cuando suceda este tipo de delitos, lo que se puede realzar es una reforma al código penal para sancionar cuando ocurran este tipo de hechos.

Por otro lado, también se analiza el nivel de sanción penal de los delitos informáticos por cada país de América Latina y el Caribe. De acuerdo a los resultados que se presentan en la siguiente tabla es de suma importancia que todos los países adopten políticas y actualización de normativas, que permitan mitigar las existencias de paraísos legales para la ciberdelincuencia.

Tabla 3

Estadísticas sobre el nivel de sanción penal de los delitos informáticos por país.

País	%
Bolivia	0%
Nicaragua	0%
Paraguay	0%
Perú	0%
Haití	9%
México	9%
Nicaragua	9%
Panamá	9%
Uruguay	9%
El Salvador	18%
Honduras	18%
Brasil	27%
Argentina	36%
Chile	36%
Colombia	36%
Ecuador	36%

CONTINÚA

Guatemala	36%
Venezuela	55%
Costa Rica	64%
República Dominicana	64%
Puerto Rico	91%

Fuente: (Temperini Marcelo, 2014, pág. 137)

En Latinoamérica, de acuerdo al estudio realizado por la Organización de Estados Americanos (OEA),

> México presentó un incremento entre el 8% y el 40% en ataques durante 2012, siendo este el mercado más problemático. Dicho aumento se generó en ciberataques y acciones "hacktivistas", lavado de dinero y ataques a infraestructuras críticas. Dicho aumento se generó en ciberataques y acciones "hacktivistas", lavado de dinero y ataques a infraestructuras críticas. El robo de la banca en línea ha sido ampliamente reportado en América Latina. Esta actividad presentó características distintivas entre los países, dependiendo del banco o país de destino y la naturaleza de las medidas de autenticación y seguridad que protegen los datos financieros. (Fayad Omar, 2015)

Sostiene que: "En el país, las pyme viven un proceso más lento en cuanto a la implementación de estrategias de seguridad; sin embargo, poco a poco, tanto los proveedores como esas empresas han buscado los mecanismos para solventar esta falta" (Ojeda Pérez Jorge Eliécer: Arias Flórez Miguel Eugenio, 2010)

Refiriéndonos al tema en su estudio de investigación intitulado El avance de las TIC en Latinoamérica en las actividades de la empresa menciona que en los últimos años; en "América Latina se han implementado diversas iniciativas para mejorar la medición de TIC en las empresas, pero estas se concentran esencialmente alrededor de datos básicos y aún es muy incipiente el debate sobre la construcción de nuevos indicadores para mejorar" (Vega Alfredo, 2013, pág. 17).

La incorporación de Tecnología de la Información y Comunicación (TIC) requiere complementariedades entre las inversiones en esas tecnologías y otras inversiones que produzcan cambios en las empresas y en su productividad. Estas inversiones comprenden el desarrollo de procesos, el cambio organizacional, la adquisición de mejores habilidades por parte de los ejecutivos y trabajadores, la obtención de soluciones digitales específicas y la modificación de métodos de trabajo, así como la producción de bienes y servicios para apoyar nuevos modelos de negocios.

c. Micro.

En Ecuador "según el estudio de Deloitte, el 54% de las firmas cuenta con una estrategia de ciberamenazas y seguridad de la información. De estas empresas, casi todas corresponden al sector bancario" (Revista Líderes, 2016). El mayor obstáculo según opinión de los empresarios que afrontan para implementar sistemas de seguridad es no contar con los recursos suficientes, este mismo estudio menciona que las organizaciones no han incrementado o directamente redujo el presupuesto destinado a ciberseguridad.

Convirtiendo a las PYMES en un segmento vulnerable cuando se trata de robos de información. Esto debido a que como se dijo anteriormente no cuenta con presupuestos o el equipo necesario para hacer frente a los retos de seguridad y de esta forma proteger la información.

De acuerdo a datos porporcionados por la Fiscalía General del Estado entre enero y mayo del 2016 se registraron los siguientes 530 delitos informáticos en el país.

Tabla 4

Delitos informáticos denunciados en Ecuador

Delito	Denuncias Enero-Mayo 2016
Apropiación fraudulenta por medios informáticos	160
Apropiación fraudulenta por medios electrónicos con inutilización de alarmas, descifrada de claves o encriptados.	318

CONTINÚA

Acceso no consentido a un sistema informático, teelmático o de telecomunicaciones.	30
Ataque a la integridad de sistemas informáticos	5
Transferencia electrónca del activo patrimonial	3
Intercepción ilegal de datos	2
Revelación ilegal de base de datos	4
Transferencia electrónoca del activo patrimonial. La persona que facilite o proporcione su cuenbta bancaria para recibir de forma ilegítima un activo	4
Ataque a la integridad de sistemas informáticos. Persona que diseñe, desarrolle, programe, adquiera, envíe, introduzac, ejecute, venda o distribuya dispositivos o programs informáticos maliciosos	2
Delitos contra la información pública reservada legalmente	2
TOTAL	530

Mediante informe (Fiscalía General del Estado, 2015) 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*. (El Telegrafo, 2016)

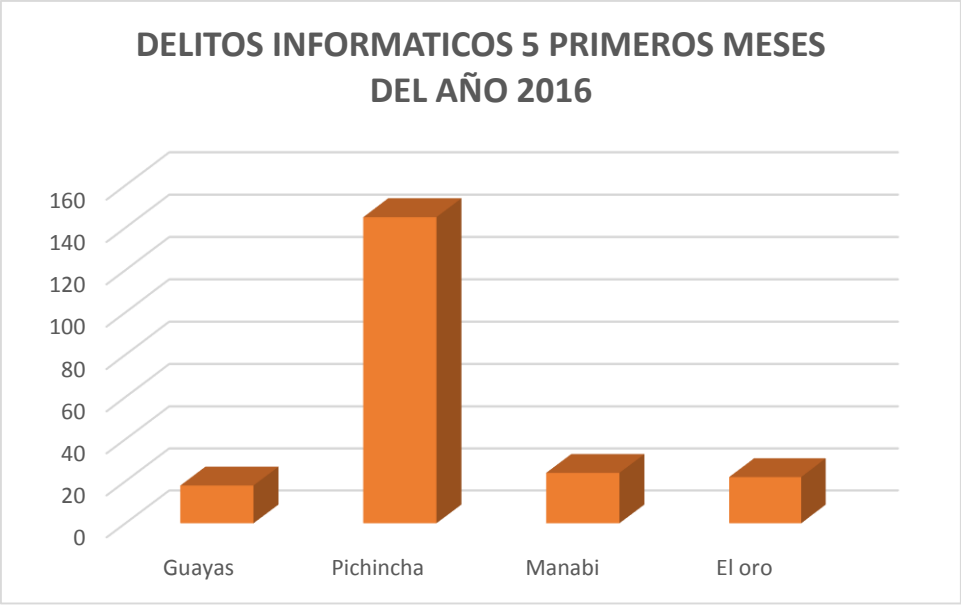


Figura 1. Delitos informáticos

Los delitos informáticos se encuentran tipificados en el Código Integral Penal (COIP), sin embargo expetos en la materia, sostienen que en “Ecuador existen dificultades dutrante la investigación de fraudes propiciados con el uso de tecnología, por cuanto la información cruzada a nivel de correos electrónicos o redes sociales no se encuentran dentro del país”. (Fiscalía General del Estado, 2015). Además los proveedores de sistemas informáticos como Facebook, Google, etc., y redes sociales tienen su banco de datos en Estados Unidos, frente a lo cual la situación se complica aún más.

Por tanto, es fundamental que se establezca medidas preventivas que permitan contrarrestar fraudes informáticos y reducir el nivel de vulnerabilidad a los que se encuentran expuestas entidades financieras, empresas o cualquier ciudadano común, puesto que inciden directamente sobre el crecimiento económico de un país. Se puede contemplar sus efectos sobre la inversión, el capital humano, el capital social, el comercio y finalmente, sobre la innovación y emprendimiento.

En lo que se refiere al uso de herramientas tecnológicas el (Ministerio de Telecomunicaciones y de la la Sociedad de la Información, 2014), revela que en “Ecuador

las microempresas, pequeñas y medianas empresas utilizan Tecnología de Información y Comunicación, ya sea para vender productos, servicios, facturar, realizar contactos mediante el correo electrónico o redes sociales como una manera de mejorar sus servicios y optimizar sus operaciones".

> Esta misma fuente destaca la proporción de empresas que utilizan TIC; de las cuales las microempresas alcanzan un 48,6%, las medianas empresas un 56,9% y las pequeñas empresas un 52,9%, dando un total general de 52,8%. (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2014). Además, se establece el indicador de proporción de empresas con presencia en la web con un total general de 27,4%, algunas MIPYMES por su naturaleza de productos perecibles no los promocionan mediante una página web, pero el estudio indica que el uso de Internet se ha incrementado lo que genera grandes oportunidades de crecimiento para Ecuador.

No obstante también ha provocado que el riesgo sea mucho mayor, debido a que es información sensible quede expuesta a los fraudes informáticos, y robo de datos financieros de las empresas, sino cuenta con medidas de protección adecuadas.

En la provincia de Cotopaxi el desconocimiento de la sociedad sobre el uso adecuado y mecanismos que permitan confrontar actos ilícitos utilizando medios tecnológicos, la falta de seguridad informática y la falta de control de privacidad de las páginas web, colocan en una situación de vulnerabilidad a las empresas. Las entidades financieras como bancos, cooperativas o cualquier tipo de institución que maneja dinero han tenido que infundir sus propios sistemas de seguridad informática para de esta forma evitar ser víctimas de este tipo de delito.

Considerando que la provincia de Cotopaxi el mayor generador de empleo y riqueza (después de Pichincha), compuesta por las PYMES, vendedores formales e informales, sin dejar de lado el aporte del sector agrícola, ganadero, y otros sectores. Se hace necesario en el caso específico y de abordaje de esta investigación, destacar la importancia que tiene adoptar medidas preventivas que permitan contrarrestar delitos informáticos en el marco de disminuir en gran manera los fraudes e implementar una cultura de seguridad.

d. Árbol de Problemas.

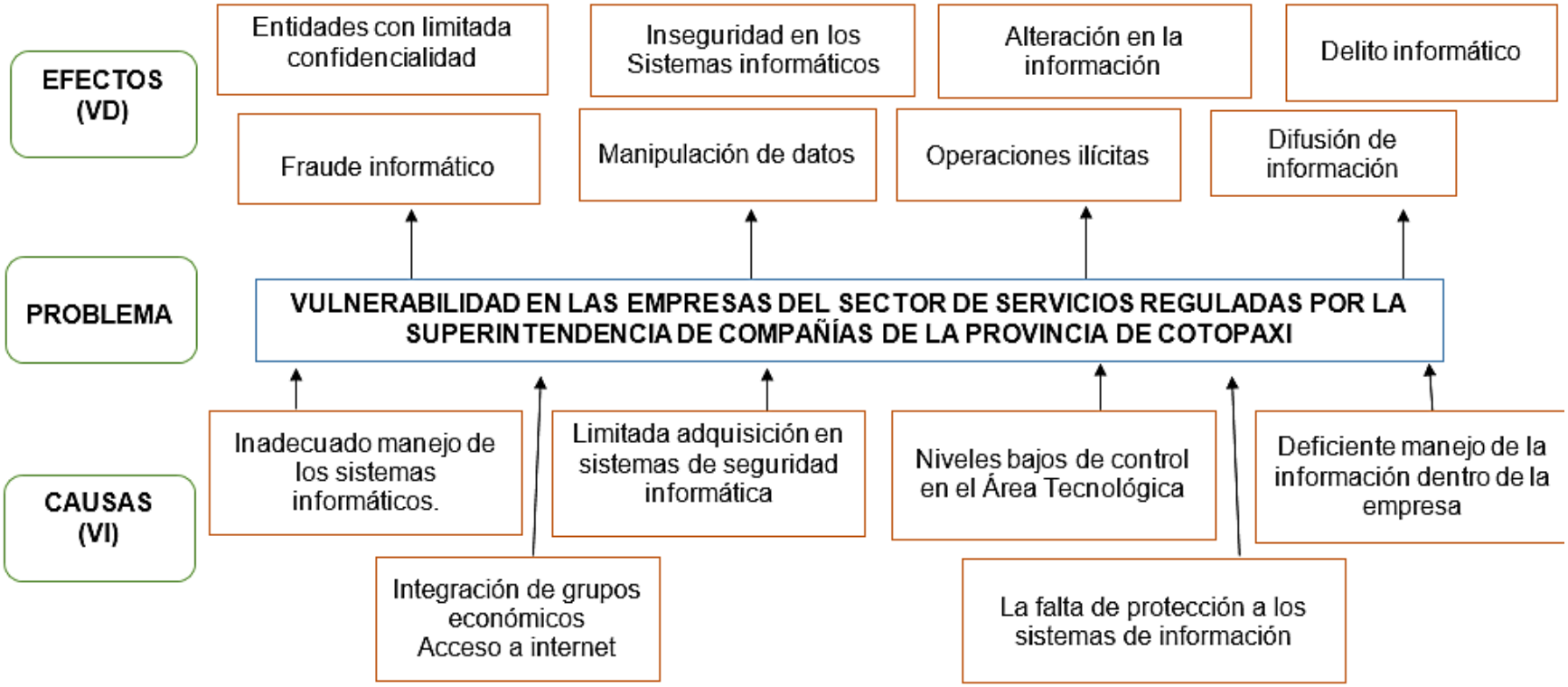


Figura 2. Relación Causa Efecto

e. Análisis Crítico.

En la actualidad nos vemos inmersos en un mundo altamente cambiante y competitivo el cual es cada vez más dependiente de las TIC para sus procesos comerciales, sociales y servicios de las empresas. La penetración universal de las mismas se debe fuertemente a la vulnerabilidad de los sistemas informáticos de las organizaciones, lo que ha repercutido en un aumento en el control de las TIC. En particular, las TIC han ayudado a democratizar el acceso a la información permitiendo que las empresas resguarden de una mejor manera sus datos, procesos y conozcan mejor a sus clientes, y mantengan mejores y más estrechas relaciones con sus empleados y socios estratégicos.

Las TIC han facilitado la interconexión e integración de mercados, creando nuevos canales de distribución y transformando profundamente la economía y la sociedad en general y, por ende, la manera en que los intercambios de bienes y servicios son realizados. Sin embargo al mismo tiempo que se ha desarrollado las tecnologías de la información y comunicación, evolucionando e innovando con nuevas herramientas que permiten adaptarse a un entorno y suplicar necesidades, como por ejemplo el uso de un sistema de manejo e información; estas mismas herramientas son utilizadas para acceder a un sistema sin autorización, alterar archivos, destruir y alterar datos entre otros.

Con el uso del internet se abrió paso a nuevas forma de delincuencia que vas desde transferencia ilícita de dinero, ataque a los sistemas de información, robo de información de las empresas, etc. La falta de una cultura de seguridad y los altos costos que supone adquirir, licencias de software de seguridad que pueden llegar a costar más de $10.000, montos que suelen sobrepasar el reducido presupuesto de las PYMES, que en sus primeros años de operaciones se procura priorizar otros costo, razón por la cual se convierten en un blanco fácil para los ciberdelincuentes.

1.4. Objetivos

1.4.1. Objetivo General.

Estudiar la vulnerabilidad de las empresas del sector servicios reguladas por la Superintendencia de Compañías y Superintendencia de Economía Popular y Solidaria mediante un examen especial con la finalidad de prevenir fraudes informáticos en la Provincia de Cotopaxi durante el periodo 2012 – 2016.

1.4.2. Objetivos Específicos.

- Analizar cada una de las variables de la investigación de acuerdo al tema planteado con la finalidad de obtener información necesaria para la ejecución del proyecto.
- Delimitar las bases teóricas bajo las cuales se sustenta la investigación en torno a vulnerabilidad de fraudes informáticos en las empresas de servicios reguladas por la Superintendencia de Compañías y Superintendencia de Economía Popular y Solidaria de la Provincia de Cotopaxi.
- Analizar qué tan vulnerables son las empresas del sector de servicios de intermediación financiera, reguladas por la Superintendencia de Compañías y Superintendencia de Economía Popular y Solidaria a los fraudes informáticos mediante encuestas realizadas a los representantes de cada organización.
- Estudiar los hallazgos más relevantes con la finalidad de elaborar un informe de auditoría, que sustente el trabajo realizado en las empresas de servicios reguladas por las Superintendencias de Compañías y la Superintendencia de Economía Popular y Solidaria en la Provincia de Cotopaxi.
- Construir una Guía de Buenas Prácticas con la finalidad de tener un control de Fraudes Informáticos en las empresas de servicios reguladas por la Superintendencia de Compañías y la Superintendencia de Economía Popular y Solidaria en la Provincia de Cotopaxi.

1.5. Justificación e Importancia

En la actualidad las empresas se hallan introducidas a negociaciones digitales de carácter global por lo tanto son vulnerables a las ciberamenazas, el delito mediante el uso de medios informáticos hoy en día es una de las preocupaciones primordiales de las entidades, los hackers se encuentran buscando las vulnerabilidades durante las 24 horas del día, es así que las amenazas pueden surgir tanto dentro como fuera de las compañías. Por lo tanto es recomendable implementar un gobierno de seguridad de la información dentro de la institución, esto significa detallar políticas procedimientos y un responsable encargado de enfrentar los riesgos.

Las empresas que tienen mayor amenaza a fraudes financieros son las de servicio, en este caso nos enfocamos a la intermediación financiera por lo que en nuestro país ya existen casos de robo, fraude informático que representan cifras muy altas a nivel nacional este tipo de delitos se han venido desarrollando desde años pasados y su impacto en la sociedad cada vez es más alto, por lo que se debe efectuar normas, políticas de seguridad al momento de manejar un paquete informático en las instituciones de intermediación financiera por lo que las mismas deben contar con software y profesionales en seguridad informática, de esta forma brindan garantías a los cuenta ahorristas evitando ser víctimas de delitos informáticos.

Hoy en día dentro de las organizaciones la seguridad Informática en las empresas generalmente es considerada como un gasto mas no como una inversión. Lo que se pretende es crear una cultura preventiva porque la seguridad de la información es uno de los activos más importantes para los directivos institucionales. Para la ejecución de este proyecto nos alinearemos a lo que nos establece el objetivo N° 11 del Plan Nacional del Buen Vivir, el mismo que asegura la soberanía eficiencia de los sectores estratégicos para la transformación industrial y tecnológica.

Según Kotler, Philip indica:

> Las empresas del sector de servicios brindan una gran cantidad de empleo, especialmente a las personas de la zona centro del país, por lo que es fundamental impulsar la inversión e implementación de sistemas informáticos 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. (Kotler, Philip, 2010)

Para nuestro estudio está considerada la política y lineamiento del literal 11.3 (Plan Nacional del Buen Vivir, Plan Nacional del Buen Vivir, 2013)

Política y Lineamiento

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 de la ciudadanía para el uso de las TIC, priorizando a las MIPYMES y a los actores de la economía popular y solidaria.
- 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.
- Fortalecer la seguridad integral usando las TIC.

Lo importante de esta investigación es analizar los fraudes informáticos y la vulnerabilidad de las empresas de servicios reguladas por la Superintendencia de Compañías y la Superintendencia de Economía Popular y Solidaria que normalmente son desarrolladas para engañar o perjudicar a una persona, con la finalidad de adquirir un beneficio propio, que conlleva a incurrir en un acto delictivo que puede estar o dentro de una sanción, por lo tanto para mitigar estos riesgos las empresas tendrán que realizar una adecuada capacitación del personal en el área de tecnologías de información que en la actualidad son muy necesarias ya que los cambios tecnológicos están a la orden del

día, lo que incita a las organizaciones estar a la vanguardia de las últimas herramientas con respecto a la protección y seguridad de la información.

Teniendo en cuenta los diferentes aspectos anteriormente mencionados, todas las empresas tienen la necesidad de implementar una solución de seguridad que contemple todas las protegidas.

Intermediación Financiera

Según indica Leiva

> Se entiende por intermediación financiera el servicio que se hace para contactar a los poseedores de los recursos financieros (dinero, bienes de capital, captación de recursos, etc.) con aquellas personas físicas o jurídicas que necesitan dicho recurso financieros (prestamos) para utilizarlos y generar utilidades. (Leiva, 2007, pág. 32)

Los servicios de intermediación financiera en nuestro país tienen un gran impacto en cuanto a bancos privados , públicos y cooperativas por lo tanto cumplen una función muy importante con los servicios financieros para la sociedad, ya que los mismos protegen y velan el interés de los cuenta ahorristas (persona que tiene una cuenta de ahorro). En la actualidad las instituciones financieras son de gran aporte para las personas por lo que brindan servicios de acuerdo a las necesidades de la sociedad para emprender sus propios negocios y así obtener en un determinado tiempo utilidades.

Según Sistema Financiero de Ecuador Define sistema financiero como:

> El conjunto de instituciones que tiene como objetivo canalizar el ahorro de las personas. Esta canalización de recursos permite el desarrollo de la actividad económica (producir y consumir) haciendo que los fondos lleguen desde las personas que tienen recursos monetarios excedentes hacia las personas que necesitan estos recursos. Los intermediarios financieros crediticios se encargan de captar depósitos del público y, por otro, prestarlo a los demandantes de recursos. (Sistema Financiero del Ecuador, s.f.)

Todas las instituciones financieros sean estas públicas o privadas su finalidad es contar con una excelente administración del recurso económico en el cual cuenta

ahorristas depositan sus excedentes y de esta formar prestar dinero a los que necesiten para satisfacer necesidades de los mismos.

1.6. Hipótesis

(H1) = Los fraudes informáticos inciden en los resultados financieros y de gestión de las empresas del sector de servicios reguladas por la Superintendencia de Compañías y la Superintendencia de Economía Popular y Solidaria en la Provincia de Cotopaxi.

(H0) = Los fraudes informáticos no inciden en los resultados financieros y de gestión de las empresas del sector de servicios reguladas por la Superintendencia de Compañías y la Superintendencia de Economía Popular y Solidaria en la Provincia de Cotopaxi.

1.7. Variables de Investigación

1.7.1. Variable Independiente.

- Fraude Informático

1.7.2. Variable Dependiente.

- Vulnerabilidad de las empresas del sector de servicios reguladas por la Superintendencia de Compañías y la Superintendencia de Economía Popular y Solidaria.

1.8. Operacionalización de las variables

Tabla 5

Matriz de Operacionalización de la variable independiente

CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	ITEMS BÁSICOS	TÉCNICAS E INSTRUMENTOS DE INFORMACIÓN
Fraude. - Actividad ilícita realizada por personas inescrupulosas que aprovechan la vulnerabilidad de algún sistema informático con el objeto de obtener beneficios.	Actividades Ilícitas	Manipular datos	¿Qué tipo de fraude es más común?	Encuestas
	Espionaje Informático	Hackers	Existen políticas de seguridad	Encuestas

Tabla 6

Matriz de Operacionalización de la variable dependiente

CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	ITEMS BÁSICOS	TÉCNICAS E INSTRUMENTOS DE INFORMACIÓN
	Vulnerabilidad	Base de datos. Sistema RRHH	¿Según su criterio cuál es el recurso de mayor vulnerabilidad en los sistemas informáticos?	Encuesta
	Sistemas Informáticos	Manipulación de sistemas informáticos.	¿Cree usted que los sistemas informáticos en la institución son seguros?	Encuesta

CONTINÚA

	Beneficios	Económicos Causar daño material. Causar daño moral.	¿Cuál cree usted sea la finalidad de los ciberdelincuentes al cometer fraudes informáticos?	Encuesta

CAPÍTULO II

MARCO TEÓRICO

2.1. Empresa

2.1.1. Definición.

> Indica que: Una empresa es una unidad económico-social, integrada por elementos humanos, materiales y técnicos, que tiene el objetivo de obtener utilidades a través de su participación en el mercado de bienes y servicios. Para esto, hace uso de los factores productivos (trabajo, tierra y capital). (Pérez Porto Julián, 2008)

Una empresa o entidad como nosotros lo llamemos su objetivo o fin brindar un servicio a la sociedad, con la ayuda del recurso humano material y técnico y como resultado de esto tendremos una utilidad o ganancia.

2.1.2. Actividad económica.

- Sector primario: Todos los recursos provienen de la naturaleza como son la agrícolas, pesqueras o ganaderas.
- Sector secundario: Su actividad principal es la transformación de bienes, como son las industriales y de la construcción.
- Sector terciario: son todas las empresas que su actividad principal de ofertar servicios y comercio.

2.1.3. Empresa de servicios.

Define a una “Empresa de Servicios aquella cuya actividad principal es ofrecer un servicio (intangible) con el objetivo de satisfacer necesidades colectivas, cumpliendo con su ejercicio económico (fines de lucro)”. (E General - Definista, 2008)

Toda empresa o entidad que brinda algún tipo de servicio está enfocada a satisfacer necesidades de la sociedad y como resultado de toda actividad económica tenemos una ganancia.

2.1.4. Tipos y características de empresas de servicios.

De acuerdo a (Villa Irene, 2017) indica lo siguiente:

- Empresas de actividades uniformes
  Son aquellas que mantienen estables los valores esenciales del negocio. Por ejemplo, los gastos en mano de obra, los costes de producción, las vías de ejecución del servicio y, sobre todo, la actividad en sí misma.
- Empresas de gestión de proyectos
  En este caso, además de prestar un servicio puntual y definido, se trata de empresas que desarrollan proyectos de duración media o corta, es decir, con unas actividades y fases definidas de antemano, como por ejemplo la programación web, la consultoría especializada o los procesos de selección de personal, entre otros.
- Empresas de servicios combinadas
  A esta última categoría pertenecen aquellas empresas que combinan la oferta de un servicio con la venta de productos. Es bastante habitual encontrarlas en sectores como la hostelería, los servicios de reparación del hogar o las funerarias, entre otros.

De acuerdo a la actividad de servicios que cada entidad maneja tienen un grado de diferencia una de otra por lo que se distinguen de acuerdo a lo que se dedica cada organización.

2.1.5. Clasificación de empresas de servicios.

(Beatriz, s.f.) Clasifica a las empresas de servicios de la siguiente manera:

- Servicios públicos varios: comunicaciones, energía, agua
- Servicios privados varios: servicios administrativos, contables, jurídicos, entre otros.
- Transporte: de personas o mercaderías.
- Turismo.

- Instituciones financieras.
- Educación.
- Salud.
- Finanzas y seguros.

2.1.6. Empresas de intermediación financiera.

> Según (Leiva, 2007, pág. 32) Se entiende por intermediación financiera el servicio que se hace para contactar a los poseedores de los recursos financieros (dinero, bienes de capital, captación de recursos, etc.) con aquellas personas físicas o jurídicas que necesitan dicho recurso financieros (prestamos) para utilizarlos y generar utilidades.

Los servicios de intermediación financiera en nuestro país tienen un gran impacto en cuanto a bancos privados, públicos y cooperativas por lo tanto cumplen una función muy importante con los servicios financieros para la sociedad, ya que los mismos protegen y velan el interés de los cuenta ahorristas (persona que tiene una cuenta de ahorro). En la actualidad las instituciones financieras son de gran aporte para las personas por lo que brindan servicios de acuerdo a las necesidades de la sociedad para emprender sus propios negocios y así obtener en un determinado tiempo utilidades.

Según Sistema F. de Ecuador Define sistema financiero como:

> El conjunto de instituciones que tiene como objetivo canalizar el ahorro de las personas. Esta canalización de recursos permite el desarrollo de la actividad económica (producir y consumir) haciendo que los fondos lleguen desde las personas que tienen recursos monetarios excedentes hacia las personas que necesitan estos recursos. Los intermediarios financieros crediticios se encargan de captar depósitos del público y, por otro, prestarlo a los demandantes de recursos. (Sistema Financiero del Ecuador, s.f.)

Todas las instituciones financieras sean estas públicas o privadas su finalidad es contar con una excelente administración del recurso económico en el cual cuenta

ahorristas depositan sus excedentes y de esta formar prestar dinero a los que necesiten para satisfacer necesidades de los mismos.

Según (Lema Cerda, Andaluz Victor, Pinsha, & Quevedo Kleber, 2017) De acuerdo a investigaciones realizadas sobre “Computer Fraud: Analysis of Vulnerability in Companies of the Industrial Sector“ dicho proyecto tiene como enfoque el análisis de fraude y vulnerabilidad de las computadoras en las empresas del sector industrial en la provincia de Cotopaxi, enfocándose a otro sector industrial en nuestra provincia que también se ha destacado como partícipe del desarrollo económico y social.

2.2. Auditoría

2.2.1. Definición, Alcance y Principios.

a. Definición.

Según (Arens, Randal, & Beasley, 2012, pág. 4) 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”.

Así también según la opinión de, Montilla & Herrera

“La auditoría es la verificación de estados financieros y de la contabilidad que los produce, para determinar si ellos representan fielmente la realidad económica de la empresa”. (Montilla Galvis & Herrera Marchena, 2006)

Con lo anterior podemos definir a la auditoría como un conjunto de procedimientos que es llevado que permite determinar la credibilidad de la información financiera de una entidad sobre la cual los usuarios puedan usarlo como base para la toma de decisiones.

> La auditoría es revisar que los hechos, fenómenos y operaciones se den en la forma en que fueron planteados, que las políticas y procedimientos establecidos se han observado y respetado. Es evaluar la forma en que se administra y opera para aprovechar al máximo los recursos. (Tapia Iturriaga, Guevara Rojas, Castillo Prieto, Rojas Tamayo, & Salomón Doroteo)

La auditoría permite realizar una evaluación en los diferentes procesos que se traza la organización y de esta manera se cumplan con todo, y así poder verificar si se están cumpliendo con todos los métodos fijados por la organización de esta manera analizar la administración y en qué nivel se aprovechan los recursos de la empresa.

b. Procedimiento de auditoría.

(Arens, Randal, & Beasley, 2012, pág. 162) La instrucción detallada para la recopilación de un tipo de evidencias de auditoria que se ha de obtener en cierto momento durante la auditoria.

Ejemplo:

- Obtener el diario de salida en efectivo y compararla el nombre de la persona que paga, el monto y la fecha del cheque cancelado con el diario de salidas de efectivo.

Para realizar la auditoría es necesario tener un plan a seguir para desarrollar de manera eficiente la misma de esta manera se utilizará como manual a seguir y no tener complicaciones.

c. Alcance.

El término alcance hace referencia a todos los procedimientos que engloba las auditorías indispensables para llevar a cabo los diferentes objetivos que se plantean, en otras palabras, el alcance son los procedimientos requeridos para ejecutar la auditoría.

Según (Rodriguez, s.f.) “Se debe especificar el alcance del área examinada, los aspectos a examinar, los funcionarios responsables y la comisión encargada de la auditoría administrativa”

2.3. Tipos de Auditoría

La auditoría a los estados financieros de una empresa esta sea pública o privada con su objetivo es conseguir una alta transparencia de acuerdo a lo financiero y económico de la organización. Existe otro tipo de auditoría que no necesariamente está relacionada con la contabilidad que lleva la organización que comprenden a la vez la evaluación de otras actividades como el desempeño, administración de los directivos, operaciones y cumplimiento de normas.

2.3.1. Auditoría Administrativa.

Para López la auditoría administrativa se define como:

"Un examen completo y constructivo de la estructura organizativa de una organización, empresa, institución o de cualquier otra entidad y de sus métodos de control, medios de operación y empleo que dé a sus recursos humanos y materiales". (López López, 2010)

Dicho de otra forma, la auditoría administrativa permite a la gerencia evaluar el nivel de desempeño que tiene la entidad con el objetivo de dictar o emitir recomendaciones que permitan mejorar la administración de la misma.

"Es la revisión analítica total o parcial de una organización con el propósito de precisar su nivel de desempeño y perfilar oportunidades de mejora para innovar valor y lograr una ventaja competitiva sustentable". (Enrique Bejamin, 2007, pág. 11)

La auditoría administrativa es de mucha importancia para las empresas, ya que por medio de esta rama se puede tener resultados para el bienestar, desarrollo y por medio de recomendaciones tengan mejores tomas de decisiones para un futuro.

a. Alcance de la auditoría Administrativa.

Se puede decir que la finalidad fundamental de la auditoría administrativa es encontrar, fijar todas las irregularidades o deficiencias que tiene la organización al momento de ser

examinada y de esta forma indicar, recomendar las posibles soluciones para mejorar las operaciones de la misma.

b. Objetivos de la Auditoría administrativa.

Según (Ecured, 2017) nos indica algunos objetivos de la auditoría administrativa tenemos los siguientes:

- **De control.-** Destinados a orientar los esfuerzos en su aplicación y poder evaluar el comportamiento organizacional en relación con estándares preestablecidos.
- **De productividad.-** Encauzan las acciones para optimizar el aprovechamiento de los recursos de acuerdo con la dinámica administrativa instituida por la organización.
- **De organización.-** Determinan que su curso apoye la definición de la estructura, competencia, funciones y procesos a través del manejo efectivo de la delegación de autoridad y el trabajo en equipo.
- **De servicio.-** Representan la manera en que se puede constatar que la organización está inmersa en un proceso que la vincula cuantitativa y cualitativamente con las expectativas y satisfacción de sus clientes.
- **De calidad.-** Disponen que tienda a elevar los niveles de actuación de la organización en todos sus contenidos y ámbitos, para que produzca bienes y servicios altamente competitivos.
- **De cambio.-** La transforman en un instrumento que hace más permeable y receptiva a la organización.
- **De aprendizaje.-** Permiten que se transforme en un mecanismo de aprendizaje institucional para que la organización pueda asimilar sus experiencias y las capitalice para convertirlas en oportunidades de mejora.
- **De toma de decisiones.-** Traducen su puesta en práctica y resultados en un sólido instrumento de soporte al proceso de gestión de la organización.

c. Características de la Auditoría Administrativa

Su principal característica de la auditoría administrativa es por el sentido de evaluación debido a que nos permite evaluar la calidad individual y colectiva de los gerentes como del personal de la empresa en sus diferentes departamentos, es decir de aquel personal responsables de las funciones operacionales que maneja la misma, de esta manera poder determinar que la calidad del trabajo esté encaminada a la normativa que se establece y así poder cumplir con los objetivos planteados por la empresa.

2.3.2. Auditoría Informática.

> Un proceso formal ejecutado por especialistas del área de auditoría y de informática; se orienta a la verificación y aseguramiento de que las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología de informática en la organización se lleven a cabo de una manera oportuna y eficiente. (Hernandez Hernandez Enrique, 1996, pág. 17)

> (Martínez, Blanco, & Loy Marichal, 2012) definen como un: Conjunto de procedimientos y técnicas que permiten en una entidad: evaluar, total o parcialmente, el grado en que se cumplen la observancia de los controles internos asociados al sistema informático; determinar el grado de protección de sus activos y recursos; verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existentes en la entidad, y para conseguir la eficacia exigida en el arco de la organización correspondiente

Nos permite examinar, evaluar, recopilar, recoger evidencias con el objetivo de determinar si el sistema informatico que posee la empresa salvaguarda el activo de la entidad y esta sea integra al manejar un paquete de datos cumpliendo con las diferentes leyes y regulaciones actuales, de esta manera verificamos si se maneja eficientemente y esten vigilados de manera correcta por el responsable de los mismo.

> Es un examen metódico del servicio informático, o de un sistema informático en particular, realizado de una forma puntual y de modo discontinuo, a instancias de la Dirección, con la intención de ayudar a mejorar conceptos como la seguridad, la eficacia, y la rentabilidad del servicio o del sistema que resultan auditados. (Rivas, 1989, págs. 39-40)
> Es un examen metódico del servicio informático, o de un sistema informático en particular, realizado de una forma puntual y de modo discontinuo, a instancias de la Dirección, con la intención de ayudar a mejorar conceptos como la seguridad, la eficacia, y la rentabilidad del servicio o del sistema que resultan auditados. (Rivas, 1989, págs. 39-40)
> La auditoría informática es la revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad de la organización que participa en el proceso de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones. La auditoría en informática deberá

> comprender no solo la evaluación de los equipos de cómputo o de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtener la información adecuada y la organización especifica (departamento de computo, departamento de informática, gerencia de procesos electrónicos, etc.) que hará posible el uso de los equipos de cómputo. (Echenique Garcia Jose Antonio, 2001, pág. 16)

La auditoría informática está orientada en el proceso para recopilar información que será diagnosticada para obtener evidencias si la empresa tiene un manejo adecuado de las TIC brindando seguridad de la información en todos los procesos que se realiza dentro de una organización, que nos permitirá tener un manejo eficiente de la información.

a. Objetivos de la Auditoría Informática

El objetivo primordial para la alta dirección del negocio es asegurar que el desempeño de las actividades de auditoría en informática se ejecute oportuna y eficiente según (Hernandez Hernandez Enrique, 1996, pág. 34) de manera que se logre que los auditores cuenten con:

- Independencia funcional
- Libertad de acción
- Facultad para la toma de decisiones
- Negociación con los niveles de gerenciales
- Involucramiento e proyectos de alto impacto en el negocio.

Para contar con un enfoque adecuado en la auditoria informática se debe contar con un excelente desempeño en todas las actividades que se realiza al momento del desarrollo de la misma de esta manera se logra obtener bueno resultados.

> En su Tesis de Magister: La auditoría informática confirma la consecución de los objetivos tradicionales de la auditoría: objetivos de protección de activos e integridad de datos; y objetivos de gestión, que abarcan no solamente los de protección de activos, sino también los de eficacia y eficiencia. (Quintuña Rodriguez, 2012)

En otras palabras es cuidar, precautelar a todos los activos y de esta manera velar sobre la integridad, y brindando confianza al momento de manejar información y datos que posee la organización, pero a la vez también nos enfocamos a ver qué tan eficaz y eficiente es la entidad.

b. Metodología y Fases de la Auditoría Informática

(Kuna Horacio, 2006) Tesis de Magister: Asistente para la realización de Autoría de Sistemas en Organismos Públicos o Privados, enuncia una metodología de desarrollo de Auditoría Informática muy general, se contemplan las siguientes fases:

Fase 1. Identificar el alcance y los objetivos de la Auditoría Informática
En esta fase se determinan los límites y el entorno en que se realizará la auditoría, debe existir un acuerdo muy preciso entre autoridades y auditores. El éxito del proceso depende de una clara definición de esta etapa.
Fase 2. Realizar el estudio inicial del entorno a auditar
En esta fase es necesario examinar las funciones y actividades generales de la organización a auditar y en particular de las relacionadas con las tecnologías de la información. Se debe definir el organigrama, los departamentos, las relaciones funcionales y jerárquicas entre las distintas áreas de la organización, el flujo de información, el número de puestos de trabajo y personas por puesto de trabajo, la estructura organizativa del departamento de informática, características de hardware y software, las metodologías de desarrollo y mantenimiento de aplicaciones, y aspectos relacionados con la seguridad.
Fase 3. Determinación de los recursos necesarios para realizar la auditoría Informática.
Después de realizar el estudio preliminar se debe determinar los recursos materiales y humanos necesarios para implementar el plan de auditoría.
Fase 4. Elaborar el plan de trabajo
En esta fase se define el calendario de actividades a realizar, formalizando el mismo para la aprobación por parte de las autoridades.
Fase 5. Realizar las actividades de auditoría
Es el momento donde se efectivizan las actividades planificadas en la fase anterior, aplicando distintas técnicas y utilizando herramientas que garanticen el cumplimiento de los objetivos planteados.
Fase 6. Realizar el informe final
La elaboración del Informe Final es la única referencia constatable de toda auditoría, y el exponente de su calidad.”
Fase 7. Carta de Presentación.
Es la última etapa de la auditoría consta de un resumen del contenido del informe final, dirigida a las autoridades de la institución.

El autor nos indica una metodología apropiada con siete fases muy importantes la primera es muy indispensable ya que con ella determinamos muy bien los límites en el cual se lleva la auditoría entre las dos partes, ya que si se plantea una excelente definición se llevara a cabo un proceso eficiente. Teniendo mucho en cuenta los diferentes departamentos y todo su recurso tanto humano como tecnológico que posee la empresa, en todas las fases nosotros llevamos un adecuado objetivo en el cual es tomar en cuanta claramente el recuso necesario para llevar acabo la auditoría, elaboración de un plan de trabajo con su respectivo calendario y especificando las actividades a cumplir por día, ya que con este proceso nosotros podemos concluir a un informe final es el documento más importantes en él se presentan los resultados obtenidos durante la evaluación dicho informe debe ser claro preciso para poder facilitar acciones correctivas por parte de la empresa.

2.3.3. Auditoría Forense.

> Debe entenderse como el proceso de recopilar, evaluar y acumular evidencia con la aplicación de norma, procedimiento y técnicas de auditoria, finanzas y contabilidad, para la investigación de ciertos delitos, a los que se ha dado en llamar “financieros” o de “cuello blanco”. (Chavarría & Roldán, Auditoría Forense, pág. 3)

Como el autor indica es un proceso que nos permite verificar y evaluar llevando a cabo una investigación para verificar si existió algún tipo de fraude o delitos.

Partiendo de la idea expuesta, podemos decir que la Auditoría Forense es una técnica integrada por conocimientos de criminalística, contable, jurídico y de negocio, para detectar fraudes financieros, especializada en la prevención y detección de delitos financieros.

Por los que la auditoria forense se especializa en la prevención y detectar fraudes financieros a continuación los siguientes enfoques:

a. Características de la auditoria forense.

Es analizar, evaluar e interpretar toda la información que se presenta durante la auditoria y si se encuentra algún tipo de delito hacer conocer de manera inmediata en el informe que se presenta.

Técnicas y procedimientos de auditoria forense son:

- Orientados a detectar si existe algún tipo robo de activos
- Orientados a detectar si hay corrupción.

b. Objetivos de la auditoria forense.

Según (Fontán Tapia María Evangelina, s.f.) Cita los siguientes objetivos:

- Identificar y demostrar el fraude o el ilícito perpetrado.
- Prevenir y reducir el fraude a través de la implementación de recomendaciones para el fortalecimiento de acciones de control interno propuestas por el auditor.
- Participar en el desarrollo de programas de prevención de pérdidas y fraudes.
- Participar en la evaluación de sistemas y estructuras de control interno.
- Recopilar evidencias aplicando técnicas de investigación.
- En el caso de organizaciones gubernamentales, brindar soporte técnico (evidencias sustentables) a los órganos del Ministerio Público Fiscal y de la Función Judicial, para la investigación de delitos y su ulterior sanción, entre otros.

c. Metodología de la Auditoría Forense.

El autor (Rizo José Mario, 2007, pág. 36), indica que independientemente del tipo de fraude que se investigue, la metodología está constituida por las siguientes actividades:

- Definición y reconocimiento del problema
- Recopilación de evidencias de fraude.
- Evaluación de la evidencia recolectada.
- Elaboración del informe final con los hallazgos.
- Evaluación del riesgo forense.
- Detección de fraude.

- Evaluación del Sistema de Control Interno.

La aplicación de la metodología parte del hecho de realizar una auditoría de forma integral y no solamente de la aplicación de un sistema particular de control, sin olvidarse que de detectarse irregularidades, el proceso puede verse afectado en cuanto a los objetivos, alcance de las pruebas entre otros aspectos, Forense Digital, ISO27307, Manejo de evidencia digital.

2.3.4. Auditoria forense Preventiva y Detectiva.

a. Auditoría Forense Preventiva.

> Según (Tapia Iturriaga, Guevara Rojas, Castillo Prieto, Rojas Tamayo, & Salomón Doroteo, o) la Auditoría Forense Preventiva esta; Orientada a proporcionar aseguramiento (evaluación) o asesoría a las organizaciones respecto de su capacidad para disuadir, prevenir (evitar), detectar y reaccionar ante fraudes financieros, puede incluir trabajos de consultoría para implementar: programas y controles anti fraude; esquemas de alerta temprana de irregularidades; sistemas de administración de denuncias. Este enfoque es proactivo por cuanto implica tomar acciones y decisiones en el presente para evitar fraudes en el futuro.

En general la auditoría forense preventiva es aquella enfocada en prevenir y evitar fraudes financieros, corrupción financiera sea esta en lo público o privado proporcionando herramientas que permitan proceder frente, disuadir y detectar acciones de fraude.

La auditoría forense preventiva, es la que nos permite mediante prevenir hechos que se pueden suscitar en un tiempo determinado dentro de una organización, la cual permite tomar acciones y decisiones para poder enfrentarnos a un futuro fraude.

b. Auditoría Forense Detectiva.

Ibídem

Está orientada a identificar la existencia de fraudes financieros mediante la investigación profunda de los mismos llegando a establecer entre otros aspectos los siguientes: cuantía del fraude; efectos directos e indirectos; posible tipificación (según normativa penal aplicable); 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 de fraudes sucedidos en el pasado

Es de mucha importancia la auditoria forense detective porque se investiga de una manera minuciosa para poder encontrar; fraudes, autores en un acto de estafa y como se realizó dicho fraude. Y así la auditoría nos permite tomar decisiones ha hechos sucedidos.

2.4. Fraude

2.4.1. Tipos de fraude.

Según INCPC (Instituto Nacional de Contadores Públicos de Colombia) (Moncayo Carolina, 2016) cita los siguientes fraudes:

- Ventas y Servicios no contabilizados depositándose a cuentas bancarias personales.
- Ventas y Servicios no declarados en impuestos.
- Créditos recuperados no contabilizados.
- Pagos autorizados a empresas y bienes no ingresados físicamente, estando únicamente registrados.
- Pago de sueldos a personal que no labora.
- Sueldos pagados a jubilados o personas inexistentes.
- Cuentas por Cobrar en cheques rechazados.
- Cuentas por cobrar no liquidadas oportunamente
- Faltantes sin recuperación oportuna, haciendo caso omiso la administración.
- Ingresos no registrados y pago menor de impuestos.

- Alteración en facturas y registros contables.
- Anulación de facturas cobradas.
- Facturas no autorizadas por entes fiscalizadores.
- Una persona realiza varias funciones de control y registro cobrando cheques a su nombre.
- Pasivos registrados sin documentación soporte.
- Falta de normas internas que castiguen fraudes.
- Cheques endosados más de una vez.
- Inventarios registrados sin documentación soporte.
- Transacciones inusuales a fin de año, ejecutando el gasto y no Recibiendo el bien o servicio.
- Servicios recibidos en informes y que al ser evaluados no existe el servicio.
- Doble facturación.
- Doble contabilidad, financiera y fiscal.
- Pérdida de libro de inventarios para ocultar faltantes de bienes.
- Clientes y Proveedores sin cumplir requisitos de calidad del bien o servicio y autorizados por la Gerencia para su pago.
- Activos fijos sin tarjetas de kárdex bajo responsabilidad de personas que las usan, perdiéndose el activo.
- Destrucción de documentos legales.
- Ajustes contables a final de año sin contar con documentación soporte, para ocultar ganancias.
- Ocultamiento contable en sub cuentas de gastos ficticios, pérdidas del ejercicio y ganancias.
- Transacciones autorizadas por gerencia, sin conocimiento de propietarios.
- Mermas ficticias en inventarios.
- Traslado de facturas para ocultar ingresos y evadir impuestos entre empresas relacionadas de socios.
- Sobrevaloración de servicios y bienes.
- Gastos personales pagados con fondos de la empresa.
- Contratación de empresas que a su vez sub contratan a otras para prestar el servicio o bien.
- Bienes trasladados a agencias o unidades internas que se registran dos veces en control de salida y realmente aparece registrado en la unidad únicamente una vez su ingreso.
- Gastos pagados en teléfono, usándose para otros fines las llamadas.
- Bienes o servicios pagados, que usualmente no son recibidos.
- Cotizaciones falsas con datos de teléfonos, direcciones que no existen.
- Desviación del presupuesto aprobado a cuentas de gastos específicas a otros rubros de gasto, provocando malversación de fondos.

Son algunos de los tipos de fraudes que se puede encontrar en las empresas de servicios ya que cuentan con un sin número de irregularidades por lo tanto son vulnerables a cometer alguno de ellos por lo que la auditoria forense nos permite evaluar, analizar y comprobar si toda la información es real y cumple con los registros de la entidad ya que al realizar todo el proceso de análisis se puede detectar algunos de los tipos de fraudes mencionados anteriormente.

2.4.2. Principales fraudes financieros.

En lo que sucedió del año pasado 2017 los tipos de fraudes mencionados según (Juarez Edgar, 2017) son los siguientes:

- **Fraudes cibernéticos**
  La Condusef cataloga los fraudes cibernéticos como aquellas estafas que utilizan la red para realizar transacciones ilícitas.
- **Correo basura o spam**
  El correo basura, o spam, se trata de mensajes enviados a varios destinatarios, que no lo solicitaron, con fines publicitarios o comerciales.
- **Smishing**
  En este tipo de fraude, los delincuentes envían mensajes SMS al teléfono móvil, con la finalidad de que se visite una página web fraudulentos, con el fin de obtener información bancaria de la persona, y realizar transacciones a su nombre.
- **Phishing**
  También conocido como suplantación de identidad. Aquí el objetivo es que, al hacerse pasar por una institución financiera, se enviará al usuario un mensaje indicando un error en la cuenta bancaria, para que al ingresarse los datos, se obtenga la información confidencial como números de tarjetas, claves y contraseñas.
- **Pharming**
  Consiste en redirigir a una página de Internet falsa mediante ventanas emergentes para robar la información del usuario. Estos sitios suelen mostrar leyendas como: Error en el sistema. Para solucionarlo, da clic aquí.
- **Fraude en comercio electrónico**
  La Condusef refiere que el comercio electrónico es la compra-venta de bienes y servicios a través de Internet, cuyas transacciones se pagan con tarjetas de débito y crédito, por lo que debe ponerse mucha atención al momento de llevar a cabo las compras, pues no existe contacto directo con el vendedor y puede convertirse en fraude.

Los mencionados fraudes financieros que afectaron en el primer trimestre del año pasado afectaron de manera muy grave a personas que utilizan los servicios de intermediación financiera por lo que los que realizan los delitos tomaron por ventaja el nuevo servicio de transacciones por medio de internet o un teléfono móvil es por lo que nos convertimos en una sociedad vulnerable hacer víctimas de este tipo de fraudes.

2.4.3. Fraudes tradicionales.

Ibídem

Otros tipos de fraudes que se mencionaran a continuación:

- **Créditos exprés**

  Se trata de aquellas estafas en las que falsas empresas que se hacen pasar por gestoras de crédito, ofrecen grandes préstamos con mínimos requisitos e inclusive sin consultar el historial crediticio, y con tasas de interés por debajo del mercado. Usualmente piden un depósito anticipado argumentando que son gastos de solicitud y comisión por apertura, pero que nunca se devuelve.
- **Pirámides**

  Son cadenas de ahorro que ofrecen ganancias elevadas. Existen varios tipos como la Flor de la Abundancia, Células de Gratitud, Bolas Solidarias, Círculo de la Prosperidad, entre otros. Usan mucho las redes sociales.
- **Ahorro informal**

  La tanda, por ejemplo, es el esquema más conocido en materia de ahorro informal. Sin embargo, no debe olvidarse que aunque se trate de una persona de confianza quien la administra, puede dejar al usuario sin su dinero en cualquier momento.
- **Trashing**

  Se trata de buscar información valiosa en la basura, como estados de cuenta, copias de identificaciones oficiales u otro documento que contenga datos importantes, con los cuales se puede realizar un fraude como robo de identidad o realizar transacciones bancarias a su nombre.

- **Alteración de cheque**

  Ocurre cuando una persona se acerca al cliente que está en la fila del banco y ofrece comprarlo para que no se pierda tiempo en la sucursal. Una vez que el delincuente tiene el documento, se retira y procede a alterar alguna parte como el nombre al portador, el monto a cobrar y el endoso.

- **Tallado de tarjetas**

  Se realiza en cajeros y opera en grupos que alteran la ranura donde va el plástico y al tratar de retirar dinero, una persona le comenta al usuario que el cajero está fallando. Después le piden la tarjeta argumentando que se debe tallar o limpiar, pero en este momento se cambia el plástico y el delincuente se retira. Un cómplice entra entonces al ATM y en lo que la afectada trata de realizar una operación con la tarjeta que no es la suya, observa el NIP que se está tecleando.

Este tipo de fraudes son los que existen desde años anteriores por lo que son de conocimiento de toda persona ya que alguna vez fuimos víctima de alguno de ellos por lo que el modo de operación era hacer creer la existencia de empresas que facilitan créditos a la sociedad la cual eran entidades fantasmas, al momento de que una persona accede a este tipo de servicio se convierte en una víctima al caer en la estafa que ellos realizan al pedir dinero anticipado como parte de una entrada para obtener dicho crédito. En diferencia de las pirámides que alguna vez en nuestro país escuchamos una noticia de esta índole ya que su modo de operación era colocando dinero y a través de ese ahorro se conseguía ganancias muy altas las cuales se convertían en un futuro en fraude. Son algunos de los tipos de fraudes que los delincuentes se inventan aprovechaban de estar en las instituciones financieras para realizar robos a los clientes que están acudiendo a la entidad aplicando sus diferentes técnicas de fraude mencionadas en el párrafo anterior.

2.4.4. Fraude en los sistemas computarizados.

Manipulación de datos

Este es uno de los métodos que más se ha utilizado según (Estupiñán Gaitán Rodrigo, 2006, págs. 361-362-363)

> Para realizar este tipo de fraude sistemático o informático consiste en cambiar los datos de antes y durante la entrada al computador. Puede ser ejecutado por cualquier persona que tenga acceso a crear, registrar, transportar, codificar, examinar, comprobar o convertir los datos que entran al computador.
>
> - **Técnicas de Salami**
>   La técnica de salami consiste en sustraer pequeñas cantidades (tajadas) de un gran número de registros, mediante la activación de rutinas incluidas en los programas aplicativos corrientes. La empresa es la dueña del salami (archivo de datos) de donde el desfalcador toma pequeñas sumas (centavos) para llevarlos a cuentas específicas conocidas solamente por el perpetrador del fraude.
> - **Técnica del caballo de Troya**
>   Consiste en insertar instrucciones, con objetivos de fraude, en los programas aplicativos, de manera que, además de las funciones propias del programa, también ejecute funciones no autorizadas.
> - **Las bombas lógicas**
>   Son una técnica de fraude, en ambientes computarizados, que consiste en diseñar e instalar instrucciones fraudulentas en el software autorizado, para ser activadas cuando se cumpla una condición o estado específico.
> - **Trampas-puertas**
>   Son deficiencias del sistema operacional, desde las etapas de diseño original (agujeros del sistema operacional).
> - **Superzaping**
>   Un programa utilizado de IBM de un alto riesgo por sus capacidades. Permite adicionar, modificar y/o eliminar registro de datos. Datos de registro o agregar caracteres dentro de un archivo maestro, sin dejar rastro y sin modificar ni corregir los programas normalmente usados para mantener el archivo.
> - **Evasiva astuta**
>   Se trata de que los System programmers se inventaron la forma de comunicarse con la computadora a través del lenguaje de máquina. Esta técnica también se le conoce con el nombre de parches. Es un método limpio para entrar en la computadora, cambiar las cosas, hacer que algo suceda y hasta cambiarlas para que vuelva a su forma original sin dejar rastros para auditoria.

Para realizar algún tipo de fraude dentro de un sistema se necesita conocer muy bien del sistema que se maneja dentro de una institución o entidad, de la misma forma también se puede realizar enviando pequeñas cantidades en este caso hablamos de centavos a cuentas de terceros y de esta forma estamos cometiendo un fraude siendo autores intelectuales del mismo ya que nosotros manejamos el sistema transaccional y aplicado un plan de delito. Otro tipo de fraude es por medio de un computador en el cual cuando el programa realiza cambios en la información o en los datos que posee la entidad ya que son operaciones sin autorización que causan mucho daño, de esta forma es como desarrollan y ejecutan los delitos los ejecutores del fraude.

2.5. Programa de Auditoría

> Se define el programa de Auditoría, como el procedimiento a seguir, en el examen a realizarse, el mismo que es planeado y elaborado con anticipación y debe ser de contenido flexible, sencillo y conciso, de tal manera que los procedimientos empleados en cada Auditoría estén de acuerdo con las circunstancias del examen. (Alatrista Gironzini, 2016)

En este sentido el autor manifiesta que para elaborar un programa de auditoría se demo tener en cuenta aspectos importantes como las normas, técnicas, de auditoría, experiencias anteriores, experiencias de terceros, etc.

“Es la evaluación de la eficiencia técnica, del uso de diversos recursos (cantidad de memoria) y del tiempo que utilizan los programas, su seguridad y confiabilidad, con el objetivo de optimizarlos y evaluar el riesgo que tiene para la organización”. (Echenique Garcia Jose Antonio, 2001)

Nos indica que este tipo de técnica que evalúa los programas ya que estos deben ser eficientemente tratados para brindar seguridad a la organización al momento de manejar

un paquete o base de datos, la cual debe ser manejada con cautela para evitar el riesgo en un futuro.

2.5.1. Objetivos de los programas de auditoría.

La Norma (ISO 19011, 2015), menciona que un programa de auditoría debe incluir cierta información para organizar de forma eficaz y eficiente; por lo que se consideran los siguientes:

- Prioridades de la dirección
- Propósito comercial y de negocio
- Características de procesos, productos y proyectos
- Requisitos del Sistema de Gestión
- Requisitos legales y otros requisitos con los que la empresa se encuentre comprometida
- Necesidad de evaluar a los proveedores
- Las necesidades y las expectativas de las partes interesadas
- Nivel de desempeño del auditado
- Riesgos que debe asumir el auditado
- Resultados de las auditorias previas
- El nivel de madurez del Sistema de Gestión que se audita.

Los objetivos deben basarse mucho en a base de la auditoria como nos indica tener un enfoque en la dirección de la entidad, actividad a la que se dedica y de esta manera podemos plantear los objetivos.

a. Características de los programas de auditoría.

Las principales características que un programa de auditoría debe tener se consideran las siguientes:

- Debe ser sencillo y comprensivo.
- Debe ser elaborado tomando en cuenta los procedimientos que se utilizarán de acuerdo al tipo de empresa a examinar.
- El programa debe estar encaminado a alcanzar el objetivo principal.
- Debe desecharse los procedimientos excesivos o de repetición.

- El programa debe permitir al Auditor a examinar, analizar, investigar, obtener evidencias para luego poder dictaminar y recomendar.
- Las Sociedades Auditoras, acostumbran tener formatos pre establecido los cuales deben ser flexibles para que puedan ser adecuados a un determinado tipo de empresa.
- El programa debe ser confeccionado en forma actualizada y con amplio sentido crítico de parte del Auditor. (Alatrista Gironzini, Auditool, 2016)

Las características básicas o esenciales que se manejan en los programas de auditoría vienen de un plan general de la auditoría estos deben ser claros precisos, que estén enfocados en la actividad principal que se dedica la entidad, siempre y cuando el programa de auditoría este guiado por el objetivo principal ya que nos permite tener un plan o cronograma na de actividades en el cual se debe ir cumpliendo cada proceso para llevar una auditoría exitosa.

a. Informes de Auditoría

De acuerdo a la opinión de (Velázquez Labrada Yadira, 2015) los informes de auditoría:

> Son el resultado final del proceso, que tendrá su basamento en las conclusiones obtenidas, en las llamadas de atención sobre las deficiencias detectadas y en las observaciones y medidas correctoras que deberán tomarse. Se expresará, con claridad y precisión, los hechos y situaciones reales, mediante los informes preliminares y las evidencias reflejadas en los papeles de trabajo. De existir alguna limitante en cuanto al cumplimiento de los aspectos que contiene el programa aplicado, esta debe quedar reflejada en dicho informe.

Sin embargo, previa la elaboración del informe definitivo de la auditoría, es importante informes parciales, donde los especialistas que integran el equipo formulen todas las deficiencias encontradas en las diferentes actividades auditadas. Mismos que servirán como proceso de análisis de las causas y de las recomendaciones que, en lo posterior, formarán parte del informe final.

2.6. Tecnologías de Información y Comunicación (TIC)

El término TIC forma parte de nuestra cultura, de nuestra vida, de nuestras actividades cotidianas, puesto que ha eclosionado nuevas posibilidades para el ser humano en torno a la digitalización de datos, de su transportación a través de diferentes medios, a grandes distancias y en pequeños intervalos de tiempo.

La revolución informática que vive la humanidad en esta última década es en buen parte gracias a las TIC, caracterizada por la globalización de la información y el desenvolvimiento científico y tecnológico.

Haciendo referencia a este término mencionan que las “tecnologías de la Información y Comunicación son el conjunto de procesos y productos derivados de las nuevas herramientas (hardware y software), soportes de la información y canales de comunicación relacionados con el almacenamiento, procesamiento y transmisión digitalizada de la información”. (Díaz Lazo, Pérez Guitiérrez, & Florido Bacallao, 2011)

En la actualidad las tecnologías de información y comunicación son de gran aporte para la sociedad ya que estas nos permiten estar comunicados a través del mundo entero a través de un computador y de una red de internet, esto ha facilitado al ser humano para realizar muchas actividades.

> En líneas generales podríamos decir que las nuevas tecnologías de la información y comunicación son las que giran en torno a tres medios básicos: la informática, la microelectrónica y las telecomunicaciones; pero giran, no sólo de forma aislada, sino lo que es más significativo de manera interactiva e interconexionadas, lo que permite conseguir nuevas realidades comunicativas. (Cabrero, 1998, pág. 198)

De acuerdo al concepto del autor se puede decir que la Tecnología de Información y Comunicación son de vital importancia para el desarrollo informático en las empresas por que cuentan con el cruce de información, que una entidad necesita conocer.

Hoy en día tenemos todos en nuestros hogares un televisor que el mismo está conectado por cable, un computador y estar conectado a una banda de internet es un aporte de TIC hacia la sociedad para que estén conectados a través de un celular todo esto tenemos gracias a las tecnologías de información y comunicación.

Según (González Cruz Maité, 2011) Como aporte de las TIC tenemos:

- “Fácil acceso a una inmensa fuente de información
- Proceso rápido y fiable de todo tipo de datos
- Canales de comunicación inmediata
- Capacidad de almacenamiento
- Automatización de trabajos
- Interactividad
- Digitalización de toda la información”

2.7. Delitos Informáticos

Se define como delitos informáticos o ciberdelitos, a toda aquella actividad ilícita que:

- Se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación (la informática es el medio o instrumento para realizar un delito); o
- Tienen por objeto robo de información, robo de contraseñas, fraude a cuentas bancarias, etc. (Policía Nacional del Ecuador, 2015)

Los delitos informáticos de acuerdo a lo publicado en el año 2015 por la Policía Nacional, están basados en acciones por medio de ordenadores que permiten entrelazar comunicación para realizar dicho robo de información personal y confidencial.

Así también la Organización para la Cooperación Económica y el Desarrollo lo define como “cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automatizado de datos y/o la transmisión de datos" (Hernandez Jesus, 2016)

En otras palabras el autor nos indica que es un hecho ilegal realiado por una persona para causar un daño atraves un delito informático tiene un sin numero de actividades tales como robos, fraudes y estafa por medio de herramientas usadas por la persona que realiza el delito utilizando la informática como arma importante para llevar acabo su objetivo.

Se define al Delito informático como: “la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software”. (Davara Rodriguez Miguel Angel, 1993)

> Se podría definir como delito informático como toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima tipificado por la ley, que se realiza en el entorno informático y está sancionado con su pena. (Piattini Velthius Mario Gerardo: Del Peso Navarro Emilio, 2004)

Como se puede evidenciar de acuerdo a los diferentes puntos de vista de los autores se puede manifestar que, de delito informático, llamamos a todo acto ilícito no ético por

parte de personas que con el único fin es de dañar la integridad y privacidad de la información.

2.7.1. Tipos de delitos Informáticos.

Los tipos de delitos informáticos reconocidos por las Naciones Unidas son los siguientes:

a. Fraudes cometidos mediante manipulación de computadoras.

Manipulación de los datos de entrada

> Este tipo de fraude informático, conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos. (Hall Andrés)

Al momento de manipular una base de datos suscitan desviaciones de información a lo que denomina en el documento como sustracción, ya que no tiene dificultad al momento de sustraer los datos, y lo contrario al momento de encontrar responsables de dicho acto tiene un grado de dificultad.

Manipulación de programas

> Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal. (Hall Andrés)

Para este tipo de manipulación se debe contar con un conocimiento adecuado al momento de manejar programas por lo tanto se convierte en una tarea muy difícil para el delincuente como lo manifiesta el documento.

Manipulación de los datos de salida

> Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. (Hall Andrés)

El blanco perfecto de esta manipulación son las tarjetas de crédito, para dar paso a este tipo de eventos deben utilizar programas adecuados para poder dar con los códigos respectivos en cada tarjeta tanto bancaria como de crédito. Son utilizados últimamente para realizar estafas o robos a los usuarios afectados.

Manipulación informática aprovechando repeticiones automáticas de los procesos de cómputo.

“Es una técnica especializada que se denomina "técnica del salchichón en la que rodajas muy finas, apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra”. (Hall Andrés)

Técnica muy sofisticada que afecta de forma directa a los procesos de cómputo ya que con este tipo de modalidad se aprovecha de repeticiones sucesivas y ahí es donde se encuentra el fraude, al momento de enviarlas a otras cuentas.

(Téllez Valdés Julio, 1996, págs. 103-104) clasifica a los delitos informáticos en base a dos criterios: como instrumento o medio y como fin u objetivo.

Como instrumento o medio: en esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

- Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.).
- Variación de los activos y pasivos en la situación contable de las empresas.
- Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.).
- Lectura, sustracción o copiado de información confidencial.
- Modificación de datos tanto en la entrada como en la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
- Uso no autorizado de programas de cómputo.
- Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.
- Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
- Obtención de información residual impresa en papel luego de la ejecución de trabajos.
- Acceso a áreas informatizadas en forma no autorizada.
- Intervención en las líneas de comunicación de datos o teleproceso.

Como fin u objetivo: en esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

- Programación de instrucciones que producen un bloqueo total al sistema.
- Destrucción de programas por cualquier método.
- Daño a los dispositivos de almacenamiento.
- Atentado físico contra la máquina o sus accesorios.

- Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
- Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.)

b. Falsificaciones informáticas.

Como objeto

En este mismo orden de ideas (Hall Andrés) indica que este tipo de delitos se da, “cuando se alteran datos de los documentos almacenados en forma computarizada”.

Como instrumentos

Según, (Hall Andrés)

> Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

c. Daños o modificaciones de programas o datos computarizados.

(Hall Andrés) Indica lo siguiente:

> **Sabotaje informático**
> Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:
> **Virus**

> Es una serie de claves programáticas que pueden adherirse a los programas y propagarse a otros programas informáticos. Un virus puede ingresar al sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada.
> **Gusanos**
> Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

Este tipo de delito mencionado por el autor tiene como objetivo el cambio o modificación sin autorización de la persona afectada realizada a través de un computador de esta manera interfieren en la información real del usuario por lo tanto se convierte en un sabotaje informático realizado por medio de virus y gusanos informáticos.

d. Acceso no autorizado a servicios y sistemas informáticos

Ibídem

Piratas informáticos o hackers

El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

Reproducción no autorizada de programas informáticos de protección legal

Puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.

Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual".

En este tipo de delitos el delincuente en este caso Hackers toma ventaja por los niveles de seguridad que no son los adecuados para un sistema informático con el fin de ingresar como usuario para poder robar información por lo tanto se convierte en vulnerables a tener acceso a la información confidencial. En estos casos como consecuencia a la vulnerabilidad al acceso de información atrae grandes consecuencias económicas para los verdaderos dueños de la información, y tiene como castigo al autor intelectual sanciones penales bajo el código penal.

2.8. Sistemas de Información

> Un sistema de información (IS) es cualquier sistema organizado para la recopilación, organización, almacenamiento y comunicación de información. Más específicamente, es el estudio de redes complementarias que las personas y las organizaciones usan para recopilar, filtrar, procesar, crear y distribuir datos. (Enciclopedia Financiera, s.f.)

Según (López Aguilera Purificacion, 2010, pág. 8) indica que "Es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el

funcionamiento global de una empresa o de cualquier otra actividad humana para conseguir sus objetivos".

Los elementos que conforman son:

- **Recursos:** Están conformados por computadores conexiones, como también los sistemas operativos y aplicaciones en informática.
- **Equipo humano:** Es todo el personal que labora para la empresa u organización.
- **Información:** Son todos los datos que tiene la organización, dicha información se encuentra en diferente soporte.
- **Actividades:** Aquellas que se desarrolla dentro de la organización.

Nos permiten verificar, analizar y controlar todo lo que sucede en una entidad por medio de un sistema informático manejado por una persona que tenga la capacidad y el conocimiento necesario.

Según COBIT los recursos de ti son: aplicaciones, infraestructura, información y personas.

Ibídem

"Un sistema informático está constituidos por un conjunto de elementos físicos (hardware, dispositivos, periféricos conexiones), lógicos (sistemas operativos, aplicaciones, protocolos…) y con frecuencia se incluyen también los elementos humanos (personal experto en el manejo de software y hardware)".

El autor manifiesta que los sistemas informáticos están conformados de recursos lógicos, físicos y humanos para obtener un adecuado y correcto funcionamiento en el mismo.

2.9. Tipo de seguridad

2.9.1. Activa.

Según (García Alfonso: Hurtado Cervigón: Alegre Ramos María Del Pilar, 2011, pág. 3)

“Se entiende por seguridad activa todas aquellas medidas que se utilizan para detectar las amenazas y en caso de su detección generar los mecanismos adecuados para evitar el problema”

Indica (López Aguilera Purificacion, 2010, pág. 10) que comprende el conjunto de defensa o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema”.

Son todas las seguridades que se aplican en la empresa para proteger, salvaguardar ante posibles amenazas y riesgos que se pueden detectar.

2.9.2. Pasiva.

Según (García Alfonso: Hurtado Cervigón: Alegre Ramos María Del Pilar, 2011) “Comprende todo el conjunto de medidas utilizadas para que una vez que se produzca el ataque o el fallo en la seguridad de nuestro sistema, hacer que el impacto sea el menor posible, y activar mecanismos de recuperación del mismo”

“Está formada por las medidas que se implantan para, una vez producido el incidente de seguridad, minimizar su repercusión y facilitar la recuperación del sistema; por

ejemplo, teniendo siempre al día copias de seguridad de los datos". (López Aguilera Purificacion, 2010, pág. 10)

El autor nos indica en el párrafo anterior, que son todas las disposiciones que se toma en cuenta después de un ataque a la seguridad en el sistema, y de esta manera minimizar el riesgo.

2.10. Seguridad Informática

"El conjunto de normas, mecanismos, herramientas, procedimientos y recursos orientados a brindar protección a la información resguardando sus disponibilidad, integridad y confidencialidad". (Universidad Nacional Autonoma de Mexico, s.f.)

(López Aguilera Purificacion, 2010, pág. 9) sostiene: "Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable".

La seguridad informática es la encargada de diseñar todos los procesos para llevar a cabo un excelente manejo, con el objetivo de tener un sistema seguro y confiable, tratando de evitar el riesgo en el mismo.

> **Servicios de Seguridad Informática** (Universidad Nacional Autonoma de Mexico, s.f.) es aquel que mejora la seguridad de un sistema de información y el flujo de información de una organización. Los servicios están dirigidos a evitar los ataques de seguridad y utilizan uno o más mecanismos de seguridad para proveer el servicio.

Clasificación

Una clasificación muy utilizada de los servicios de seguridad es la siguiente:

- Confidencialidad
- Autenticación
- Integridad
- No repudio
- Control de acceso
- Disponibilidad

En tanto la seguridad informática juega un papel importante dentro de las organizaciones empresariales, porque permite hacer frente contra multiples amenazas, la mayoria de estas son causadas por programas maliciosos con la intención de generar daños o a la vez para utlizar la informacion de la empresa de forma ilegitima. Para todo estos daños existen servicios de seguridad que brndan servicios para la proteccion de la informacion.

(López Aguilera Purificacion, 2010, pág. 9) Dice que para afrontar el establecimiento de un sistema de seguridad es necesario conocer:

- **Cuáles son los elementos que componen un sistema.** Esta información se obtiene mediante entrevistas con los responsables o directivos de la organización para la que se hace el estudio de riesgo y mediante apreciación directa.
- **Cuáles son los peligros que afectan al sistema, accidentalmente o provocados.** Se deducen tanto de los actos aportados por la organización como por el estudio directo del sistema mediante la realización de pruebas y muestreo sobre la misma.
- **Cuáles son las medidas que deberían aportarse para conocer, prevenir, impedir, reducir o controlar los riesgos potenciales.** Se trate de deducir cuáles serán los servicios o mecanismos de seguridad que reducirían los riesgos al máximo posible.

2.11. Vulnerabilidad

> (Piattini Velthius Mario Gerardo: Del Peso Navarro Emilio, 2004, pág. 50) La situación creada, por la falta de uno o varios controles, con lo que la amanezca pudiera acaecer y así afectar el entorno informático. Ejemplo: la falta de control de acceso lógico, falta de control de versiones, inexistencia de un control de soportes magnéticos, falta de separación de entornos en el sistema, falta de cifrado en las telecomunicaciones.

Debilidad del sistema informático que puede ser manipulada para causar daños ya sea en el hadware, software, y el sistema operativo, es un componente de un sistema informático, mismo que puede ser utilizado para violentar la seguridad causando daños, sin intención alguna.

> La vulnerabilidad de un sistema informático son todas aquellas debilidades que se están presentando en el sistema, lo cual hace susceptible de ser afectado, alterado o destruido por alguna circunstancia indeseada, que afectan al funcionamiento normal o previsto de dicho sistema informático. (Universidad Nacional Autonoma de Mexico, s.f.)

Las vulnerabilidades pueden clasificarse en seis tipos:

1. **Física:** Lo podemos encontrar en el edificio o entorno físico. La relacionamos con la posibilidad de entrar o acceder físicamente al lugar donde se encuentra el sistema para robar, modificar o destruir el mismo. Esta vulnerabilidad se refiere al control de acceso físico al sistema.
2. **Natural:** Se refiere al grado en que el sistema puede verse afectado debido a los fenómenos naturales que causan desastres.

Las vulnerabilidades pueden ser:

- No contar con un espejo del sistema en otro lugar geográfico en caso de inundaciones o terremotos.

- No disponer de reguladores, no-breaks, plantas de energía eléctrica alterna
- Tener una mala instalación eléctrica de los equipos, en caso de rayos, fallas eléctricas o picos altos de potencia.
- En caso de inundaciones, el no contar con paredes, techos impermeables y puertas que no permitan el paso del agua.

3. **De hardware:** El no verificar las características técnicas de los dispositivos junto con sus respectivas especificaciones, la falta de mantenimiento del equipo. Desde el punto de vista del hardware, ciertos tipos de dispositivos pueden ser más vulnerables que otros. Así, pueden existir algunos sistemas que no cuenten con la herramienta o tarjeta para poder acceder a los mismos; adquirir un equipo de mala calidad o hacer un mal uso del mismo, tener el equipo de cómputo expuesto a cargas estáticas, etc.
4. **De software:** Ciertas fallas o debilidades de los programas del sistema hace más fácil acceder al mismo y lo hace menos confiable. Este tipo de vulnerabilidades incluye todos los errores de programación en el sistema operativo u otros de aplicaciones que permite atacar al sistema operativo desde la red explotando la vulnerabilidad en el sistema.
5. **De red:** La conexión de las computadoras a las redes supone un enorme incremento de la vulnerabilidad del sistema, aumenta considerablemente la escala de riesgos a que está sometido, al aumentar la cantidad de gente que puede tener acceso al mismo o intenta tenerlo. También se añade el riesgo de intercepción de las comunicaciones:
   - Se puede penetrar al sistema a través de la red.
   - Interceptar información que es transmitida desde o hacia el sistema.

   Se debe tener cuidado en que el centro de cómputo no tenga fallas debido a una mala estructura y en el diseño del cableado estructurado por no seguir ningún estándar para el diseño e implementación del mismo.
6. **Humana**

   Algunas de las diferentes vulnerabilidades humanas se tienen:

- Contratar personal sin perfil psicológico y ético
- No tener personal suficiente para todas las tareas,
- El descuido,
- El cansancio,
- Maltrato del personal, así como la mala comunicación con el personal, malos entendidos
- Personal irresponsable, que descuida el acceso a su área de trabajo,
- No tener servicio técnico propio de confianza,
- No instruir a los usuarios para que eviten responder a preguntas sobre cualquier característica del sistema,
- No asegurarse de que las personas que llaman por teléfono son quienes dicen ser,
- El no tener control de acceso o acceso basado en restricciones de tiempo,
- No contar con guardias de seguridad,
- No tener un control de registros de entrada y salida de las personas que visitan el centro de cómputo,

Tenemos muchas vulnerabilidades los cuales engloba la infraestructura, desastres que provienen de la naturaleza y que no se puede controlar, programas que necesitan los computadores para desarrollar cierto tipo de actividades las cuales se manejan a través de programas y estos son vulnerables a la vez, la red en la cual se está conectando por que presentan mayor grado de debilidad para ser atacados por un hackers, virus informático que su único objetivo es robar, manipular y causar daños y por ultimo tenemos las falla humana estas son oportunidades para los que realizan delitos informáticos.

(López Aguilera Purificacion, 2010, pág. 14) “Probabilidad que existen de que una amenaza se materialice contra un activo. No todos los activos son vulnerables a la misma amenaza”.

Posibilidad que puede suscitar algún evento en contra de un activo, pero no todos tienes la misma posibilidad de ser atacados.

> **Ataques no intencionados** es cuando un hecho perjudica a la información, a la TI o a la empresa sin que ocurra por las acciones intencionales por alguien. **Ataques intencionados** se considera a los accesos no autorizados al sistema donde el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, con el fin de robar información o alterar registros o los emplea con fines inapropiados aun cuando tiene autorización para usarlos. (Baca Urbina Gabriel, 2016)

En otras palabras, los ataques provienen cuando estos tienen intención en causar algún tipo de daño al sistema que ataca, y el otro en cambio es cuando no se tiene un fin de realizar algún daño estos son los no intencionados al momento de realizar cualquier actividad.

2.12. Riesgo

(Piattini Velthius Mario Gerardo: Del Peso Navarro Emilio, 2004, pág. 50) “La probabilidad de que una amenaza llegue a acaecer por una vulnerabilidad. Ejemplo: los datos estadísticos de cada evento de una base de datos de incidentes”.

Es la probabilidad en la que una amenaza llegue a suceder por una vulnerabilidad. Es necesario que en las empresas cuenten con una herramienta que asevere la correcta evaluación de los riesgos, a los mismos que están sometidas las actividades y procesos que participan en el área informática.

(López Aguilera Purificacion, 2010) “Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe una amenaza para la misma”.

La posibilidad en la cual un evento puede suscitar en un futuro causando daños a personas u organizaciones.

Proceso del Análisis de Riesgos según (Universidad Nacional Autonoma de Mexico, s.f.) Indica que un proceso de análisis del riesgo debe considerarse la siguiente terminología:

- **Activo:** es todo aquello con valor para una organización y que necesita protección –datos infraestructura, hardware, software, personal y su experiencia, información, servicios.
- **Riesgo:** posibilidad de sufrir algún daño o pérdida.
- **Aceptación del riesgo:** decisión para aceptar un riesgo.
- **Análisis de riesgo:** uso sistemático de información disponible para identificar las fuentes y para estimar qué tan seguido determinados eventos no deseados pueden ocurrir y la magnitud de sus consecuencias.

Ante el hecho de un riesgo debemos actuar y considerar que la entidad necesita seguridad para manejar información única de la entidad y de esta manera brindando seguridad a la sociedad, se debe tomar en cuenta que todos estamos expuestos a cualquier tipo de riesgo y debemos aceptarlo como tal para luego analizarlo en qué frecuencia el riesgo nos está atacando.

Análisis de Riesgos Objetivo

Ibídem

El objetivo del análisis de riegos es tener capacidad de:

- Identificar, evaluar y manejar los riesgos de seguridad.
- Estimar la exposición de un recurso a una amenaza determinada.
- Determinar qué combinación de medidas de seguridad proporcionará un nivel de seguridad razonable a un costo aceptable.
- Tomar mejores decisiones en seguida de la información.
- Enfocar recursos y esfuerzos en la protección de activos

2.12.1. Amenaza.

Para (López Aguilera Purificacion, 2010, pág. 13) “En un sistema de información se entiende por amenaza la presencia de uno o más factores de diversa índole (personas, maquinas o sucesos) que de tener la oportunidad atacarían al sistema produciéndoles daños aprovechándose de su nivel de vulnerabilidad”

Las amenazas vienen de la mano cuando se presenta algún tipo de oportunidad las cuales son generadas por el recurso humano y físico que posee la empresa, dando la apertura algún tipo de daño por parte de los autores principales de robo o daño de información.

> Las amenazas siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en la operativa de la empresa. Comúnmente se indican como amenazas a las fallas, a los ingresos no autorizados, a los virus, uso inadecuado de software, los desastres ambientales como terremotos o inundaciones, accesos no autorizados, facilidad de acceso a las instalaciones, etc. (Carrasquel Meneses Dorela: Méndez Aray, s.f.)

Una entidad u organización toda su vida estará expuesta a amenazas ya que puede originarse por distintas formas en las cuales pueden ser por fallas o mal manejo del sistema que maneja la empresa, como también puede ser ocasionada por ingresos indebidos de software sin tener un permiso de autorización, como los virus que también forman parte de una amenaza.

(Piattini Velthius Mario Gerardo: Del Peso Navarro Emilio, 2004, págs. 49-50) “Una persona o cosa vista como posible fuente de peligro o catástrofe. Ejemplo: inundaciones, incendio, robo de datos, sabotaje, agujeros publicados, falta de procedimientos de emergencia, divulgación de datos, implicaciones con la ley, aplicaciones mal diseñadas, gastos incontrolados, etc.”.

La amenaza proviene de un suceso que posee el potencial de originar un daño o una pérdida representativa para la entidad.

2.12.2. Exposición o Impacto.

(Piattini Velthius Mario Gerardo: Del Peso Navarro Emilio, 2004, pág. 50) “La evaluación del efecto del riesgo. Ejemplo: es frecuente evaluar el impacto en términos económicos, aunque no siempre lo es, como vidas humanas, imagen de la empresa, honor, defensa nacional, etc.”

Los sistemas informáticos están expuestos como manifiesta el autor en los párrafos anteriores, hay riesgos con una probabilidad de amenazas que pueden recaer en los sistemas por medio de su grado de vulnerabilidad, por lo tanto, se pueden dar tratamiento a los mismos para evitar problemas.

2.12.3. Riesgos que presentan.

Ibídem

Todos los riesgos que se presentan podemos:

- **Evitarlos** (por ejemplo: no construir un centro donde existe peligro de constante inundaciones).
- **Transferirlo** (por ejemplo: uso de un centro de cálculo contratado).
- **Reducirlos** (por ejemplo: sistema de detección y extinción de incendios).
- **Asumirlos** que es lo que se hace si no se controla el riesgo en absoluto.

Software Malicioso: Virus, Gusanos, Caballo de Troya y Spyware

Según (Laudon Kanneth & Laudon Jane, 2006, pág. 296) sostiene que:

> Los programas de software malicioso se conocen como malware e incluyendo una variedad de amenazas, como virus de computadora, gusanos y caballos de Troya.
>
> - **Gusanos:** programas de computadora independientes que se copian a si mismo de una computadora a otras computadoras a través de una red (a diferencia de los virus, pueden operar por su cuenta sin necesidad de unirse a otros archivos de programa de computadora y dependen menos del comportamiento humano para poder espaciarse de una computadora a otra. Esto explica por qué los gusanos de computadora se esparcen con mucha mayor rapidez que los virus). (Laudon Kanneth & Laudon Jane, 2006, pág. 296)
> - **Caballo de Troya:** es un programa de software que parece ser benigno, pero entonces hace algo distinto de lo esperado, como el virus troyano Zeus. El caballo de Troya en si no es un virus, ya que no se reproduce, pero es en frecuencia un medio para que los virus u otro tipo de software malicioso entren en un sistema computacional. (Laudon Kanneth & Laudon Jane, 2006, pág. 296)

Los softwares maliciosos provienen por diferentes amenazas que se adhieren en los computadores los más representativos son los gusanos dicho programa independiente que traslada la información de un computador hacia otra herramienta que se complementa con la conexión a una red y tienen un mayor impacto para esparcirse en los computadores. En tanto el Caballo de Troya tiene una singularidad en los medios para que los virus entren con mayor facilidad en un sistema del computador.

Ibídem pág. 50

“Programa de software malintencionado tipo “caballo de Troya” llamado Zeus, diseñado para robar datos financieros y personales al rastrear de manera furtiva las

pulsaciones de teclas de los usuarios al momento en que introducen información en sus computadores”.

Como el autor nos indica, son programas de software malicioso que su objetivo es provocar robo de información y daños como interrumpir, detener procesos diarios operacionales al momento de su ejecución.

2.13. Los Hackers y los Delitos Computacionales

Los hackers en los sistemas informáticos, expertos encontrando debilidades en computadores y en redes.

> Un hacker es un individuo que intenta obtener acceso sin autorización a un sistema computacional. Dentro de la comunidad de hackers, el termino cracker se utiliza con frecuencia para denotar a un hacker con intención criminal, aunque en la prensa publica los términos hacker y cracker se utilizan sin distinción. (Laudon Kanneth & Laudon Jane, 2006, pág. 298)

El objetivo principal de un hacker es entrar o ingresar en un sistema sin autorización, por lo que esto le convierte en un fraude y delito al momento de tener algún tipo de información con la cual desarrolla su mala intención para causar daño a la entidad o usuario afectado.

2.13.1. Tipo de hackers.

Según (Terán Perez David Moises, 2014) existe algunos tipos de hacker, los cuales detallaremos a continuación:

- **Cracker** se denominan así a aquella persona con comportamiento compulsivo, que alardea de su capacidad para reventar sistemas electrónicos e informáticos. Un cracker es un hábil conocedor de programación de software y de hardware; así como fabrica programas de guerra para

hardware, para reventar software y para las telecomunicaciones como el teléfono, el correo electrónico o el control de otras computadoras remotas.

- **Lammer** a este grupo pertenecen aquellas personas deseosas de alcanzar el nivel de un hacker, pero su poca formación y sus conocimientos, les impiden realizar este sueño. Su trabajo se reduce a ejecutar programas creados por otros, a bajar, en forma indiscriminada, cualquier tipo de programa público en la red.
- **Copyhacker** son una nueva generación de falsificadores dedicados al "crackeo" de hardware, especialmente en el sector de tarjetas inteligentes. Su estrategia radica en establecer amistad con los verdaderos Hackers, para copiarles los métodos de ruptura, y después venderlos a los bucaneros.
- **Los copyhackers** se interesan por poseer conocimientos de tecnología, son aficionados a las revistas técnicas y a leer todo lo que hay en la red. Su principal motivación es el dinero.
- **Indica que Bucaneros** son los comerciantes de la red, mas no existen en ella; aunque no poseen ningún tipo de información en el área de los sistemas, si poseen un amplio conocimiento en el área de negocios.
- **Phreaker** se caracterizan por poseer vastos conocimientos en el área de telefonía terrestre, móvil, hibrida, etc. incluso poseen más información que los propios técnicos de las compañías telefónicas; recientemente con el auge de los teléfonos celulares, han tenido que ingresar también al mundo de la información y del procesamiento de datos.
- **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 programas de hackeo, baja todo lo que puede y empieza a trabajar con ello.
- **Script Kiddie** denominados también "skid kiddie", son simples usuarios de internet, sin conocimientos sobre Hack o Crack, aunque aficionados a estos temas, no los comprenden realmente, simplemente son internautas que se limitan a recopilar información de la red y a buscar programas que luego ejecutan sin los más mínimos conocimientos, infectando en algunos casos de virus sus propios equipos.

Los hackers están enfocados a quebrantar, vulnerar y crear accesos para ingresar a los sistemas informáticos que tienen las entidades, mediante el cual realizan delitos informáticos (computacionales), robando información confidencial mediante mecanismos creados por hackers expertos, como lo manifiestan en los párrafos anteriores tenemos una gran variedad de tipos de hackers los cuales manejan diferentes métodos para ejecutar en los sistemas informáticos y obtener provecho de su trabajo con el fin de recuperar datos que son muy valiosos para realizar fechorías y daño con la información

recolectada de diferentes usuarios que se manejan desde un sistema de cómputo, de este modo su objetivo principal es realizar estafas mediante los datos robados.

Spoofing Y Sniffing

(Laudon Kanneth & Laudon Jane, 2006, pág. 299) Con frecuencia, los hackers que intentan ocultar sus verdades identidades utilizan direcciones de correo falsas o se hacen pasar por alguien más.

- **Spoofing:** también puede implicar el hecho de redirigir un vínculo Web a una dirección distinta de la que se tenía pensada, en donde el sitio se hace pasar por el destino esperado. Por ejemplo, si los hackers redirigen a los clientes a un sitio Web falso que se ve casi igual que el sitio verdadero, pueden recolectar y procesar pedidos para robar de manera efectiva la información de negocios, así como la información confidencial de los clientes de sitio verdadero.
- **Un husmeador (sniffer):** es un tipo de programa espía que monitorea la información que viaja a través de una red. Cuando se utiliza de manera legítima, los husmeadores ayudan a identificar los potenciales puntos problemáticos en las redes o la actividad criminal en las mismas, pero cuando se usan para fines criminales pueden ser dañinos y muy difíciles de detectar.

Su intención es el robo de información confidencial de personas en las cuales su objetivo es pedir información privada y así poder ejecutar con la misma provocando daños, por otro lado, son de uso delictivo para generar hurto.

2.14. Control Interno COSO

Es:

> El control interno se define como un proceso, efectuado por el personal de una entidad, diseñado para conseguir unos objetivos específicos. La definición es amplia y cubre todos los aspectos de control de un negocio, pero al mismo tiempo permite centrarse en objetivos específicos. El control interno consta de cinco componentes relacionados entre sí que son inherentes al estilo de gestión de la

> empresa. Estos componentes están vinculados entre si y sirven como criterios para determinar si el sistema es eficaz. (Lybrand Coopers, 1997)

El control interno nos permite análisis integrado de todas las actividades sean estas operacionales y de administración que tiene la entidad en la cual podemos prevenir riesgos que se pueden presentar en un futuro.

2.14.1. Objetivos del control interno.

> (Estupiñan Gaitan Rodrigo, 2015, pág. 19) El control interno comprende el plan de organización y el conjunto de métodos y procedimientos que aseguren que los activos están debidamente protegidos, que los registros contables son fidedignos y que la actividad de la entidad se desarrolle eficazmente según las directrices marcadas por la administración.
>
> - De acuerdo a lo anterior los objetivos básicos son:
> - Proteger los activos y salvaguardar los bienes de la institución
> - Verificar la razonabilidad y confiabilidad de los informes contables y administrativos
> - Promover la adhesión a las políticas administrativas establecidas
> - Lograr el cumplimiento de las metas y objetivos programados.

El objetivo principal del control interno es salvaguardar y la protección los activos de la entidad y verificar que todos los procesos desarrollados en la entidad contengan un adecuado seguimiento, enfocándonos a la política de la organización, cumpliendo metas trazadas por la misma.

2.14.2. Beneficios de control interno.

> Nos indica (La Contraloria General del Estado, s.f.) Seguridad razonable de:
>
> - Reducir los riesgos de corrupción
> - Lograr los objetivos y metas establecidos
> - Promover el desarrollo organizacional
> - Lograr mayor eficiencia, eficacia y transparencia en las operaciones
> - Asegurar el cumplimiento del marco normativo

- Proteger los recursos y bienes del Estado, y el adecuado uso de los mismos
- Contar con información confiable y oportuna
- Fomentar la práctica de valores
- Promover la rendición de cuentas de los funcionarios por la misión y objetivos encargados y el uso de los bienes y recursos asignados

2.14.3. Componentes del Control Interno.

Al contar con un adecuado control interno dentro de la organización como resultado tenemos un control adecuado y preciso de esta forma minimizamos todo tipo de riesgo que se puede presentar en la entidad, cumpliremos metas y objetivos que son planteados por la misma, como también se da una confianza de trasparencia en todas las operaciones que realizamos y de esta manera se puede decir que el control interno es de mucha importancia en las entidades ya que nos permite tomar el control de la misma.

2.14.4. Elementos de control interno.

- **Entorno de Control**

El entorno de control se refiere a la forma en la que una organización trabaja, e influye en el comportamiento de las personas; en tanto es el factor primordial que proporciona disciplina y estructura. La ausencia de un entorno de control conveniente ha ocasionado enormes fracasos empresariales.

- **Evaluación de los riesgos**

Es el análisis de la organización ante posibles riesgos que están expuestos o se pueden enfrentar para esto se establecen mecanismo para cada tipo de riesgo, se trazan objetivos para cada departamento y que estos vayan de la mano.

- **Actividades de control**

En este componente se establecen procedimientos manuales con el objetivo de tener una seguridad, con acciones eficaces para poder enfrentar riesgos que se presentan para cumplir con los objetivos establecidos.

- **Información y comunicación**

El personal que labora en la organización debe informar y comunicar de todos los acontecimientos, para llevar un adecuado desarrollo y control en sus actividades operacionales.

- **Supervisión**

Es de gran importancia la supervisión para llevar a cabo el proceso adecuado en actividades, con el fin de que si pasa un acontecimiento se puedan presentar cambios y que reaccionen de cuerdo a la modificación que sea necesaria.

2.14.5. Limitaciones del Control Interno.

Las limitaciones del control interno hacen referencia a los acontecimientos que no pueden ser controlados por medio de la auditoría interna.

El objetivo del control interno es la salvaguardar los activos de la empresa; por lo tanto, la supervisión de este departamento de calidad es responsabilidad de la administración, y su evaluación es de auditoría externa; el control interno, que especificamente va

orientado a la protección de los activos de la organización, como también a la verificación de la información y procesos.

Elementos fundamentales del control interno informático (Muñoz Razo Carlos, 2002, pág. 135)

- Controles internos sobre la organización del área de informática
- Controles internos sobre el análisis, desarrollo e implementación de sistemas.
- Controles internos sobre la operación del sistema
- Controles internos sobre los procedimientos de entrada de datos, el procesamiento de información y la emisión de resultados
- Controles internos sobre la seguridad del área de sistemas

El control es un instrumento que nos permite observar cómo se manejan todas las operaciones que realiza la entidad en el departamento de sistemas de esta manera logramos comprobar si se cumplen con todos los procedimientos al momento de realizar operaciones y como resultado tendremos un adecuado manejo informático.

2.15. Cobit

> Según (CIBERTEC , s.f.) COBIT es el marco aceptado internacionalmente como una buena práctica para el control de la información, TI y los riesgos que conllevan. Se utiliza para implementar el gobierno de IT y mejorar los controles de IT. Contiene objetivos de control, directivas de aseguramiento, medidas de desempeño y resultados, factores críticos de éxito y modelos de madurez.

Lo que nos indica el autor sobre Cobit es una herramienta que ayuda mucho a todas las empresas a llevar un excelente manejo y de esta manera estamos controlando la información que posee la entidad.

2.15.1. Principios de COBIT

Según (Osores Melisa, 2014) en su publicación indica los siguientes principios:

- **Satisfacer las necesidades de los colaboradores.** Es crítico definir y vincular los objetivos empresariales y los objetivos relacionados con TI.
- **Cubrir la empresa de extremo a extremo.** Las compañías deben cambiar de visión, con el objetivo de considerar el área de TI como un activo y no un costo.
- **Aplicar un solo marco integrado.** Usar un solo marco de gobierno integrado puede ayudar a las organizaciones a brindar valor óptimo de sus activos y recursos de TI.
- **Habilitar un enfoque holístico.** El gobierno de TI empresarial (GEIT) requiere de un enfoque holístico que tome en cuenta muchos componentes, también conocidos como habilitadores.
- **Separar al gobierno de la administración.** Los procesos de gobierno aseguran que los objetivos se alcancen mediante la evaluación de las necesidades de los interesados, el establecimiento de la dirección a través de la priorización y la toma de decisiones; y el monitoreo del desempeño, el cumplimiento y el progreso.

Los principios citados son de mucha importancia por lo que ayuda a la empresa a tomar mejores decisiones con respecto a TI, con el objetivo que todos estemos direccionados en un único camino y saber a donde debemos llegar, optimizando los costes de TIC así la empresa debe tomar en cuenta que el área de TIC no representaría un costo más bien vendría hacer un activo con mucho valor ya que si manejamos adecuadamente.

2.16. Marco Legal

2.16.1. Garantías Constitucionales.

Según (Constitución de la República del Ecuador, 2008):

> El Estado fomentará la pluralidad y la diversidad en la comunicación, y al efecto: Facilitará la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de información y comunicación en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada.
> Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o

> privadas, en soporte material o electrónico. Así mismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. (Constitución de la República del Ecuador, Garantías constitucionales Capitulo VIII Articulo 16, 2011)
>
> La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados. (Constitución de la República del Ecuador, Garantías constitucionales Capitulo VIII Articulo 16, 2011)

Todo lo establecido en la Constitución del Ecuador se convierte en garantías dentro del marco legal que se aprobó en el año 2008, que garantiza a todos los ecuatorianos tener el libre derecho de conocer, acceder a información que manejan entidades públicas y privadas según nos indica la presente ley.

2.16.2. Código Orgánico Integral Penal.

Según (Código Organico Integral Penal Delitos contra la información Art.22, 2014) menciona que:

“El empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad”.

Código Obtención y utilización no autorizada de información

Según (Código Organico Integral Penal Delitos contra la información Art.22, 2014) manifiesta que “La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares”.

Con el Código Orgánico Integral Penal se asegura la información personal de persona, empresa para no ser violentadas con el robo de información confidencial por lo tanto el presente Código da sentencia a las personas que tiene obtienen provecho de los delitos informáticos.

Falsificación Electrónica

> Se menciona que son reos de falsificación electrónica la persona o personas que con el ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático. (Ley Comercio Electrónico, Código Organico IntegralPenal Art. 353, 2014)

Tienen un propósito el de lucro por medio de la falsificación causando daño a tercera persona utilizando medios electrónicos, tergiversando datos o información relevante.

Daños Informáticos

Según (Ley Comercio Electrónico, Código Organico IntegralPenal Art. 415, 2014) menciona que:

“El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, utilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos contenido en un sistema de información o red electrónica”.

Apropiación Ilícita

> Los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuraren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos. (Ley Comercio Electrónico, Código Organico IntegralPenal Art. 552, 2014)

La apropiación ilícita consta de adueñarse de un bien ajeno utilizando mecanismos engañosos con el fin de hacer daño a terceras personas como resultado de la manipulación de los sistemas tecnológicos.

Según (Ley General de Instituciones del Sistema Financiero, 2001) menciona en los siguientes artículos:

> **Art. 1.-** (Reformado por la disposición reformatoria primera de la Ley 2001-55, R.O. 465-S, 30-XI-2001).- Esta ley regula la creación, organización, actividades, funcionamiento y extinción de las instituciones del sistema financiero privado, así como la organización y funciones de la Superintendencia de Bancos y Seguros, en la órbita de su competencia, entidad encargada de la supervisión y control del sistema financiero, en todo lo cual se tiene presente la protección de los intereses del público. En el texto de esta ley la Superintendencia de Bancos y Seguros, en la órbita de su competencia, se llamará abreviadamente "la Superintendencia".
> Las instituciones financieras públicas, las compañías de seguros y de reaseguros se rigen por sus propias leyes en lo relativo a su creación, actividades, funcionamiento y organización. Se someterán a esta ley en lo relacionado a la aplicación de normas de solvencia y prudencia financiera y al control y vigilancia que realizará la Superintendencia dentro del marco legal que regula a estas instituciones en todo cuanto fuere aplicable según su naturaleza jurídica. La Superintendencia aplicará las normas que esta ley contiene sobre liquidación forzosa, cuando existan causales que así lo ameriten.

> **Art. 2.-** Para los propósitos de esta ley, son instituciones financieras privadas los bancos, las sociedades financieras o corporaciones de inversión y desarrollo, las asociaciones mutualistas de ahorro y crédito para la vivienda y las cooperativas de ahorro y crédito que realizan intermediación financiera con el público. Los bancos y las sociedades financieras o corporaciones de inversión y desarrollo se caracterizan principalmente por ser intermediarios en el mercado financiero, en el cual actúan de manera habitual, captando recursos del público para obtener fondos a través de depósitos o cualquier otra forma de captación, con el objeto de utilizar los recursos así obtenidos, total o parcialmente, en operaciones de crédito e inversión.

Las instituciones financieras son entidades de intermediación financiera que se rigen a la presente ley quien regula y controla sus actividades con el propósito de proteger los intereses del público, promoviendo el desarrollo económico del país.

Según (Constitucion de la Republica del Ecuador. Art. 308, 2008)

> Las actividades financieras son un servicio de orden público, y podrán ejercerse, previa autorización del Estado, de acuerdo con la ley; tendrán la finalidad fundamental de preservar los depósitos y atender los requerimientos de financiamiento para la consecución de los objetivos de desarrollo del país. Las actividades financieras intermediarán de forma eficiente los recursos captados para fortalecer la inversión productiva nacional, y el consumo social y ambientalmente responsable.

Ibídem

La Constitución de la República del Ecuador en su Art. 302, dice:

Las políticas monetarias, cambiarias y financieras tendrán como objetivos:

- Suministrar los medios de pago necesarios para que el sistema económico opere con eficiencia.
- Establecer niveles de liquidez global que garanticen adecuados márgenes de seguridad financiera.
- Orientar los excedentes de liquidez hacia la inversión requerida para el desarrollo del país.

- Promover niveles y relaciones entre las tasas de interés, pasivas y activas que estimulen el ahorro nacional y el financiamiento de las actividades
- Productivas, con el propósito de mantener la estabilidad de precios y los equilibrios monetarios en la balanza de pagos, de acuerdo al objetivo de estabilidad económica definido en la Constitución.

Las actividades financieras es un conjunto de operaciones económicas que nos ayudan a salvaguardar los depósitos, a fortalecer la inversión nacional para una mayor competitividad en el sistema financiero, con la finalidad de obtener una estabilidad económica en el país.

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

El proyecto será ejecutado en la provincia de Cotopaxi específicamente en las empresas del sector de servicios reguladas por las Superintendencias de Compañías y Superintendencia de Economía Popular y Solidaria, en la cual nos enfocamos en el servicio de intermediación financiera por parte de las instituciones financieras como también en la Clasificación Industrial Internacional Uniforme (CIIU) inciso K. Donde por el nivel de atención y actividad a que se dediquen, deben poseer un almacenamiento de la información y de su seguridad al cien por ciento, siendo el sector de servicios como una de las actividades de mayor aporte en el desarrollo económico de nuestra provincia y nivel nacional, actualmente existen empresas que se dedican principalmente a las actividades del sector servicios: hoteles y restaurantes; transporte, almacenamiento y comunicaciones; e intermediación financiera; seguros, educación.

Con la finalidad de evaluar, analizar e interpretar cual es la seguridad que poseen las entidades de servicios al momento de salvaguardar los datos Informáticos reguladas por las superintendencias de bancos y compañías, así como también para asegurar aquellos recursos que estén expuestos para un posible fraude por parte de personas internas como externas de la organización.

Por lo tanto en el desarrollo de nuestra investigación utilizaremos un procedimiento adecuado como es el tipo y diseños de investigación para llegar con un claro conocimiento a los que respecta población y muestra, dentro de ello tenemos las técnicas e instrumentos de recolección de datos para entrar en un análisis adecuado para la presente investigación.

La investigación se basa en un análisis cuantitativo está orientado al resultado por lo que trabajaremos con datos numéricos montos de inversión de esta manera analizaremos niveles de medición y su comportamiento en el tiempo, con este tipo de análisis nosotros como investigadores podremos definir el problema que puede existir en cada entidad de servicios observando su nivel de inversión durante los periodos 2012 - 2016 en la cuenta equipo de cómputo y software.

Cualitativo está orientado al proceso cuando desde el punto de vista investigativo al aplicar los exámenes especiales tanto de auditoría informática como de forense hemos visto la percepción que tiene la gente. El análisis cualitativo en la presente investigación se fija en cuáles son las características de un fenómeno y la relación con la calidad que se emplea en el cuidado sobre las bases de datos de las entidades de servicios.

3.1. Tipos y diseños de investigación

3.1.1. Tipos de investigación.

a. La investigación histórica.

> (Tesis de Investigadores, 2011) Define investigación histórica que: Se trata de la experiencia pasada, describe lo que era y representa una búsqueda crítica de la verdad que sustenta los acontecimientos pasados. El investigador depende de fuentes primarias y secundarias las cuales proveen la información y a las cuáles el investigador deberá examinar cuidadosamente con el fin de determinar su confiabilidad por medio de una crítica interna y externa. En el primer caso verifica la autenticidad de un documento o vestigio y en el segundo, determina el significado y la validez de los datos que contiene el documento que se considera auténtico.

Este tipo de investigación trata de hechos pasados que sucedieron en algún momento en el cual sirven como sucesos que pueden presentarse en un futuro, para comprobar este tipo de información que sucedió en hechos pasados debemos tener la certeza y

cuidadosamente tratar la información recolectada en fuentes primarias, secundarias ya que nos servirá de mucho para el desarrollo del mismo.

b. La investigación descriptiva.

Ibídem**,** “Trabaja sobre realidades de hecho y su característica fundamental es la de presentar una interpretación correcta. Esta puede incluir los siguientes tipos de estudios: Encuestas, Casos, Exploratorios, Causales, De Desarrollo, Predictivos, De Conjuntos, De Correlación”.

Trabajamos con herramientas para verificar si existe algún tipo de causa en el medio por lo que es aconsejable tratar con encuestas para verificar cuales son los resultados que nos proyecta la investigación.

c. Investigación Documental.

Según (Arias Fidias G, 2012 , pág. 27) define:

> La investigación documental es un proceso basado en la búsqueda, recuperación, análisis, crítica e interpretación de datos secundarios, es decir, los obtenidos y registrados por otros investigadores en fuentes documentales: impresas, audiovisuales o electrónicas. Como en toda investigación, el propósito de este diseño es el aporte de nuevos conocimientos.

Para (Moreno Bayardo María Guadalupe, pág. 41) “La investigación documental reúne la información necesaria recurriendo fundamentalmente a fuentes de datos en los que la información ya se encuentra registrada, tales como libros, revistas especializadas, películas, archivos, videocasetes, estadísticas, informes de investigación ya realizados, etc.”.

Según (Baena Guillermina, 1985, pág. 72) “La investigación documental es una técnica que consiste en la selección y recopilación de información por medio de la lectura y critica

de documentos y materiales bibliográficos, de bibliotecas, hemerotecas, centros de documentación e información.”

La investigación documental nos ayuda a obtener distinto tipo de información relevante que se encuentra en diferentes tipos de archivos pueden ser físicos y digitales, por lo tanto, es preciso revisar documentos como libros, revistas, leyes, archivos históricos, con el fin de obtener mayor información que nos permita desarrollar la investigación de manera correcta.

Fuentes de información en la investigación documental

Según (Martinez Catherine, 2017) nos indica las principales fuentes de información utilizadas en la investigación documental:

- **Materiales impresos** (libros, periódicos, diarios, las tesis, los proyectos de investigación.
- **Materiales electrónicos** (revistas y libros especializados que solo se publican en formato digital y que constituyen fuentes valiosas de información).
- **Materiales gráficos** (Las fotografías y las pinturas constituyen fuentes de información, los mapas y los planos).
- **Materiales audiovisuales** (grabaciones y los archivos de audio y/o vídeo de noticieros, entrevistas, ponencias, conferencias).

Las fuentes de información para el desarrollo de la investigación de campo se ve registrada en diferente tipos de materiales como son físicos en este caso hablamos de libros, periódicos, revistas como también existen materiales electrónicos que se puede tener acceso por medio de un computador son de mucha importancia por tal motivo en este tipo de investigación toda información es indispensable para el desarrollo del mismo.

d. Investigación de campo.

> (Arias Fidias G, 2012 , pág. 31) La investigación de campo es aquella que consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variable alguna, es decir, el investigador obtiene la información, pero no altera las condiciones existentes. De allí su carácter de investigación no experimental.

Según (Falella Santa: Martins Feliberto, 2012, pág. 88) en su libro Metodología de la investigación cuantitativa menciona:

> La Investigación de campo consiste en la recolección de datos directamente de la realidad donde ocurren los hechos, sin manipular o controlar las variables. Estudia los fenómenos sociales en su ambiente natural. El investigador no manipula variables debido a que esto hace perder el ambiente de naturalidad en el cual se manifiesta y desenvuelve el hecho.
> La investigación de campo otorga validez y viabilidad ya que se trabaja en el lugar donde sucedieron los hechos reales permitiendo conocer de manera directa los problemas informáticos en las empresas del sector de servicios reguladas por las superintendencias de bancos y compañías, este tipo de investigación es de gran aporte para el investigador ya que nos permite el analizar, verificar y conocer los datos con más seguridad.

Tipos de investigación de campo

Según (La investigación de campo. Bogotá: E-Cultura Group, 2016)**:**

- **Investigación de Campo Exploratoria:** se basa en un tipo de investigación, en la cual el investigador acude directamente al ámbito en donde se desarrolla o produce el fenómeno, a fin de hacer una aproximación de tipo exploratoria, en donde trata de explicar y describir los elementos o características vistas a simple vista, con el objetivo de identificar algún tipo de patrón que ayude a su estudio a realizar predicciones con respecto al comportamiento del objeto de estudio.
- **Investigación de Campo enfocada a la verificación de hipótesis:** por su parte, en este tipo de investigación, el estudioso o investigador se enfrenta con el contexto del objeto de estudio, a fin de establecer las relaciones que pueden existir entre las diferentes variables, con el objetivo de encontrar una explicación al comportamiento del fenómeno que estudia.

La investigación de campo exploratoria está relacionada directamente donde ocurren los hechos o acontecimiento, en el cual el autor debe presentarse en el lugar donde se presentaron los fenómenos. El autor debe tener muy claro las variables de estudio para tener una explicación clara, precisa y veraz.

3.1.2. Diseño de la investigación.

> Según (Roldán, 2018) “El diseño de investigación constituye el plan general del investigador para obtener respuestas a sus interrogantes o comprobar la hipótesis de investigación. El diseño de investigación desglosa las estrategias básicas que el investigador adopta para generar información exacta e interpretable. Los diseños son estrategias con las que intentamos obtener respuestas a preguntas como:
> - Contar.
> - Medir.
> - Describir.

El diseño de investigación permite guiarse de acuerdo a un cronograma que es desarrollado por el investigador con el cual se puede obtener respuesta clara y precisa a cada duda o interrogante que se presente de acuerdo al tema de investigación.

Clasificación de los estudios de investigación.

Ibídem,

- Diseños experimentales. En ellos el investigador desea comprobar los efectos de una intervención específica, en este caso el investigador tiene un papel activo, pues lleva a cabo una intervención.
- Diseños no experimentales. En ellos el investigador observa los fenómenos tal y como ocurren naturalmente, sin intervenir en su desarrollo.

Estudios cuantitativos tienden a ser altamente estructurados, de modo que el investigador especifica las características principales del diseño antes de obtener un solo dato.

Por el contrario, el diseño de los estudios cualitativos es más flexible; permite e incluso estimula la realización de ajustes, a fin de sacar provecho a la información reunida en las fases tempranas de su realización.

3.2. Población y muestra

3.2.1. Población.

Según (Tamayo Mario, El proceso de la Investigacion Cientifica, 1997, pág. 28) “La población se define como la totalidad del fenómeno a estudiar donde la unidad de población posee una característica común la cual se estudia y da origen a los datos de la investigación”.

Define (Fidias Arias G, 2006, pág. 81) “La población es un conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación. Ésta queda delimitada por el problema y los objetivos del estudio.”

En la investigación nuestra población se consideran todas las empresas que están dentro de la actividad de servicios en la provincia de Cotopaxi, que se encuentran bajo regulación de la Superintendencia de Compañías y la Superintendencia de Economía Popular y Solidaria (SEPS), SUPER CIAS por lo tanto son empresas que son netamente constituidas dentro de la provincia, excluyendo empresas que están dentro de la provincia como sucursales y que no son constituidas dentro de la misma.

Tabla 7

Empresas de servicios reguladas por la Superintendencia de Compañías y la Superintendencia de Economía Popular y Solidaria (SEPS), en la Provincia de Cotopaxi.

CANTONES	# DE EMPRESAS CIIU Y SEPS	
	CIIU	SEPS
Latacunga	405	33
La Maná	22	3
Pangua	13	2
Pujilí	31	3
Salcedo	56	15
Saquisilí	24	2
Sigchos	9	2
Total 7 Cantones	560	60

3.2.2. Muestra.

> Según (Tamayo Mario, El proceso de la Investigacion Cientifica, 1997, pág. 29): La muestra es la que puede determinar la problemática ya que es capaz de generar los datos con los cuales se identifican las fallas dentro del proceso. Afirma que la muestra es el grupo de individuos que se toma de la población, para estudiar un fenómeno estadístico.

Al seleccionar la muestra se estudiará una parte o un subconjunto de la población, por lo tanto para el desarrollo de la investigación se obtendrá la respectiva información de una parte del universo con su respectiva información aportando de manera clara y precisa con la obtención de los Balances Generales y Estados Financieros del periodo 2012 – 2016 por parte de los investigadores en las empresas del sector servicios reguladas por

la Superintendencia de Compañías y la Superintendencia de Economía Popular y Solidaria en la Provincia de Cotopaxi.

a. Muestra intencional.

> Muestra Intencional o Discrecional. (QuestionPro, s.f.) Una muestra intencional o por juicio es aquella que se selecciona en base al conocimiento de una población o propósito del estudio. Por ejemplo, cuando sociólogos quieren estudiar los efectos emocionales y psicológicos a largo plazo de la terminación de un embarazo, se puede crear una muestra que incluya solamente a mujeres que se habían sometido a un aborto. En este caso, los investigadores pueden utilizar una muestra intencional porque los entrevistados cumplen con una descripción o propósito específico que es necesario para realizar la investigación.

La población para nuestro estudio está conformada de 620 empresas de servicios constituidas en la provincia de Cotopaxi, para extraer la muestra en dicha investigación aplicamos la muestra intencional que para el caso de estudio permite verificar si disponen de la cuenta Equipo de Cómputo dentro del Balance General o en los Estados Financieros con su respectiva inversión en caso de no contar con la cuenta Equipo de Cómputo y no tener ningún tipo de inversión estas empresas serán excluidas para nuestra muestra, contando con un total de 19 empresas reguladas bajo la Superintendencia de Economía Popular y Solidaria y 2 bajo la supervisión de la Superintendencia de Compañías.

Tabla 8

Empresas de servicios reguladas por la Superintendencia de Economía Popular y Solidaria en la Provincia de Cotopaxi.

RUC	RAZÓN SOCIAL	VALOR
0590024937001	EDUCADORES PRIMARIOS DEL COTOPAXI	111.877,61
0590052000001	DE LA PEQUEÑA EMPRESA DE COTOPAXI LTDA	1.234.952,88
0590060437001	SAN MIGUEL DE SIGCHOS	3.065,30
0590060461001	UNION MERCEDARIA LTDA	17.117,04

CONTINÚA

0590061123001	FUTURO LAMANENSE	58.730,43
0591711563001	SUMAK KAWSAY LTDA	66.002,49
0591712470001	PILAHUIN	29.781,72
0591713124001	15 DE AGOSTO DE PILACOTO	16. 754,7
0591714031001	ILINIZA LTDA	30.104,16
0591714236001	UNIBLOCK Y SERVICIOS LTDA	11.560,43
0591714333001	COORCOTOPAXI LTDA	22.515,46
0591714821001	PUCARA LTDA	11.283,90
0591715011001	SINCHI RUNA LTDA	15.031,06
0591715356001	SANTA ROSA DE PATUTAN LTDA	9.733,07
0591718878001	INTEGRACION SOLIDARIA LTDA	48.968,50
0591719009001	SIERRA CENTRO LTDA	138.358,50
0591719718001	VISION DE LOS ANDES VISANDES	111.638,68
1791422708001	UNIDAD Y PROGRESO	22.770,86
1791430956001	HERMES GAIBOR VERDESOTO	25.419,62

Tabla 9

Empresas de servicios reguladas por la Superintendencia de Compañías en la Provincia de Cotopaxi

RUC	RAZÓN SOCIAL	VALOR
1891741983001	CENTRO DE DIALISIS CONTIGO CENDIALCON CIA. LTDA.	18.979,52
0590035025001	LA CIENEGA C LTDA	42.563,41

CONTINÚA

3.3. Técnicas e Instrumentos de recolección de datos

Para desarrollar nuestra investigación haremos uso de la encuesta ya que nos ayudara a formular preguntas claves de acuerdo a nuestro caso con el fin de medir las variables de la investigación.

Según (Mendez Carlos, 199, pág. 143) menciona: “que las fuentes y técnicas para recolección de la información como los hechos o documentos a los que acude el investigador y que le permiten tener información”.

El uso de diversas técnicas y herramientas nos ayuda a buscar información que será útil, completa, veraz, sintetizada para un mejor desarrollo de nuestra investigación.

- **Encuesta**

Según (Rodriguez U Manuel Luis, 2010) La encuesta es un “Método de investigación capaz de dar respuestas a problemas tanto en términos descriptivos como de relación de variables, tras la recogida de información sistemática, según un diseño previamente establecido que asegure el rigor de la información obtenida”.

(García Córdoba Fernando, 2004, pág. 20) “Una encuesta sirve para recopilar datos, como conocimientos ideas y opiniones de grupos; aspectos que analizan con el propósito de determinar rasgos de las personas, proponer o establecer relación entre las características de los sujetos, lugares y situaciones o hechos.”

La opinión de los autores nos indica que la encuesta es una técnica con un propósito de obtener, recopilar datos e información a través de diferentes opiniones de acuerdo al ámbito de aplicación con el objetivo de dar respuesta a cada problema que se presenta.

Objetivo de la encuesta

> (García Córdoba Fernando, 2004, pág. 20) Obtener información relativa a las características predominantes de una población mediante la aplicación de procesos de interrogación y registro de datos. Cuando la encuesta se realiza mediante la aplicación de cuestionarios, se puede conseguir principalmente información demográfica, opiniones y conocimientos de los sujetos respecto a un asunto, situación, tema o personas.

A través de la encuesta obtenemos resultados relevantes de una población lo cual nos permite cumplir con los objetivos planteados en nuestra investigación y dar solución a los problemas que se presentan al finalizar dicha investigación.

3.3.1. Instrumento de Investigación.

Esta investigación se basa en un análisis cuantitativo por lo que trabajaremos con datos numéricos de esta manera analizaremos niveles de medición y su comportamiento en el tiempo, con este tipo de análisis nosotros como investigadores podremos definir el problema que puede existir en cada entidad de servicios observando su nivel de inversión.

Como instrumento de acuerdo a nuestra investigación haremos uso del cuestionario ya que en el mismo se encontrarán preguntas abiertas, cerradas y de escala.

- **Cuestionario**

Según (García Córdoba Fernando, 2004, pág. 29) “El cuestionario permite la recolección de datos provenientes de fuentes primarias, es decir, de personas que poseen la información que resulta de interés.”

Como lo menciona el autor el cuestionario es de gran aporte para el desarrollo de la investigación ya que a través del mismo obtenemos información confiable de la fuente primaria.

Objetivo del cuestionario

- Preguntas claves de acuerdo al planteamiento del problema
- Desarrollar un instrumento claro y preciso que nos permita obtener respuestas veraces.

Fuentes primarias

Las fuentes primeras son documentos que ofrecen evidencia directa del objeto de estudio por lo tanto para nuestra investigación utilizaremos entrevistas y encuestas que serán aplicadas al sector servicios ya que es nuestro campo de estudio.

Fuentes Secundarias

- Revisión documental bibliográfica
- Instituto Nacional de Estadísticas y Censos
- Proyectos de investigación similares
- Papers – Artículos científicos

3.4. Diseño de la encuesta

La herramienta que utilizaremos para el desarrollo de nuestra investigación es la encuesta ya que por medio de ella se plantean preguntas que están enfocadas de acuerdo a los objetivos presentes de nuestro tema a desarrollar, con la finalidad de obtener resultados claros y confiables.

Es de mucha importancia la aplicación de la encuesta ya que tiene una finalidad relevante que es la recopilar datos e información muy detallada, ya que proviene de personas que poseen información veraz y oportuna ya que a través de ella podemos observar, detectar problemas que se presentan en el medio de estudio ya sea en el ámbito social, político y económico con el propósito de dar solución a todas las falencias encontradas después de aplicar dicho instrumento. Una vez aplicada nuestra encuesta en todas las empresas del sector servicios reguladas por la Superintendencia de Compañías y la Superintendencia de Economía Popular y Solidaria en la Provincia de Cotopaxi procedemos a tabular con su respectivo análisis e interpretación con el fin de descubrir los hechos más relevantes que se hicieron presentes.

3.4.1. Modelo de encuesta.

ENCUESTA DIRIGIDA A LAS ENTIDADES DEL SECTOR SERVICIOS EN LA PROVINCIA DE COTOPAXI

Objetivo:
Conocer sobre la vulnerabilidad con respecto a los fraudes informáticos en las Empresas del sector servicios reguladas por la Superintendencia de Economía Popular y Solidaria y Superintendencia de Compañías en la provincia de Cotopaxi en el periodo 2012 - 2016”

Instrucciones:

- Lea las instrucciones de cada pregunta con atención y luego marque con una X el contenido que usted crea correcto.

1. ¿De que tamaño es su empresa?	**2. ¿Ha implementado tecnología o sistemas de información y comunicación dentro de la empresa?**
☐ 1.1. Grande (Ventas Totales: > $ 5.000.000) ☐ 1.2. Mediana (Ventas Totales: $ 1.000.001 - $ 5.000.000) ☐ 1.3. Pequeña (Ventas Totales: $ 100.001 - $ 1.000.000) ☐ 1.4. Microempresa (Ventas Totales: ≤ $ 1.00.000)	☐ 2.1. Último mes ☐ 2.2. Último trimestre ☐ 2.3. Último semestre ☐ 2.4. Último año ☐ 2.5. Último 4 años
3. ¿A que actividad de servicios se dedica su empresa?	**4. ¿Considerando la respuesta que usted dio en la pregunta anterior qué tipo de inversión es más representativa para la empresa en tecnología de información y comunicación seleccione una de ellas?**
☐ 3.1. Servicios administrativo y de apoyo ☐ 3.2. Salud ☐ 3.3. Instituciones, agencias y servicios financieros ☐ 3.4. Alojamiento ☐ 3.5. Educacion	☐ 4.1. Mantenimiento de equipo ☐ 4.2. Compra de equipo ☐ 4.3. Compra de software ☐ 4.4. Capacitación de personal ☐ 4.5. Licencias y patentes informáticas

5. ¿Desde su perspectiva, que importancia tiene la utilización del recuerso tecnológico para mejorar la productividad, calidad, control y comunicación dentro de las empresas servicios?	**6. ¿Cuánto estima usted que ha invertido en Tecnología de Información y Comunicación (TIC) durante el periodo 2012 - 2016?**
☐ 5.1. Alto ☐ 5.2. Medio ☐ 5.3. Bajo	☐ 6.1. De 0.000 a 10.000 dólares ☐ 6.2. De 10.000 a 20.000 dólares ☐ 6.3. De 20.000 a 30.000 dólares ☐ 6.4. De 30.000 a 40.000 dólares ☐ 6.5. De 40.000 a 50.000 dòlares ☐ 6.6. Màs de 50.000 dòlares
7. ¿Considera usted que los recursos tecnológicos favorecen la operatividad de la empresa, como un medio para optimizar recursos?	**8. ¿Qué tipo de software contable maneja la entidad?**
☐ 7.1. Si ☐ 7.2. No	☐ 8.1. ZEUS Sistema Administrativo ☐ 8.2. SIGA Software Integrado de Gestión Académica ☐ 8.3. SAELINEA Sistema de Apoyo a Entidades Educativas ☐ 8.4. Otros
9. ¿Con què frecuencia la empresa contrata un servicio técnico especializado en Tecnología de Información y Comunicación (TIC)?	**10. ¿Qué mòdulos tiene sus sitemas informaticos en la entidad?**
☐ 9.1. Mensual ☐ 9.2. Trimestral ☐ 9.3. Semestral ☐ 9.4. Anual ☐ 9.5. Nunca	☐ 10.1. ERP (Planificación de Recursos Empresariales) ☐ 10.2. CRM (Gestión de Servicio al Cliente) ☐ 10.3. SIAF (Sistema de Información y Adm. Financiera) ☐ 10.4. SAP (Sistemas, Aplicaciones y Productos)
11. ¿Cuántas computadoras posee su empresa?	**12. ¿Hasta cuánto podría presupuestar por un sistema informático de protección de datos?**
☐ 11.1. De 1 a 5	☐ 12.1. 0.000 a 10.000 dólares

☐ 11.2. De 5 a 10 ☐ 11.3. De 10 a 15 ☐ 11.4. De 15 a 20 ☐ 11.5. Más de 20	☐ 12.2. 10.000 a 20.000 dólares ☐ 12.3. 20.000 a 30.000 dólares ☐ 12.4. 30.000 a 40.000 dòlares ☐ 12.5. 40.000 a 50.000 dòlares ☐ 12.6. Màs de 50.000 dòlares
13. ¿Cuántas personas empleadas en su empresa utilizan habitualmente internet para su trabajo?	**14. ¿Considera usted que los medios tecnológicos con los que cuenta la empresa, provoca que la información sea vulnerable a fraudes informáticos?**
☐ 13.1. De 1 a 5 ☐ 13.2. De 5 a 10 ☐ 13.3. De 10 a 15 ☐ 13.4. De 15 a 20 ☐ 13.5. Más de 20	☐ 14.1. Si ☐ 14.2. No
15. ¿Cuál es el número de empleados que utilizan un computador en su rutina normal de trabajo?	**16. ¿En los últimos 4 años ha sufrido alguna fuga de información o ataque informático la empresa?**
☐ 15.1. De 1 a 5 ☐ 15.2. De 5 a 10 ☐ 15.3. De 10 a 15 ☐ 15.4. De 15 a 20 ☐ 15.5. Más de 20	☐ 16.1. Si ☐ 16.2. No *(En caso de ser negativa su respuesta pase a la pregunta 22)*
17. ¿Dispone su empresa de Pagina Web?	**18. ¿Qué tipo de fraude informático ha sufrido su empresa?**
☐ 17.1. Si ☐ 17.2. No *(En caso de ser negativa su respuesta pase a la pregunta 16)*	☐ 18.1. Pérdida física de dispositivos o medios que contengan datos ☐ 18.2. Fuga electrónica de datos de los sistemas internos ☐ 18.3. Suplantación de identidad/ ingeniería social en cuentas ☐ 18.4. Ataques a servicios bancarios en línea ☐ 18.5. Pérdidas financieras debidas a ataques en cajeros automáticos

19. ¿Con que frecuencia se actualiza la Pagina Web en su empresa?	20. Considerando la respuesta que usted dio en la pregunta anterior, los fraudes informáticos afectan a los resultados económicos financieros de la empresa?
☐ 19.1. Cada quince días ☐ 19.2. Mensual ☐ 19.3. Trimestral ☐ 19.4. Semestral ☐ 19.5. Una vez al año	☐ 20.1. Si ☐ 20.2. No
21. ¿Está su empresa interesada en poner en marcha un sistema informático de protección de datos o actualizarlos?	**22. ¿Realiza copias de seguridad de forma planificada y oportuna?**
☐ 22.1. Si ☐ 22.2. No	☐ 22.3. Si ☐ 22.4. No
Si No	Si No

Muchas gracias, por su valiosa colaboración

3.5. Tabulación de la encuesta

Pregunta Nº 1

1. **¿A qué segmento pertenece la entidad financiera?**

Tabla 10

Segmento de la entidad

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Segmento 1 (> a $ 80.000.000)	1	4,8	4,8	4,8
Segmento 3 (> a $5.000.000 hasta $20.000.000)	7	33,3	33,3	38,1
Segmento 4 (> a $ 1.000.000 hasta $5.000.000)	11	52,4	52,4	90,5
Pequeña (Ventas Totales: $100.001-$1.000.000)	1	4,8	4,8	95,2
Mediana (Ventas Totales: $ 1.000.001-$5.000.000)	1	4,8	4,8	100,0
Total	21	100,0	100,0	

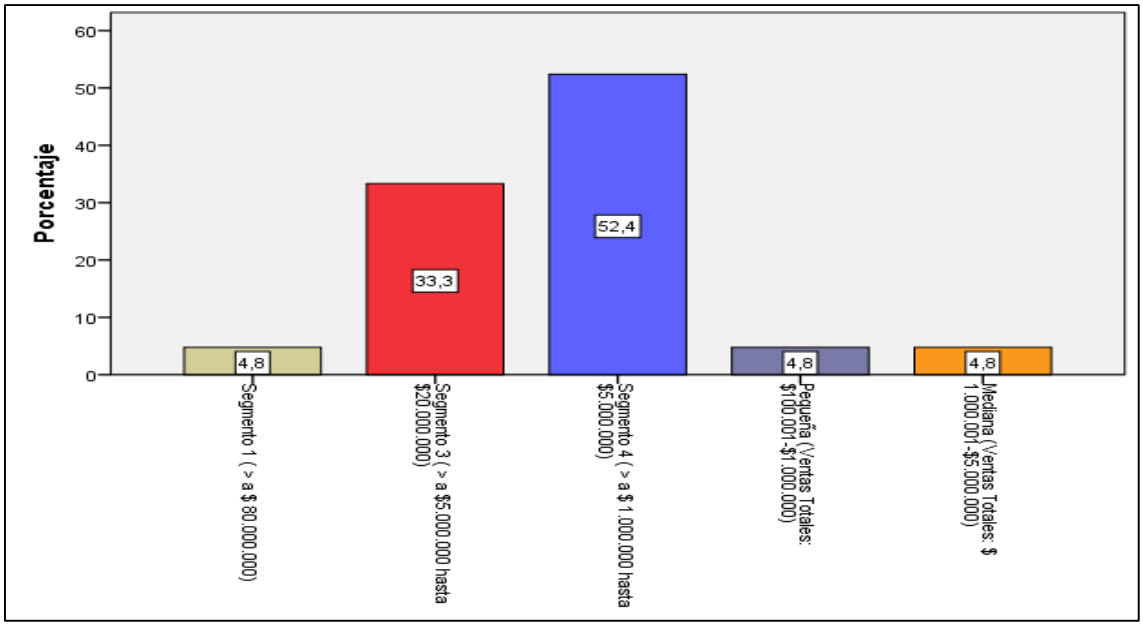


Figura 3. Segmento de la entidad

Interpretación:

De acuerdo a las encuestas aplicadas a las empresas del sector servicios controladas por la Superintendencia Economía Popular y Soldaría en la provincia de Cotopaxi, se pudo evidenciar que el total de las empresas encuestadas con valores significantes del 52.4% se encuentran en el segmento 4 (> a $ 1.000.000 hasta $5.000.000), seguidas del segmento 3 (> a $5.000.000 hasta $20.000.000) con el 33.3%. Con lo que podemos afirmar que en nuestra provincia son entidades al servicio de la sociedad prestando servicios financieros que ayudan al desarrollo económico, financiero y productivo en la provincia. Referente a nuestro tema de investigación se enfoca en fraudes informáticos y son vulnerables a los mismos por lo que manejan gran cantidad de información.

Pregunta Nº2

2. ¿A qué actividad de servicios se dedica su empresa?

Tabla 11

Actividad de las empresas

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Salud	1	4,8	4,8	4,8
Instituciones, agencias y servicios financieros	19	90,5	90,5	95,2
Alojamiento	1	4,8	4,8	100,0
Total	21	100,0	100,0	

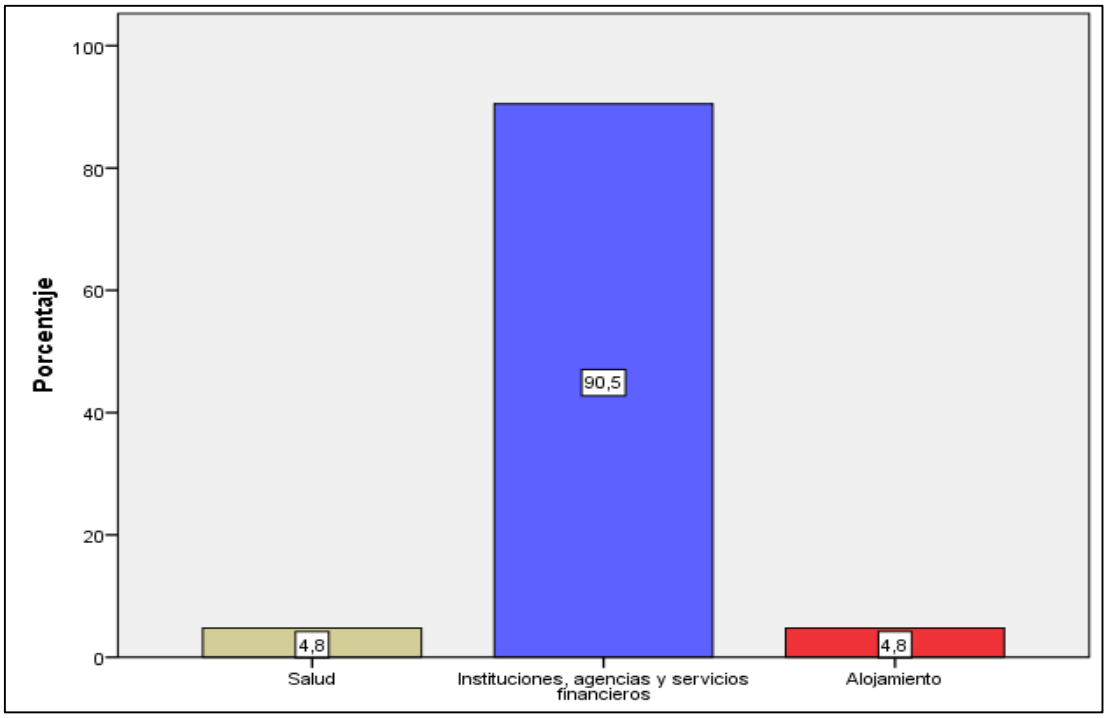


Figura 4. Tamaño de las empresas de servicios

Interpretación:

De acuerdo a las encuestas aplicadas a las empresas del sector servicios controladas por la Superintendencia de compañías y la Superintendencia de Economía Popular y Solidaria en la provincia de Cotopaxi, se pudo evidenciar que el total de las empresas encuestadas tenemos el 90.5% pertenece a las Instituciones; agencias y servicios financieros se encuentra el segmento 3 con valores (> a $5.000.000 hasta $20.000.000) y con el 33.3% seguidas del segmento 4 con valores (> a $ 1.000.000 hasta $5.000.000). Con lo que podemos afirmar que en nuestra provincia son entidades al servicio de la sociedad prestando servicios financieros que ayudan al desarrollo económico, financiero y productivo en la provincia. Referente a nuestro tema de investigación se enfoca en fraudes informáticos y son vulnerables a los mismos por lo que manejan gran cantidad de información.

Pregunta Nº3

3. **¿Desde su perspectiva, qué importancia tiene la utilización del recurso tecnológico para mejorar la productividad, calidad, control y comunicación dentro de las empresas de servicios?**

Tabla 12

Grado de importancia del recurso tecnológico en las empresas

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Alto	18	85,7	85,7	85,7
Medio	3	14,3	14,3	100,0
Total	21	100,0	100,0	

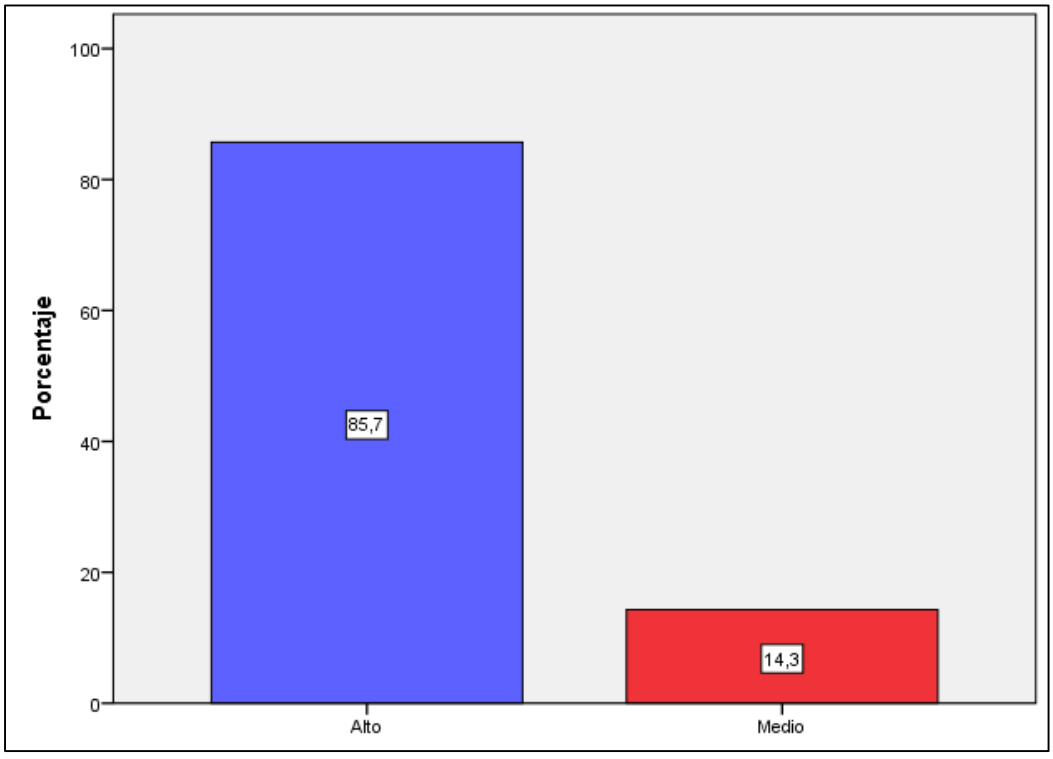


Figura 5. Grado de importancia del recurso tecnológico en las empresas

Interpretación:

El 85.7% de las empresas de servicios indican el alto grado de importancia en la utilización del recurso tecnológico, ya que con el venir del tiempo se ven constantes cambios con el único objetivo de mejorar el nivel de desempeño en las entidades brindando confianza y seguridad cuando se trata de servicios financieros cuando el recurso tecnológico es primordial para mejorar la productividad, calidad, control y comunicación dentro de la misma por lo cual deben contar con un departamento de TIC que den acceso a nuevas formas de comunicación, seguido de un 14.3% considerando en un grado medio por lo cual pueden estar conformadas la entidades que poseen una inversión muy baja en comparación de las mencionadas anteriormente.

Pregunta Nº4

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

Tabla 13

Favorece el recurso tecnológico en las operaciones de la empresa

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	20	95.2	95.2	95.2
No	1	4.8	4.8	100.0
Total	21	100.0	100.0	

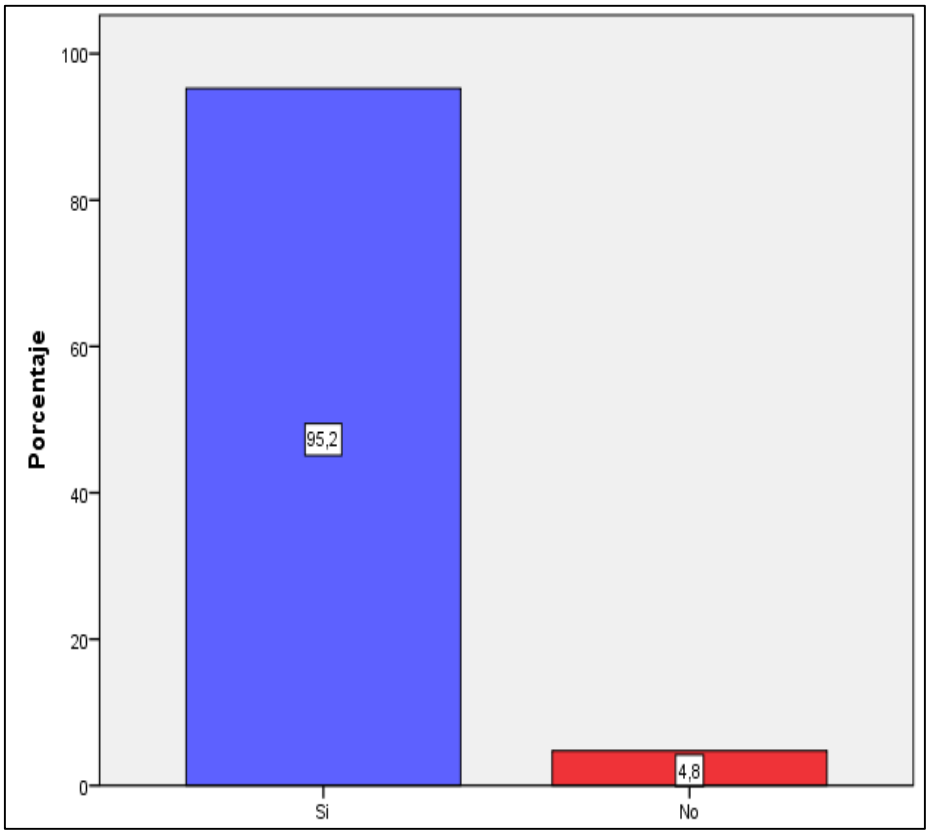


Figura 6. Favorece el recurso tecnológico en las operaciones de la empresa

Interpretación:

El 95.2% de las empresas de servicios responden que si favorecen al momento de optimización y minimización de recursos, por lo que se mencionó en la pregunta anterior son entidades que su principal herramienta para salvaguardar, controlar y efectuar operaciones viene dado por el recurso tecnológico aun así siempre estará presente la vulnerabilidad a ser atacados por un fraude informático, por lo que el manejo de la tecnología disminuye y brinda seguridad y confianza siempre y cuando esta cuente con un departamento en TIC.

Pregunta Nº5

5. **¿Con que frecuencia la empresa contrata un servicio técnico especializado en Tecnología de Información y Comunicación (TIC)?**

Tabla 14

Frecuencia en contratación de servicio técnico en TIC

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Mensual	3	14,3	14,3	14,3
Trimestral	2	9,5	9,5	23,8
Semestral	3	14,3	14,3	38,1
Anual	8	38,1	38,1	76,2
Nunca	5	23,8	23,8	100,0
Total	21	100,0	100,0	

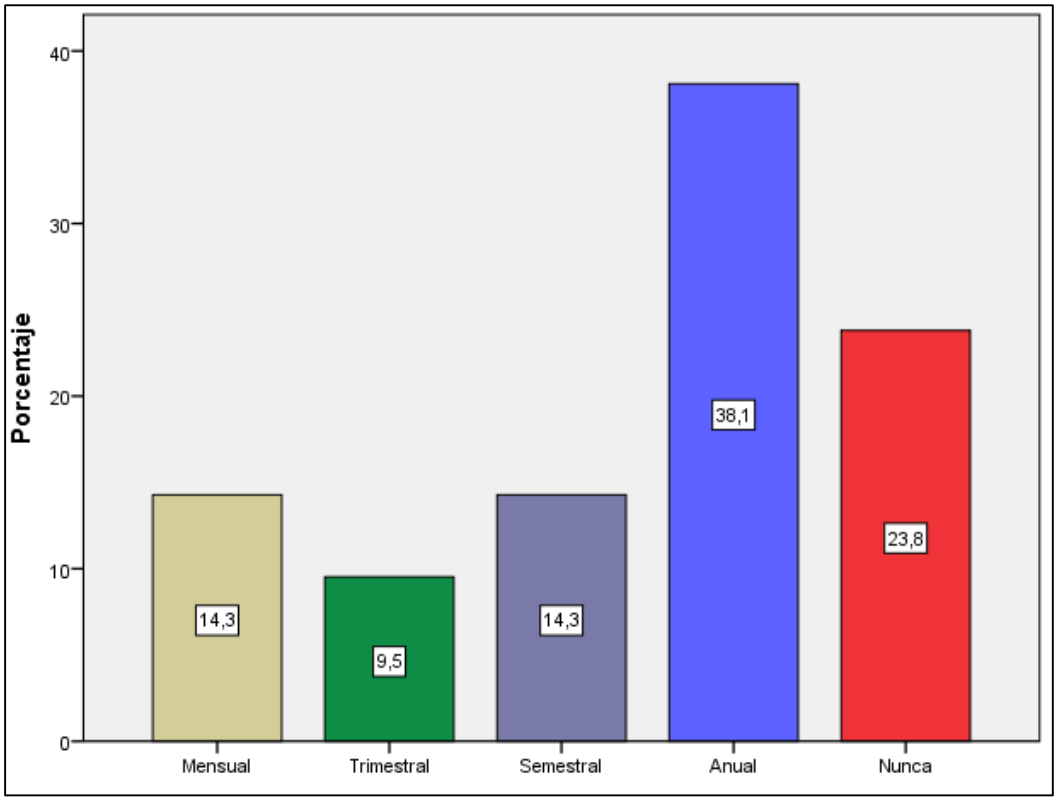


Figura 7. Frecuencia en contratación de servicio técnico en TIC

Interpretación:

Con un 23,8%, nunca lo han contratado un servicio técnico especializado en TIC lo que representa algo significativo con un riesgo alto, ya que solo cuentan con el apoyo técnico de los ingenieros en sistemas por lo que dejan a un lado al departamento de TIC esto indica una desventaja y vienen hacer vulnerables hacer atacadas por fraudes informáticos a diferencia del 38,1% contrata 1 vez al año servicios especializados en TIC por lo que se puede observar que es importante por lo menos la contratación de este servicio como una ventaja de esto se puede realizar muchas operaciones a través de la implementación o servicio técnico ya que ahora no es un lujo contar con tecnología más bien es una necesidad para las empresas y estar a la vanguardia en el mercado.

Pregunta Nº6

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

Tabla 15

Implementación de tecnología

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Último mes	6	28,6	28,6	28,6
Último trimestre	5	23,8	23,8	52,4
Último semestre	1	4,8	4,8	57,1
Último año	6	28,6	28,6	85,7
Último 4 años	3	14,3	14,3	100,0
Total	21	100,0	100,0	

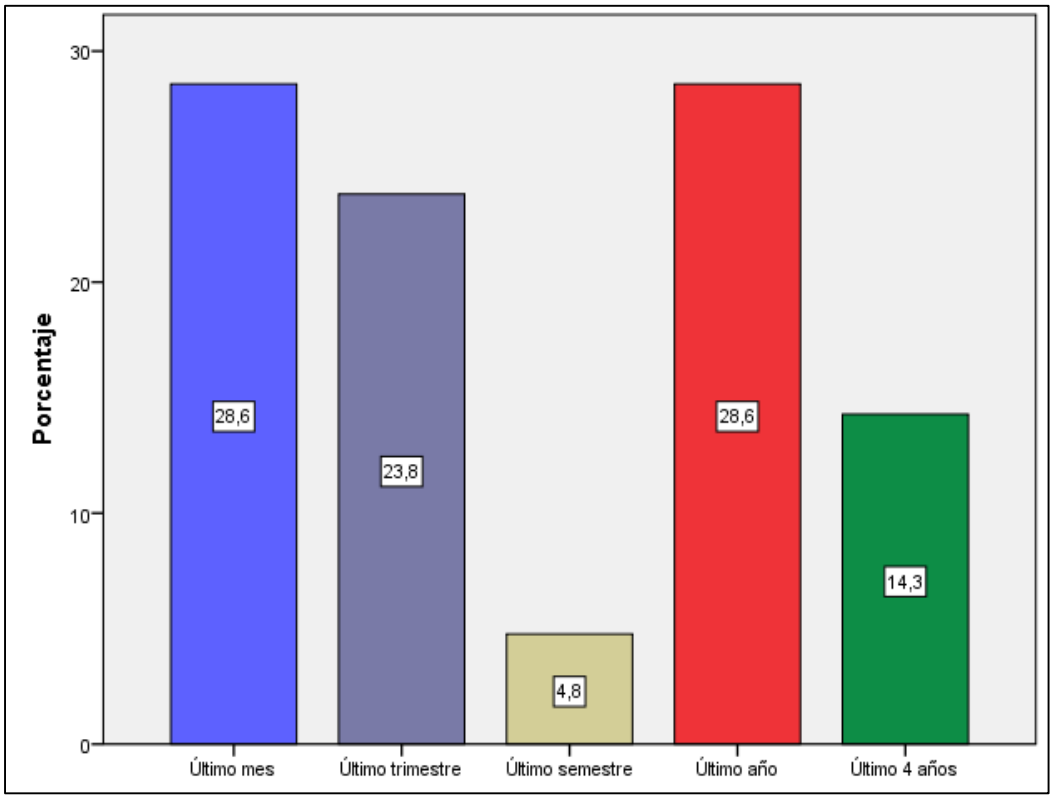


Figura 8. Implementación de tecnología

Interpretación:

Con un porcentaje bajo de 14.3% las empresas de servicios implementan tecnología o sistemas de información y comunicación lo hacen una vez a los 4 años ya que vienen hacer empresas o entidades con baja inversión por lo que no está a su alcance la adquisición en tecnología, y con el 28.6% realizan compras de equipos tecnológicos, compra de software, compra de licencias y patentes informáticas como también el mantenimiento y capacitación en tecnología información y comunicación estas implementaciones lo han hecho en el último mes y en el mismo porcentaje lo realizan una vez al año, el 23.8% han implementado en el último trimestre ya que es una necesidad realizar adquisiciones cuando hablamos de tecnología que no va ayudar en las operaciones de la entidad.

Pregunta Nº7

7. **¿Considerando la respuesta que usted dio en la pregunta anterior que tipo de inversión es más representativa para la empresa en Tecnología de Información y Comunicación seleccione una de ellas?**

Tabla 16

Inversión más representativa en TIC

	Respuestas		Porcentaje de casos
	N	Porcentaje	
Mantenimiento de equipo	6	18,2%	28,6%
Compra de equipo	7	21,2%	33,3%
Compra de software	12	36,4%	57,1%
Capacitación de personal	2	6,1%	9,5%
Licencias y patentes informáticas	6	18,2%	28,6%
Total	33	100,0%	157,1%

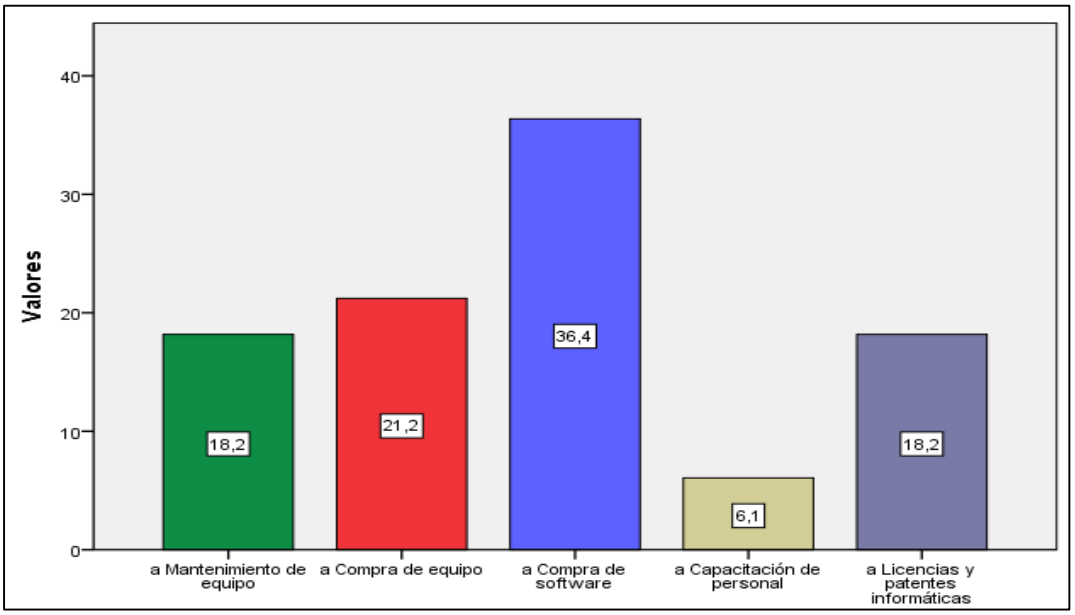


Figura 9. Inversión más representativa en TIC

Interpretación:

El 36.4% su inversión más representativa es la compra de software nuevas tecnologías al momento de gestiona de manera efectiva las entidades que brindan servicios financieros invierten en software dependiendo las necesidades que ellos presenten como la gestión de transferencia de una cuenta a otra, también los ingresos de débitos y créditos bancarios, estos software son primordiales al momento del desarrollo operativo en la institución ya que son de vital aportación para tener un excelente control en las actividades, tareas que se realizan diariamente con un valor del 21.1% las empresas invierten en lo que respecta a compra de equipo y estar a la vanguardia tecnológica y el 18.2% invierte en mantenimiento de equipo, licencias y patentes informáticas con el objetivo de tener el mejor desempeño en las operaciones y brindando seguridad a los clientes.

Pregunta Nº8

8. **¿Cuánto estima usted que ha invertido en Tecnología de Información y Comunicación (TIC) durante el periodo 2012 – 2016?**

Tabla 17

Valor de inversión en TIC periodo 2012 – 2016

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
De 0.000 a 10.000 dólares	4	19,0	19,0	19,0
De 10.000 a 20.000 dólares	7	33,3	33,3	52,4
De 20.000 a 30.000 dólares	2	9,5	9,5	61,9
De 30.000 a 40.000 dólares	3	14,3	14,3	76,2
De 40.000 a 50.000 dólares	1	4,8	4,8	81,0

CONTINÚA

Más de 50.000 dólares		4	19,0	19,0	100,0
Total		21	100,0	100,0	

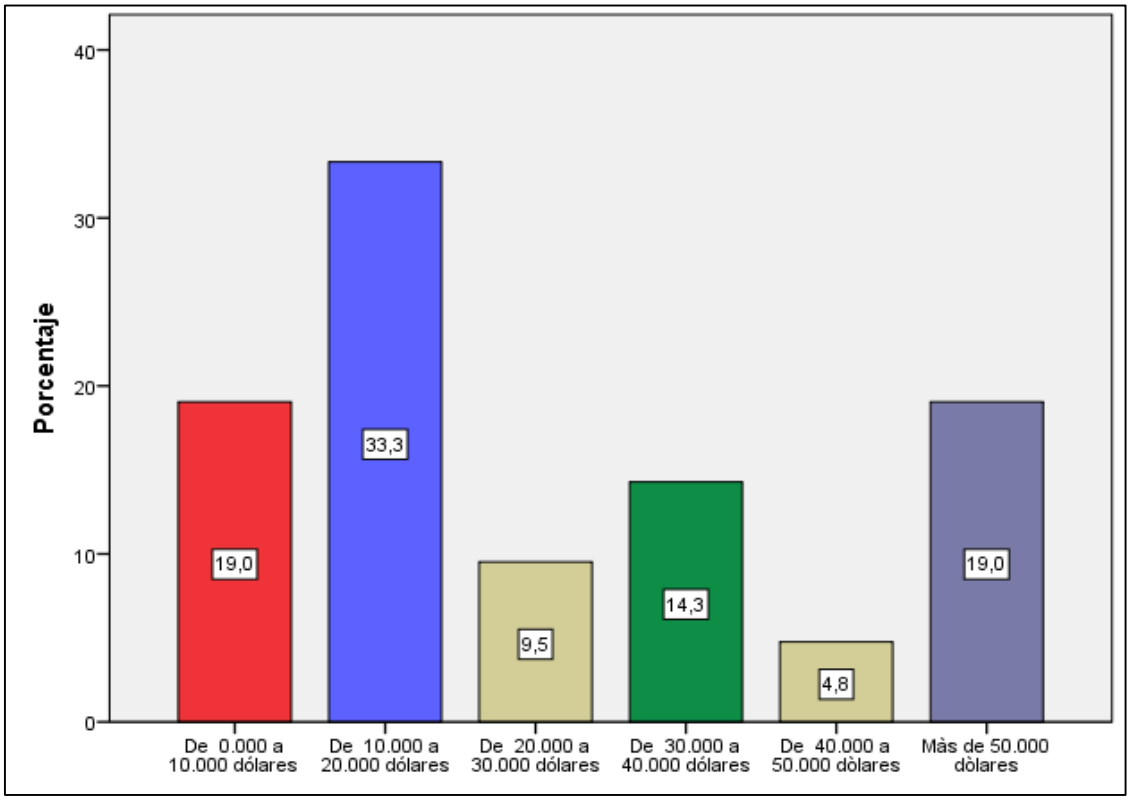


Figura 10. Valor de inversión en TIC periodo 2012 – 2016

Interpretación:

Con el 33.3% las empresas de servicios cuentan con una inversión de $10.000 a $20.000 en TIC en el periodo 2012 – 2016 ya que complementando con las preguntas anteriores su inversión está dada en la compra de software, compra de equipo, compra de licencias y patentes informáticas, mantenimiento de equipo y capacitación al personal seguido del 19.0% que va de $0.00 a más de $50.000 dólares ya que son empresas que cuentan con una buena inversión en los últimos periodos.

Pregunta Nº9

9. ¿Qué tipo de software contable maneja la entidad?

Tabla 18

Tipo de software

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
ASOTEC COOP FINANCIAL	1	4,8	4,8	4,8
SIAF Sistema de Información y Administración Financiera	3	14,3	14,3	19,0
FIB FINANCIERO	3	14,3	14,3	33,3
SISTEMA WEBCOOP	4	19,0	19,0	52,4
Otros	9	42,9	42,9	95,2
ZEUS sistema administrativo	1	4,8	4,8	100,0
Total	21	100,0	100,0	

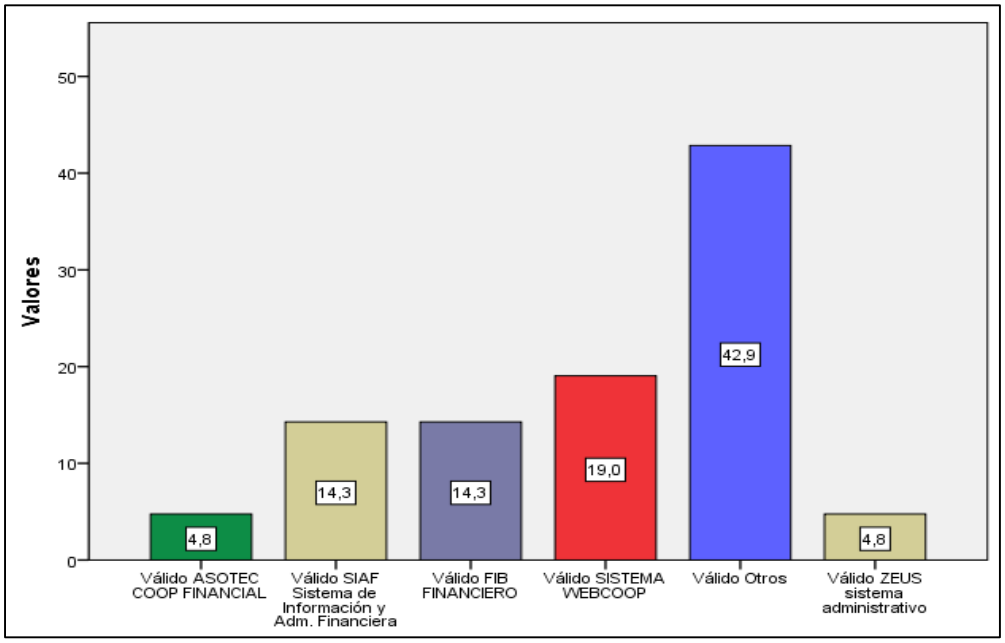


Figura 11. Tipo de software

Interpretación:

Con un 42.9% manejan otros tipos de software por lo que se puede decir que cada entidad financiera cuenta con su tipo de software de acuerdo a sus necesidades dentro de la entidad a lo que respecta en operaciones, con el 19% utilizan el software Sistema Webcoop que permite un análisis contable y administrativo todo depende de lo que requiere la entidad en cambio con el 19.0% utilizan el software SIAF Sistema de Información y Administración Financiera y el FIB Financiero

Pregunta Nº10

10. ¿Qué módulos tiene sus sistemas informáticos en la entidad?

Tabla 19

Módulos sistemas informáticos

	Respuestas		Porcentaje de casos
	N	Porcentaje	
CRM (Gestión de Servicio al Cliente)	4	13,8%	21,1%
SIAF (Sistema de Información y Adm. Financiera)	18	62,1%	94,7%
SAP (Sistemas, Aplicaciones y Productos)	7	24,1%	36,8%
Total	29	100,0%	152,6%

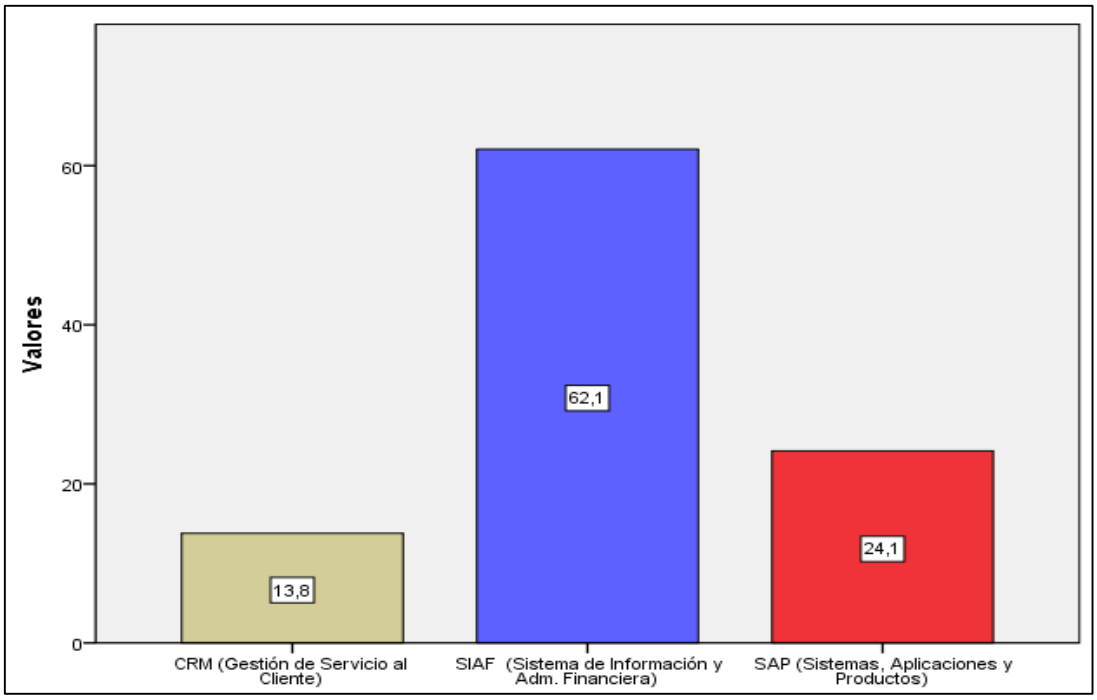


Figura 12. Módulos Sistemas Informáticos

Interpretación:

Con el 62.1% las empresas del sector servicios nos indican que utilizan como módulos el SIAF (Sistema de Información y Administración Financiera)

Pregunta Nº11

11. ¿Cuántas computadoras posee su empresa?

Tabla 20

Número de computadores que posee su empresa

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
De 1 a 5	1	4,8	4,8	4,8
De 5 a 10	4	19,0	19,0	23,8
De 10 a 15	7	33,3	33,3	57,1
De 15 a 20	2	9,5	9,5	66,7
Más de 20	7	33,3	33,3	100,0
Total	21	100,0	100,0	

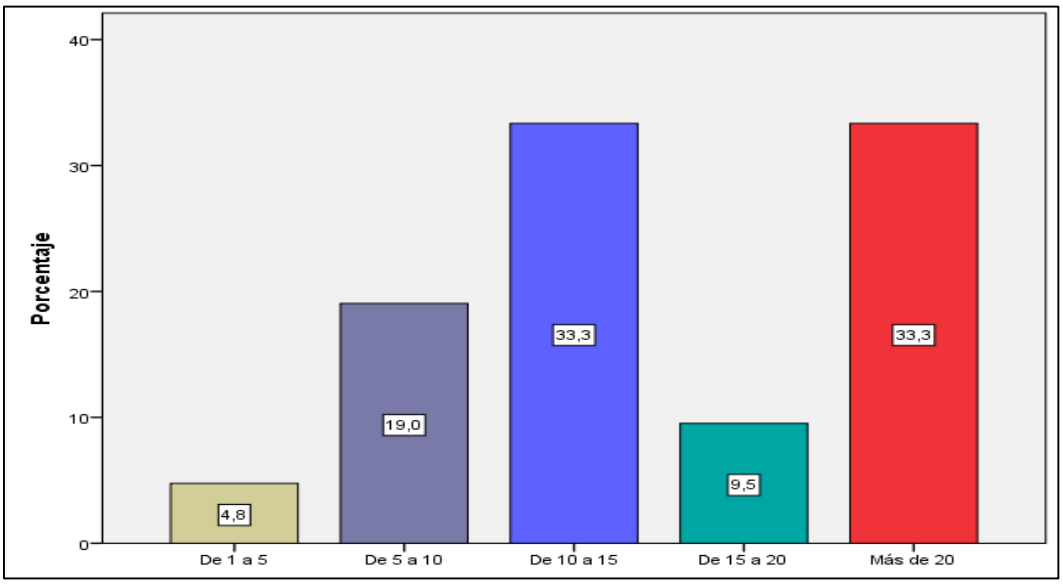


Figura 13. Número de computadoras que posee la empresa

Interpretación:

El 33,3% de las empresas de servicios poseen más de 20 computadoras debido a sus actividades diarias que realizan por lo tanto sufren mayores riesgos de fuga de información, de igual manera el 33,3% cuentan entre 10 a 15 computadoras estas

empresas son medianas con menor riesgo de fuga de información o protección de datos, el 19,0% poseen entre 5 a 10 computadoras, el 9,5% de 15 a 20 computadoras y un 4,8% entre 1 a 5 computadoras empresas con un nivel bajo de riesgo a pérdidas de información.

Pregunta Nº12

12. ¿Cuántas personas empleadas en su empresa utilizan habitualmente internet para su trabajo?

Tabla 21

Personal que utiliza internet en su lugar de trabajo

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
De 1 a 5	2	9,5	9,5	9,5
De 5 a 10	7	33,3	33,3	42,9
De 10 a 15	4	19,0	19,0	61,9
Más de 20	8	38,1	38,1	100,0
Total	21	100,0	100,0	

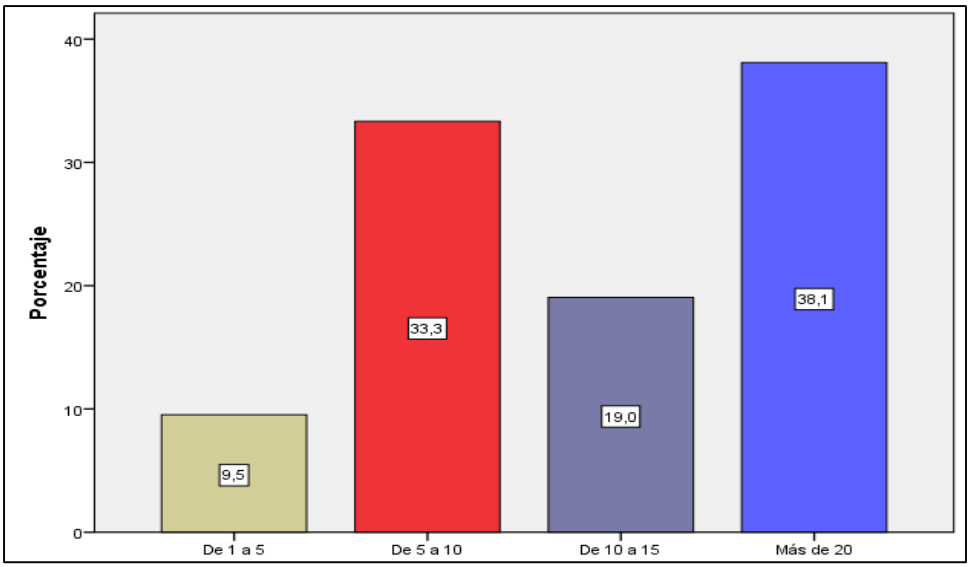


Figura 14. Personal que utiliza internet en su lugar de trabajo

Interpretación:

Es muy importante el uso del internet en la organización ya que el 9.5% nos indican que de 1 a 55 personas utilizan de esta herramienta para el desarrollo, desempeño de todas las actividades diarias, el 33.3% mediante un rango de 5 a 10 personas también hacen uso de este medio para mantener conexión en línea, como también el 19% en un rango de 10 a 15 personas acuden a este medio por lo que el 38.1% nos indican que utilizan habitualmente internet para desarrollar todas las actividades dentro de la entidad mediante el cual esta herramienta es de uso prioritario para poder enlazar conexión, por lo que mantienen un grado de vulnerabilidad hacer atacados por ciberdelincuentes que tienen un objetivo muy claro el robo de la información para realizar fraudes informáticos a los diferentes usuarios en la red.

Pregunta Nº 13

13. ¿Cuál es el número de empleados que utilizan un computador en su rutina normal de trabajo?

Tabla 22

Tabla número de empleados que utilizan un computador

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
De 1 a 5	1	4,8	4,8	4,8
De 5 a 10	10	47,6	47,6	52,4
De 10 a 15	2	9,5	9,5	61,9
Más de 20	8	38,1	38,1	100,0
Total	21	100,0	100,0	

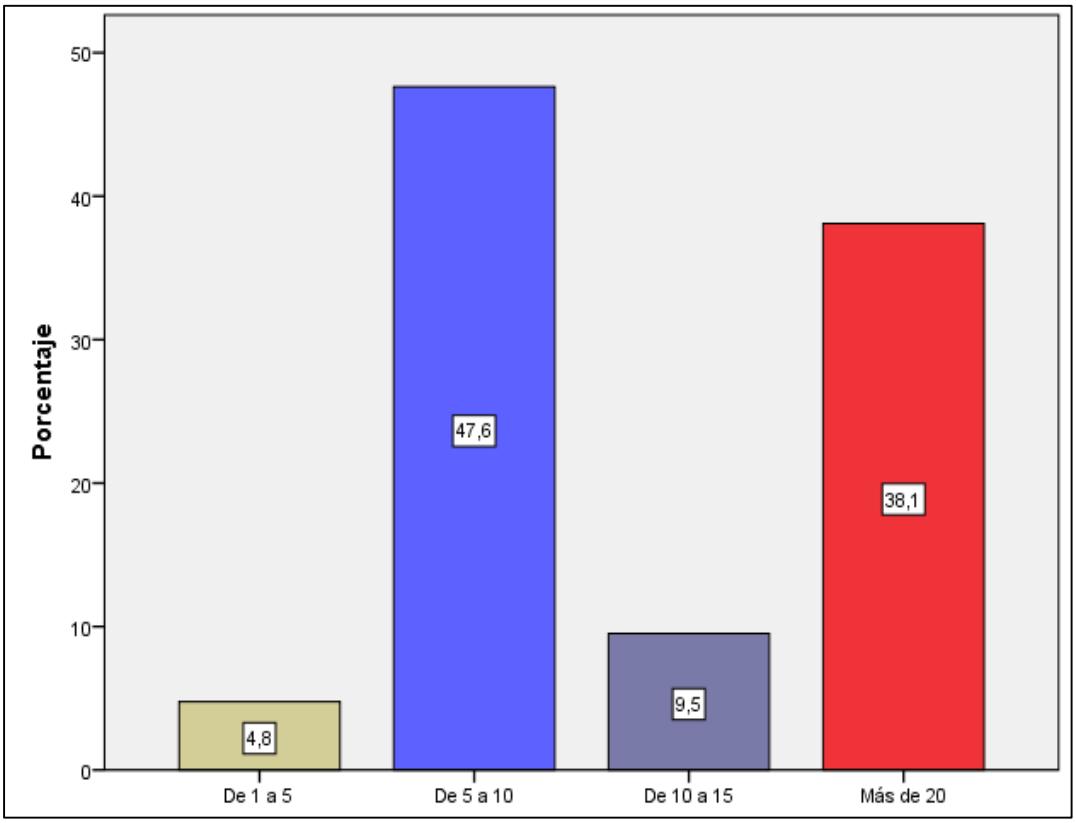


Figura 15. Número de empleados que utilizan un computador

Interpretación:

Al aplicar las encuestas en las empresas de servicios tenemos resultados que de 5 a 10 empleados utilizan un computador por lo que podemos complementar con la pregunta anterior que el personal no solo está conectado por medio de un computador sino también por un celular inteligente ya que el personal que cuenta con su propio computador en su lugar de trabajo realizan actividades que se necesita de esta herramienta para desarrollar todas las actividades dentro de la empresa y con un valor muy alto del 38.1% con un número de personas más de 20 complementan su actividad por medio de un computador sea este de escritorio o portátil lo que se pude concluir que es una necesidad dentro de organización.

Pregunta Nº 14

14. ¿Dispone su empresa de Pagina Web?

Tabla 23

Cuenta con página web en la empresa

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	13	61,9	61,9	61,9
No	8	38,1	38,1	100,0
Total	21	100,0	100,0	

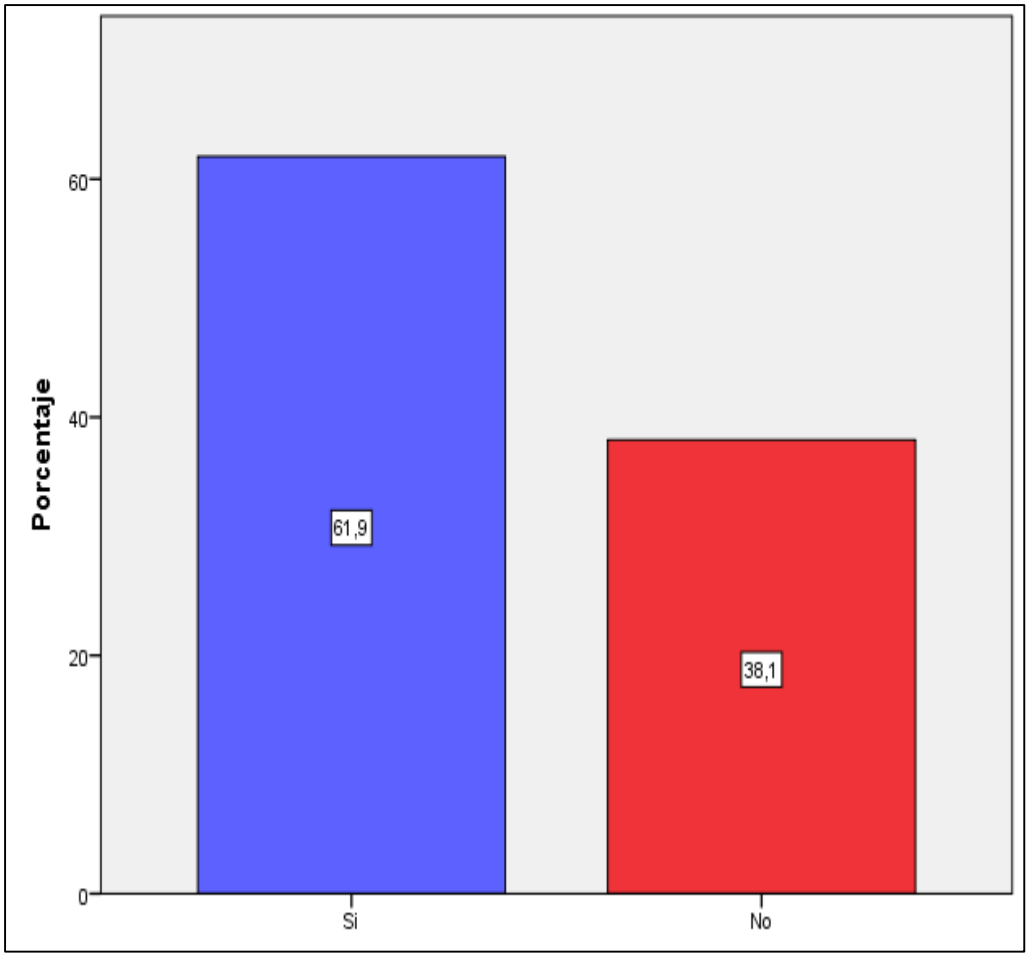


Figura 16. Cuenta con página web la empresa

Interpretación:

El resultado después de la aplicación de las encuestas indica que el 61.9% cuenta con página web ya que es necesario como medio de información y medio comercial ya que es una herramienta importante para publicar información a la sociedad sobre todos los servicios que se ofrecen en la empresa por lo que es una ventaja como medio publicitario para que el internauta haga uso del mismo.

Pregunta Nº 15

15. ¿Con que frecuencia se actualiza la Pagina Web en su empresa?

Tabla 24

Frecuencia de la empresa con la cual actualiza su página web

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Mensual	4	19,0	30,8	30,8
Trimestral	1	4,8	7,7	38,5
Semestral	3	14,3	23,1	61,5
Una vez al año	5	23,8	38,5	100,0
Total	13	61,9	100,0	
No procede según pregunta 14	8	38,1		
Total	21	100,0		

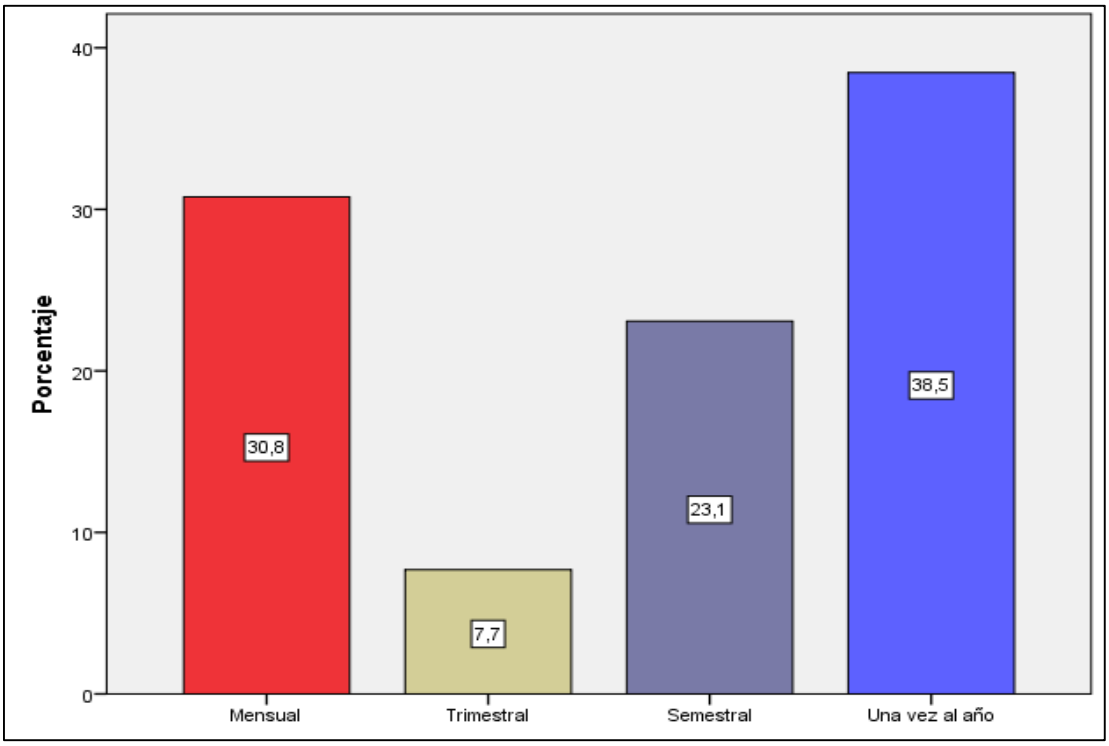


Figura 17. Tabla Frecuencia de la empresa con la cual actualiza su página web

Interpretación:

Mediante las encuestas realizadas el 38,5% de las empresas de servicios controladas por la Superintendencia Economía Popular y Soldaría en la provincia de Cotopaxi manifiestan que una vez al año actualizan su página web debido a que la tecnología web cambia día a día, el 30,8% lo realizan mensual, mientras tanto el 23,1% semestral y en un 7.7% lo realizan trimestral, es decir que las empresas están controlando su página web constantemente y de esa manera protegen su información.

Pregunta Nº 16

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

Tabla 25

Sistema Informático de protección de datos

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	18	85,7	85,7	85,7
No	3	14,3	14,3	100,0
Total	21	100,0	100,0	

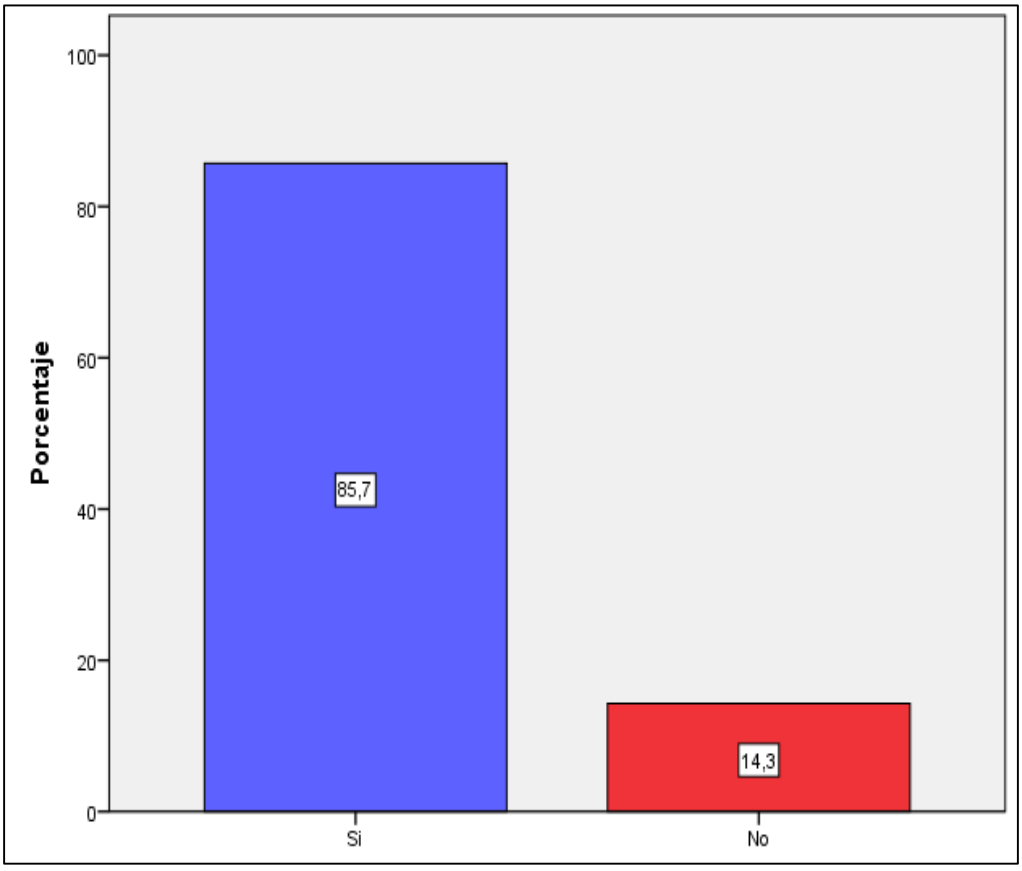


Figura 18. Sistema Informático de protección de datos

Interpretación:

El 85,4% de las empresas del sector servicios controladas por la Superintendencia Economía Popular y Soldaría en la provincia de Cotopaxi si están interesadas en poner en marcha un sistema informático de protección de datos o actualizarlos, a diferencia de que el 14,3% de las empresas dicen que no, por lo tanto la mayoría de las empresas si requieren proteger su información de manera adecuada y evitar fraudes informáticos por terceros o propios de la misma.

Pregunta Nº 17

17. ¿Hasta cuánto podría presupuestar por un sistema informático de protección de datos?

Tabla 26

Valor de presupuesto de un sistema informático

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
0.000 a 10.000 dólares	11	52,4	52,4	52,4
10.000 a 20.000 dólares	7	33,3	33,3	85,7
20.000 a 30.000 dólares	1	4,8	4,8	90,5
Más de 50.000 dólares	2	9,5	9,5	100,0
Total	21	100,0	100,0	

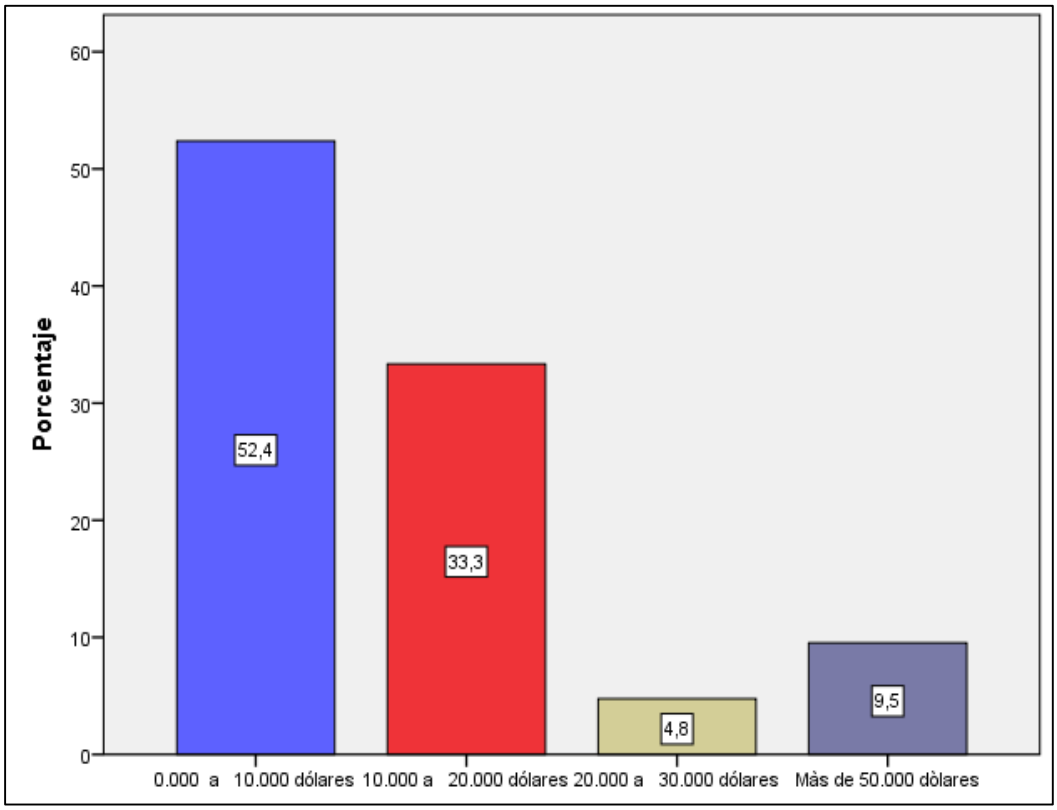


Figura 19. Valor de presupuesto de un sistema informático

Interpretación:

Mediante las encuestas realizadas se puede evidenciar que el 52,4% de las empresas de servicios pueden presupuestar por un sistema informático de protección de datos entre $0.000 a $10.000 en TIC en el periodo 2012 – 2016, seguido del 33.3% entre $10.00 a $20.000, el 9,5% más de a $50.000, es decir que las empresas en los últimos 4 años si cuentan con una inversión para proteger sus datos.

Pregunta Nº 18

18. ¿Considera usted que los medios tecnológicos con los que cuenta la empresa, provoca que la información sea vulnerable a fraudes informáticos?

Tabla 27

La información de la empresa es vulnerable a fraudes informáticos

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	11	52,4	52,4	52,4
No	10	47,6	47,6	100,0
Total	21	100,0	100,0	

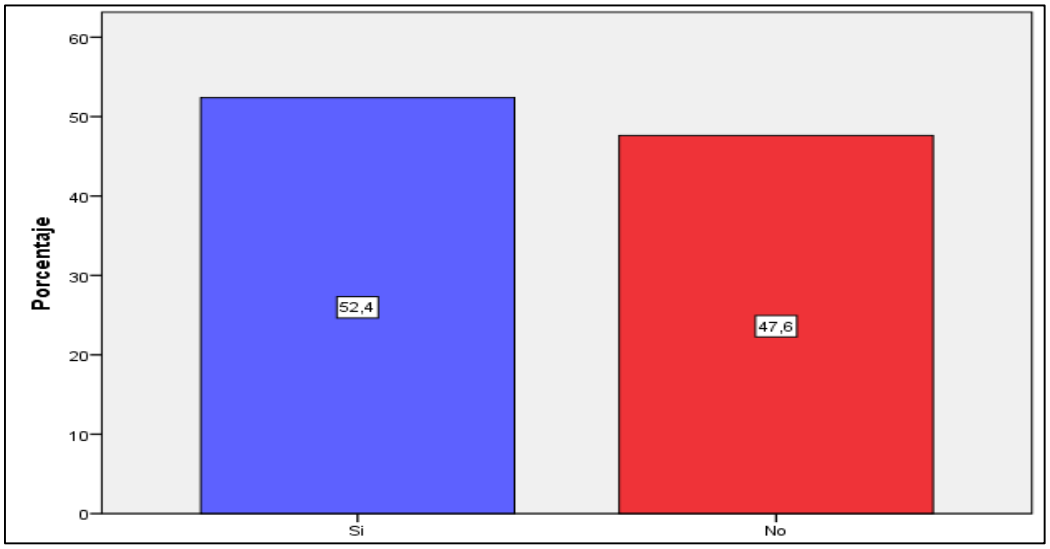


Figura 20. La información de la empresa es vulnerable a fraudes informáticos

Interpretación:

El 52,4% de las empresas del sector servicios controladas por la Superintendencia de compañías y la Superintendencia de Economía Popular y Solidaria en la provincia de Cotopaxi manifiestan que la información de la empresa si son vulnerable a fraudes

informáticos, mientras tanto el 47,6% la información de las empresas no es vulnerable a fraudes informáticos. Se puede decir que si existen un control adecuado de la información en las empresas.

Pregunta Nº 19

19. ¿En los últimos 4 años ha sufrido alguna fuga de información o ataque informático la empresa?

Tabla 28

Fuga de información en las empresas

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	9	42,9	42,9	42,9
No	12	57,1	57,1	100,0
Total	21	100,0	100,0	

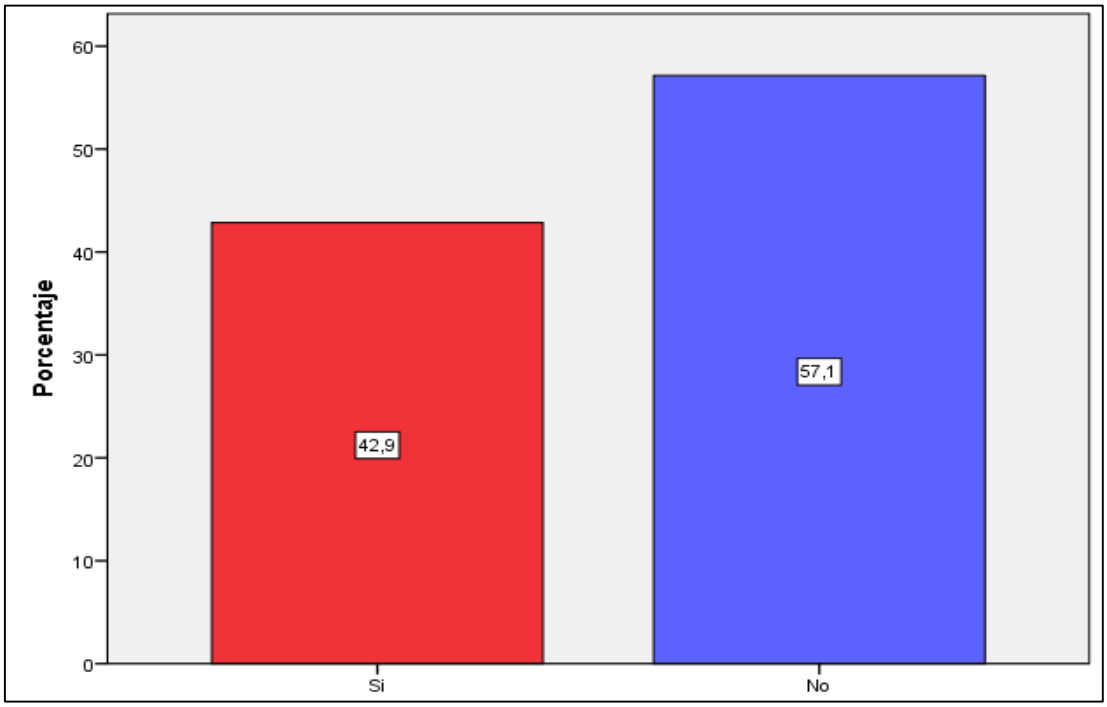


Figura 21. Fuga de información en las empresas

Interpretación:

El 57,1% de las empresas del sector de servicios controladas por la Superintendencia de compañías y la Superintendencia de economía popular y solidaria en la provincia de Cotopaxi manifiestan que en los 4 últimos años si han sufrido alguna fuga de información o ataque informático debido a que no existen un control adecuado a sus sistemas, el 42,9% manifiestan que no han sufrido fraudes informáticos, es decir que la mayoría de las empresas no cuentan con fuga de información o ataque informático.

Pregunta Nº 20

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

Tabla 29

Tipo de fraude informático

	Respuestas		Porcentaje de casos
	N	**Porcentaje**	
Pérdida física de dispositivos o medios que contengan datos	7	33,3%	77,8%
Fuga electrónica de datos de los sistemas internos	2	9,5%	22,2%
Suplantación de identidad/ ingeniería social en cuentas	3	14,3%	33,3%
Ataques a servicios bancarios en línea	3	14,3%	33,3%
Pérdidas financieras debidas a ataques en cajeros automáticos	6	28,6%	66,7%
Total	21	100,0%	233,3%

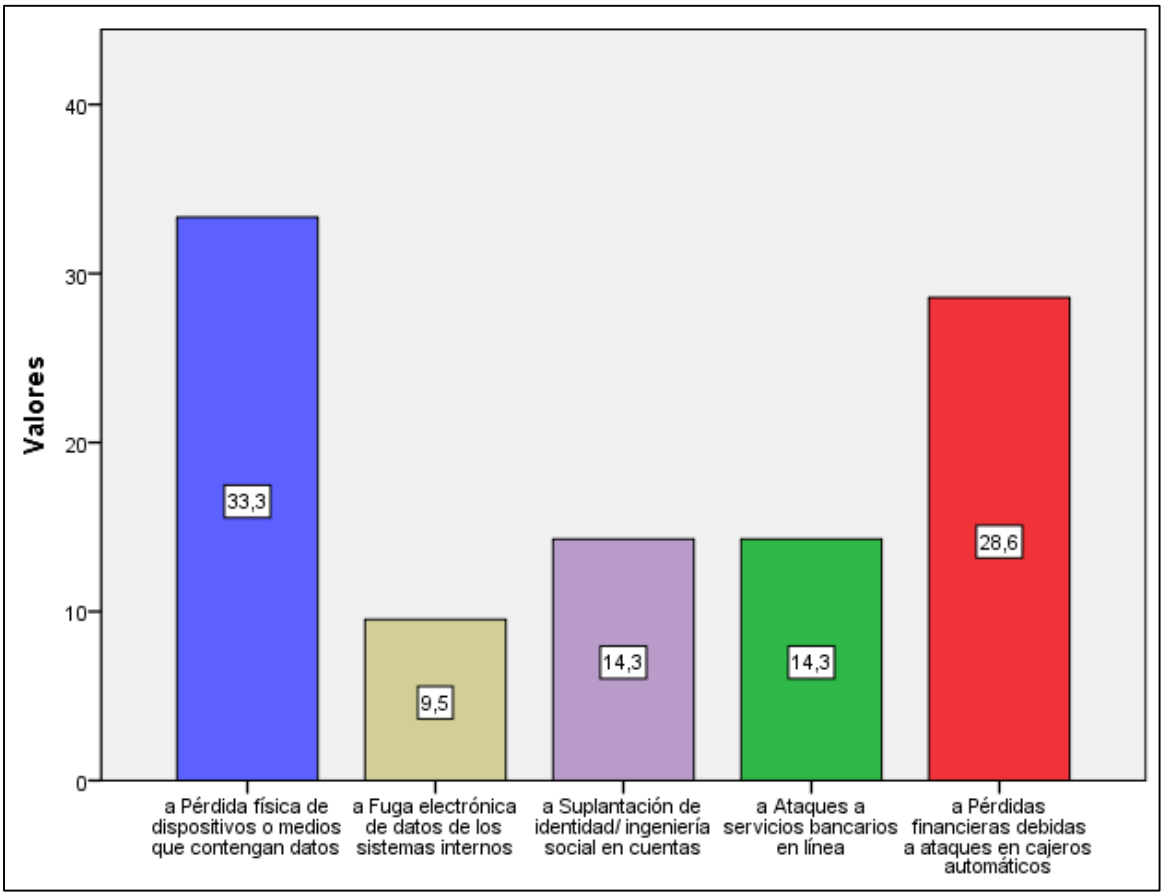


Figura 22. Tipo de fraude informático

Interpretación:

El 33,3% de las empresas del sector servicios controladas por la Superintendencia de compañías y la Superintendencia de economía popular y solidaria en la provincia de Cotopaxi han sufrido fraudes informáticos mediante pérdida física de dispositivos, seguido del 28,6 sufren fraudes informáticos por pérdidas financieras debidas a ataques en cajeros automáticos, el 14,3% por suplantación de identidad, de igual manera el 14,3% por ataques a servicio bancarios en línea y el 9.5% por fuga electrónica de datos de los sistemas internos es decir que la mayoría de las empresas sufren fraudes informáticos por pérdidas físicas de sus dispositivos y pérdidas financieras.

Pregunta Nº 21

21. ¿Considerando la respuesta que usted dio en la pregunta anterior, los fraudes informáticos afectan a los resultados económicos financieros de la empresa?

Tabla 30

Los fraudes informáticos afectan a los resultados económicos financieros de la empresa

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	9	42,9	42,9	42,9
No procede según pregunta 19	12	57,1	57,1	100,0
Total	21	100,0	100,0	

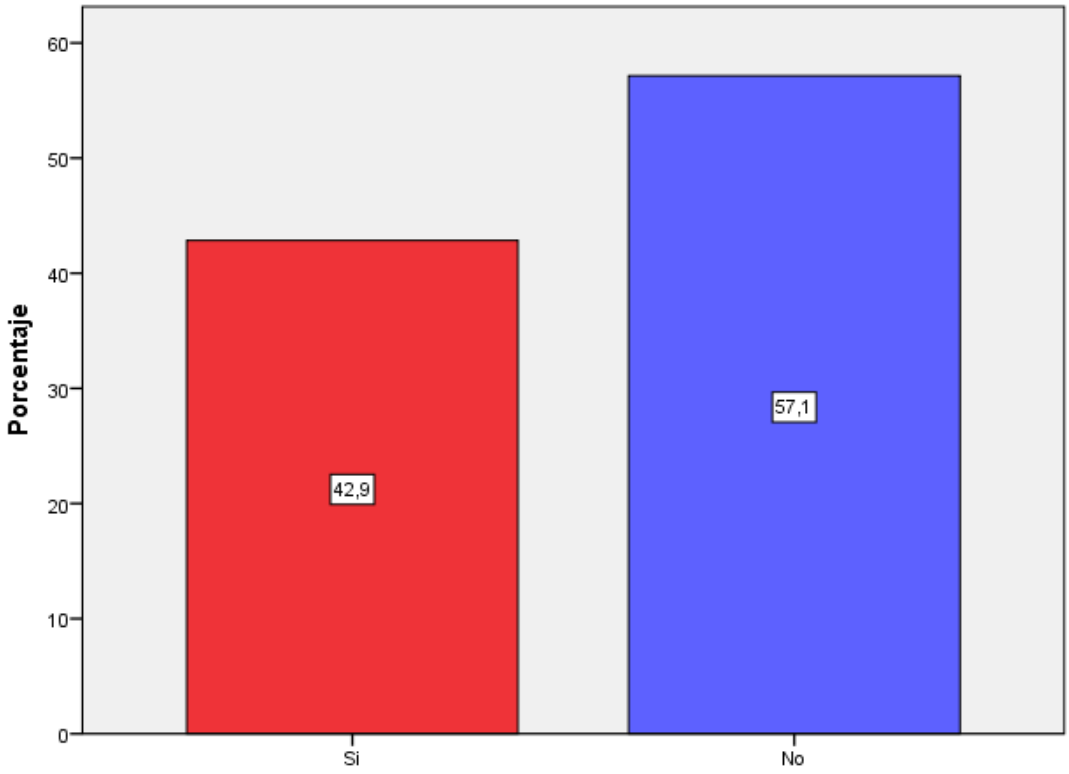


Figura 23. Los fraudes informáticos afectan a los resultados económicos financieros de la empresa

Interpretación:

De acuerdo a la información obtenida se puede evidenciar que el 57,1% de las empresas de servicios controladas por la Superintendencia de compañías y la Superintendencia de economía popular y solidaria en la provincia de Cotopaxi manifiestan que los fraudes informáticos no afectan a los resultados económicos financieros de la empresa, mientras tanto que el 42,9% si afectan los fraudes informáticos en las empresas de servicios.

Pregunta Nº 22

22. ¿Realiza copias de seguridad de forma planificada y oportuna?

Tabla 31

La empresa realiza copias de seguridad

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Si	20	95,2	95,2	95,2
No	1	4,8	4,8	100,0
Total	21	100,0	100,0	

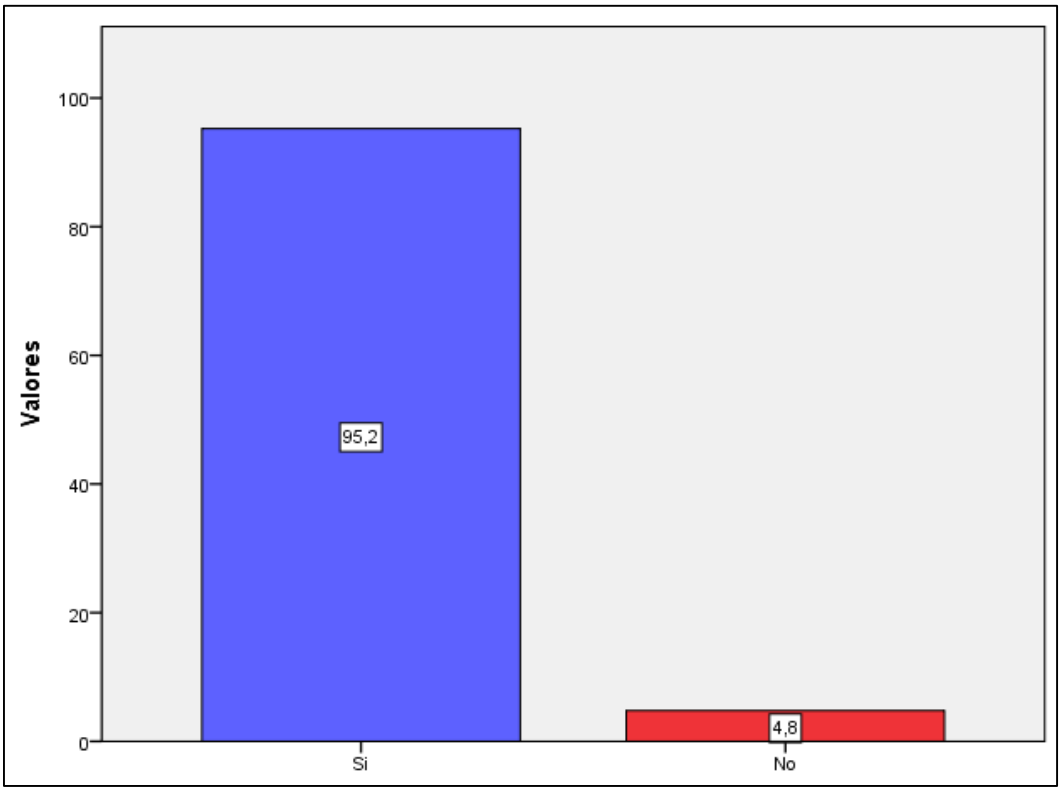


Figura 24. La empresa realiza copias de seguridad

Interpretación:

De acuerdo a la información obtenida se puede evidenciar que el 95,2% de las empresas del sector de servicios controladas por la Superintendencia de compañías y la Superintendencia de economía popular y solidaria en la provincia de Cotopaxi si realizan copias de seguridad de forma planificada y oportuna, mientras tanto solo el 4,8% no, es decir que la mayoría de las empresas tienen copias de seguridad, almacenan y protegen su información.

3.6. Discusión de los resultados obtenidos

Después de obtener los resultados en las empresas del sector servicios financieros en la provincia de Cotopaxi reguladas por la Superintendencia de Compañías y la Superintendencia de Economía Popular y Solidaria (SEPS), podemos afirmar que la información que facilitaron las cooperativas de ahorro y crédito que se encuentran dentro de la provincia la investigación se llevó a cabo bajo datos reales proporcionados por las mismas.

En lo que respecta a la seguridad informática que manejan las entidades financieras se puede decir que utilizan el servicio particular de empresas que se dedican al manejo de software de última generación están a la vanguardia de la tecnología, ofreciendo el mejor servicio en los que respecta gestión rápida y logrando la más alta eficiencia en todos los departamentos de la entidad manejados bajo normas y políticas de seguridad según las necesidades de las de las cooperativas.

El grado de vulnerabilidad de las cooperativas de ahorro y crédito es constante ya que existen delincuentes informáticos que hacen de las suyas para sacar provecho a base de fraude, en el caso de nuestra investigación se pudo verificar que la Cooperativa de Ahorro y Crédito Santa Rosa de Patutàn Ltda., fue víctima de este tipo de fraude, que gracias al buen manejo del personal para realizar algún tipo de transacción se supo manejar ante una política y normas de autorización para realizar dicha solicitud que solicitaba un “cliente” que creo un correo falso y con este tipo de fraude en comercio electrónico su objetivo era solicitar una transacción con un valor considerable y de esta manera la entidad fue víctima de los delincuentes informáticos.

Las empresas que ofrecen a las cooperativas de un software según el segmento que se encuentren nacen las necesidades de las entidades ya que estas contratan los

servicios para que se ocupen del sistema informático, lo cual crea una desventaja para la misma ya que las empresas del sector servicios financieros deben contar con un profesional en el área de sistemas que este sea el responsable del departamento de tecnología de información y comunicación y sea el mismo el que capacite al personal que ingresa a laborar para dichas entidades e esta manera obtendremos una excelente eficiencia, y de esta manera brindamos una excelente seguridad a las cooperativas y a los clientes que forman parte de la misma.

Como propuesta de nuestra investigación luego de haber analizado todos los resultados obtenidos desarrollaremos un manual de buenas prácticas en lo que respecta al manejo y uso de los sistemas informáticos ya que las cooperativas no cuentan con dicho manual o guía, y las entidades de servicios financieras deben poner más énfasis al adecuado uso o manejo de los sistemas informáticos por lo que esta se convierte en la puerta principal de entrada para tener acceso y cometer delitos informáticos, por lo tanto con un adecuado uso y protección de datos muy sensibles que tienen las cooperativas.

3.7. Recomendación

Con el propósito de que la investigación nos permita determinar en la Cooperativa de Ahorro y Crédito Santa Rosa de Patután Ltda., después de haber sufrido un intento de fraude informático por medio de correo electrónico, nosotros como investigadores proponemos realizar una auditoria informativa con el fin de verificar, evaluar y recoger evidencias para determinar en qué condiciones se encuentra actualmente el sistema informático con el que cuenta la cooperativa, de esta manera loa investigadores estamos evaluando si la entidad maneja de forma eficiente los recursos con los que cuenta la misma con el objetivo de salvaguardar la información y brindar seguridad a socios y clientes.

- Realizar una Auditoria Informática.
- Con los resultados obtenidos de la auditoria informática procedemos a realizar un Examen Especial de los sistemas informáticos que tiene la cooperativa con

el único propósito de determinar, evaluar y verificar en qué condiciones se encuentra y que garantías está brindando el sistema informático a la cooperativa, cuales son los procesos que mantienen los empleados al momento de acceder al programa.

- Realizar un análisis forense digital
- Identificación y recopilación de la amenaza o causa de riesgo - Tipo de fraude que se intentaba realizar y término en una amenaza

CAPITULO IV

APLICACIÓN DE LA AUDITORÍA INFORMÁTICA

PA – 1/2

COOPERATIVA DE AHORRO Y CRÉDITO SANTA ROSA DE PATUTÁN LTDA.

AUDITORÍA INFORMÁTICA

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

DEL 1 DE ENERO AL 31 DE JULIO DE 2018

OBJETIVO: Determinar la vulnerabilidad de los sistemas informáticos de la COOPERATIVA DE AHORRO Y CRÉDITO SANTA ROSA DE PATUTÁN LTDA., en el periodo 2012 – 2016.

Tabla 32 Programa de auditoría

Nº	Procedimientos	Referencia de P/T	Elaborado por	Fecha
1	Verificar el monto de inversión en Tecnología de Información y Comunicación (TIC) de acuerdo al balance general de la Cooperativa.	CS – 1/1	A.R.CH	10/05/2018
2	Solicitar al responsable de Departamento/Área de Tecnología de Información y Comunicación (TIC) el respectivo registro de equipos que se son usados, cuantos usuarios lo usan y cuantas horas al día son usados estos equipos.	RE – 1/1	E.M.V.S	10/05/2018

CONTINÚA

PA – 2/2

3	**Elaboración de Cuestionarios de Control Interno al Departamento/ Área de Tecnología de Información y Comunicación (TIC)**	**CCI – 1/3**	**A.A.R.CH**	**13/05/2018**
4	Aplicación de Cuestionarios de Control Interno al Departamento/ Área de Tecnología de Información y Comunicación (TIC).	CCI – 1/3 MCR – 1/1	E.M.V.S	17/05/2018
5	Realizar un examen especial a los sistemas más vulnerables del Departamento/ Área de Tecnología de Información y Comunicación (TIC).	EXES – 1/4	A.A.R.CH	17/05/2018
6	Análisis Forense de los sistemas operativos dentro del área de TIC.	AF – 1/4	A.A.R.CH	20/05/2018
7	Elaboración de una hoja de hallazgos de los resultados obtenidos.	HH – 1/3	E.M.V.S	22/05/2018
8	Elaboración de un Informe de Auditoria de los resultados obtenidos.	IA – 1/7	E.M.V.S	23/05/2018

ELABORADO POR: **A.A.R.CH - E.M.V.S**	FECHA: **12/05/2018**
REVISADO POR: **L.A.L.C**	**FECHA:** 07/05/2018

Tabla 33

Cedula Sumaria

CS – 1/1

COOPERATIVA DE AHORRO Y CRÉDITO SANTA ROSA DE PATUTÁN LTDA.						
CÉDULA SUMARIA DE LA CUENTA EQUIPO DE CÓMPUTO						
AL 31 DE JULIO DE 2018						
AÑO	**CUENTAS**	**REF P/T**	**S/S CONTABILIDAD**	**ASIENTOS DE CLASIFICACION**		**S/S AUDITORIA**
				DEBE	**HABER**	
2012	EQUIPO DE COMPUTO	BG 1/5	9.954,31			$ 9.954,31
2013	EQUIPO DE COMPUTO	BG 2/5	9.954,31			$ 9.954,31
2014	EQUIPO DE COMPUTO	BG 3/5	10.514,31			$ 10.514,31
2015	EQUIPO DE COMPUTO	BG 4/5	10.514,31			$ 10.514,31
2016	EQUIPO DE COMPUTO	BG 5/5	9.733,07			$ 9.733,07
						$ 59.222,32

ELABORADO POR: **A.A.R.CH - E.M.V.S**	FECHA: **12/05/2018**
REVISADO POR: **L.A.L.C**	**FECHA:** 07/05/2018

Tabla 34

Abreviaturas

LISTA DE ABREVIATURAS

PA	Programa de Auditoria
CS	Cedula Sumaria
RE	Registro de Equipo
CCI	Cuestionario de Control Interno
MCR	Matriz de Calificación de Nivel de Confianza y Riesgo
EXE	Examen Especial
AF	Análisis Forense
HH	Hoja de Hallazgo
IA	Informe de Auditoria
BG	Estados Financieros
REF. P/T	Referencia Papel de Trabajo
LALC	Luis Alfonzo Lema Cerda
AARCH	Ángel Alejandro Rosero Chaves
EMVS	Érica Maribel Valverde Soto
Elaborado por: A.A.R.CH – E.M.V.S	Fecha: 23/05/2018
Revisado por: L.A.L.C	Fecha: 24/05/2018

COOPERATIVA DE AHORRO Y CRÉDITO SANTA ROSA DE PATUTÁN LTDA.

LE – 1/1

AUDITORÍA INFORMÁTICA

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

Tabla 35

Lista de Equipos

LISTA DE EQUIPOS					
Nº	**NOMBRE DEL EQUIPO DE COMPUTO**	**RESPONSABLE**	**MARQUE CON UNA X**		**HORAS DE USO**
			USO UNICO	**COMPARTIDO**	
1	CPU QUASAD EC21	VILMA LLUMILUISA	X		9
2	CPU LG EC14	MONICA CHANCUSIG	X		9
3	CPU DELUXE EC10	CRISTIAN YAULE	X		9
4	CPU LG EC05	SILVIA YAULI	X		9
5	CPU LG EC16	DIEGO LAMINGO	X		9
6	CPU LG EC15	KARINA ALMACHI	X		9
7	CPU LG EC25	FLOR NIZA	X		9
8	CPU LG EC17	JESSICA LAMINGO	X		9
Elaborado por: A.A.R.CH - E.M.V.S			Fecha: 21/05/2018		
Revisado por: L.A.L.C			Fecha: 28/05/2018		

4.1. Elaboración y aplicación del Cuestionario de Control Interno

Tabla 36

Cuestionario de Control Interno

CCI – 1/3

COOPERATIVA DE AHORRO Y CRÉDITO SANTA ROSA DE PATUTÁN LTDA.					
MATRIZ DE CALIFICACION DE RIESGO Y CONFIANZA					**AUDITOR:**
CUESTIONARIO DE CONTROL INTERNO					**FECHA:**
Nº	**PREGUNTAS**	**PONDERACION**	**RESPUESTAS**		**CALIFICACION**
			SI	**NO**	
DEPARTAMENTO O AREA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN		PT			CT
SUMAN:					
PROCESOS INTERNOS					
1	¿La Cooperativa cuenta con un profesional con relación de dependencia en el área de sistemas?	1		X	0
2	¿Existe un organigrama con la estructura del área de TIC?	1		X	0
3	¿La Cooperativa cuenta con una política de confidencialidad con la persona que tiene acceso a la información de los socios?	1		X	0
4	¿La instalación (cableada y eléctrica) para el equipo de cómputo se realiza por un profesional del área?	1	X		1
5	¿La Cooperativa tiene generador eléctrico en caso de que existan inesperados cortes eléctricos?	1	X		1
6	¿La entidad cuenta con equipos de protección para el equipo de cómputo reguladores de voltaje?	1		X	0
7	¿Se realizan respaldos físicos o digitales de la información?	1	X		1

CONTINÚA

CCI – 2/3

8	**¿Se realizan informes sobre el rendimiento de los Sistemas Informáticos?**	**1**		**X**	**0**
9	¿La entidad cuenta con claves de seguridad para ingresar al Sistema?	1	X		1
10	¿Se realizan frecuentes mantenimientos del software?	1	X		1
11	¿Se realizan frecuentes mantenimientos del hardware?	1	X		1
12	¿La Cooperativa cuenta con algún plan de actualización, mantenimiento preventivo de los equipos de cómputo de acuerdo a los avances tecnológicos que se presentan día a día?	1		X	0
13	¿La entidad posee cámaras, servidores de video?	1	X		1
14	¿Existe un manual o instructivo para el manejo y uso del Software Informático?	1		X	0
15	¿El profesional encargando del área de TIC capacita al personal que labora dentro de la Cooperativa?	1		X	0
16	¿La Cooperativa cuenta con políticas para la seguridad de los Sistemas Informáticos?	1		X	0
17	¿Los sistemas Informáticos cuentan con licencia para hacer uso de sus términos y condiciones?	1		X	0
18	¿La Cooperativa lleva un registro de acceso cuando una persona (trabajador de la entidad) ingresa a la información de los Sistemas Informáticos?	1		X	0
19	¿La entidad posee sistemas de protección como antivirus frente a ataques informáticos?	1	X		1
20	¿La Cooperativa cuenta con algún servicio para almacenar información dentro de una nube?	1		X	0

CONTINÚA

CCI – 3/3

21	**¿Existe un lugar adecuado y estratégico (distribución del espacio físico) para los sistemas informáticos (hardware, software y personal informático)?**	**1**		**X**	**0**
22	¿El profesional encargado de los Sistemas Informáticos realiza procedimientos de detección de inmunización de virus en todos los equipos de cómputo?	1		X	0
23	¿La Cooperativa cuenta con algún tipo de codificación de la información como medida de protección (encriptación)?	1		X	0
24	¿El sistema informático que maneja la entidad garantiza una excelente calidad de la información?	1	X		1
25	¿El sistema informático que maneja la entidad garantiza transparencia de la información?	1	X		1
26	¿Se ha realizado algún tipo de Auditoría a los Sistemas Informáticos?	1		X	0
27	¿La Cooperativa tiene alguna restricción en los equipos de cómputo para acceso a redes sociales?	1		X	0
28	¿La entidad cuenta con algún servicio informático para recibir notificaciones en el caso de acceso indebido a la información?	1	X		1
29	¿La cooperativa cuenta con una plataforma tecnológica de Banca electrónica?	1	X		1
Calificación Total Componente 1: CT					12
Ponderación Total Componente 1: PT					29
Nivel de Confianza: NC= CT/PT*100		NC=(8/29)*100= 27,59			27,59
Nivel de Riesgo Inherente: RI= 100 % - NC %		RI=100%-27,59%=72,41			72,41
Elaborado por: **A.A.R.CH - E.M.V.S**		**Fecha:** 23/05/2018			
Revisado por: **L.A.L.C**		**Fecha:** 26/05/2018			

COOPERATIVA DE AHORRO Y CRÉDITO SANTA ROSA DE PATUTÁN LTDA.

AUDITORÍA INFORMÁTICA

MATRIZ DE CALIFICACIÓN DEL NIVEL DE CONFIANZA Y RIESGO

DEL 01 DE ENERO AL 31 DE JULIO DE 2018

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 = (8/29)*100

C.P = 27,59

2. Determinación de los niveles de riesgo

Tabla 37

Nivel de Confianza

BAJO	MODERADO	ALTO
15% - 50%	51% - 75%	76% - 95%
85% - 50%	49% - 25%	24% - 4%
ALTO	MODERADO	BAJO

Tabla 38

Nivel de Riesgo

NR = (100 - NC)			
CT	12	RIESGO	ENFOQUE
PT	29		
NC	27,59	BAJO	
RC	72,41	ALTO	CUMPLIMIENTO

3. Conclusión

Después del análisis realizado en la Cooperativa de Ahorro Y Crédito Santa Rosa de Patután Ltda., de acuerdo al componente de tecnología de información y comunicación, se puede afirmar que con un nivel de confianza de 27,59 (Bajo) y su nivel de riesgo de 72,41 (Alto) con respecto a la seguridad; por lo que podemos decir que por inexistencia de un control adecuado en los sistemas informáticos (hardware, software y personal informático) dentro de la cooperativa obtuvimos un resultado bajo en nivel de confianza y alto en respecto al nivel de riesgo, lo que se convierte la cooperativa en tener un alto grado de vulnerabilidad ante un ataque informático.

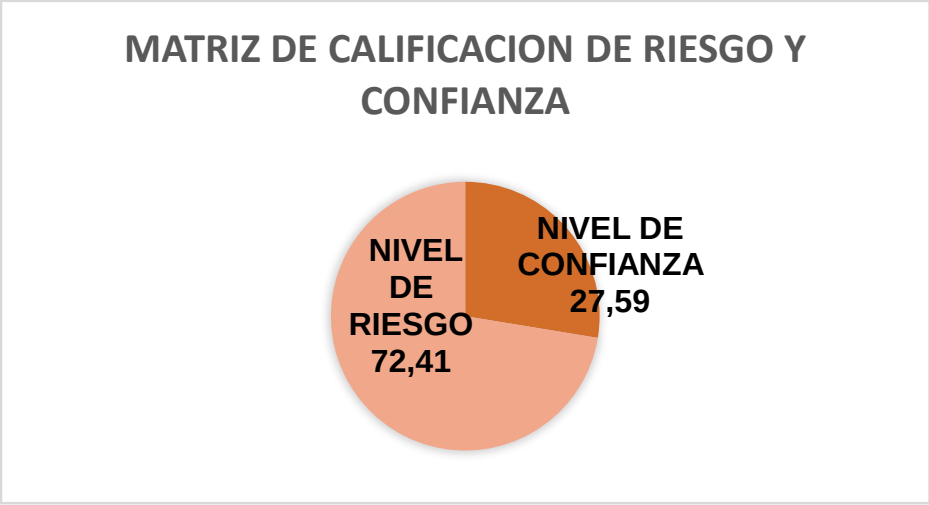


Figura 25. Matriz de calificación de riesgo y confianza

4.2. Examen Especial

4.2.1. Examen especial a los sistemas más vulnerables del departamento de Tecnología de Información y Comunicación

a. Motivo del examen.

El examen especial se realizó a la Cooperativa de Ahorro y Crédito Santa Rosa de Patután, en lo que respecta a nuestro tema de investigación “Fraude Informático, análisis de vulnerabilidad en las empresas del sector servicios reguladas bajo la Superintendencia de Compañías en la provincia de Cotopaxi periodo 2012 - 2016”, al aplicar el cuestionario de control interno identificamos diferentes hallazgos, ocasionando a la cooperativa en tener un alto grado de vulnerabilidad en los sistemas informáticos.

b. Objetivos del examen.

- Determinar el nivel de seguridad y confiabilidad que tienen los sistemas informáticos en la Cooperativa de Ahorro y Crédito Santa Rosa de Patután Ltda.
- Analizar la eficiencia de los sistemas informáticos (hardware, software y personal informático)
- Proponer mejoras en los sistemas informáticos dentro de la Cooperativa.

c. Alcance del examen.

El examen especial se realizó al área de tecnologías de información y comunicación en la Cooperativa de Ahorro y Crédito Santa Rosa de Patután Ltda., en el periodo del 1 de abril del 2018 al 31 de junio de 2018.

d. Base legal.

Con la Autorización de la Ingeniera Mónica del Roció Chancúsig Chisag gerente de la Cooperativa de Ahorro y Crédito Santa Rosa de Patután Ltda., con la ayuda respectiva del Señor Diego Lamingo administrador de la cooperativa, se produjo a la revisión de todas las computadoras tomadas como muestra para la revisión de los sistemas de información.

e. Estructura orgánica.

Gerente: Mónica del Roció Chancúsig Chisag

Administrador: Diego Lamingo

Apoyo operativo: Empresa Megasistemas Compañía Limitada

Apoyo administrativo: Silvia Yauli

f. Recurso examinando.

Tabla 39

Montos de los recursos examinados

Nº	Descripción	Valor USD
1	Computador de escritorio marca LG genérico EC 16 Windows 8, responsable Diego Lamingo, uso único con 9 horas de trabajo	600,00
2	Computador de escritorio marca QUASAD genérico EC 21 Windows 8, responsable Vilma Llumiluisa, uso único con 9 horas de trabajo.	700,00
3	Computador de escritorio marca LG genérico EC 14 Windows 8, responsable Mónica Chancusig, uso único con 9 horas de trabajo.	650,00
4	Computador de escritorio marca DELUXE genérico EC 10 Windows 8, responsable Cristian Yaule, uso único con 9 horas de trabajo.	500,00
5	Computador de escritorio marca LG genérico EC 05 Windows 8, responsable Silvia Yaule, uso único con 9 horas de trabajo.	600,00
6	Computador de escritorio marca LG genérico EC 15 Windows 8, responsable Karina Almachi, uso único con 9 horas de trabajo.	700,00
7	Computador de escritorio marca LG genérico EC 25 Windows 8, responsable Flor Niza, uso único con 9 horas de trabajo.	800,00
8	Computador de escritorio marca LG genérico EC 17 Windows 8, responsable Jessica Lamingo, uso único con 9 horas de trabajo.	600,00

4.2.2. Resultado del examen especial.

a. Seguridad y confiabilidad.

Al momento de realizar dicho examen en la Cooperativa de Ahorro y Crédito Santa Rosa de Patután Ltda., en un computador de marca LG genérico con su número de codificación EC Nº16 se pudo apreciar la seguridad que tienen los equipos al momento e ingresar al sistema, cada trabajador responsable de su equipo de cómputo tiene su usuario y clave de acceso personal que es de uso único e intransferible a una tercera persona.

Por lo tanto se puede decir que al realizar diferentes pruebas para uso y manejo de sistema en este caso el responsable del equipo de cómputo el Señor: Diego Lamingo se realizó el ingreso al sistema con su respectivo usuario y clave de acceso ya que nos supo manifestar que como su computador es de uso único al iniciar su jornada de trabajo el ingresa y al finalizar sus 9 horas de trabajo cierra la sesión de usuario por lo que es una norma dentro de la cooperativa no dejar abierto ningún programa que forma parte del sistema.

Con respecto a la confiabilidad del sistema y aplicaciones informáticas tienen un alto grado de capacidad para realizar las todas las operaciones, funciones que tienen dichas aplicaciones que forman parte del sistema, cada ordenador tiene su actualización vigente en programas, aplicaciones y antivirus.

a. Eficiencia de los sistemas informáticos.

En cuanto a la eficiencia de los programas y aplicaciones informáticos que maneja la cooperativa al realizar una función, operación tiene una excelente capacidad para desarrollar la actividad que se está efectuando con una rapidez adecuada, ya que la cooperativa cuenta con la contratación de servicios tanto en internet MEGASPEED con la responsabilidad del Señor: Ángel Benigno Condolo Guaya, y por parte de la empresa que brinda soporte técnico en cuanto a los sistemas que maneja la cooperativa proviene de la empresa Megasistemas ya que la misma se encarga de solucionar los inconvenientes que se presentan dentro de la entidad con el fin de que el personal que

hace uso del sistema solo se encargan de efectuar operaciones básicas en lo que respecta a la actividad económica de la cooperativa.

Durante el desarrollo de la prueba al computador genérico LG EC16, no se encontró inconvenientes en lo que respecta a cumplir una función o tarea dentro del programa por lo que podemos afirmar que el servicio de la empresa Megasistemas compañía limitada brinda un servicio adecuado a la entidad financiera ya que no han tenido inconvenientes en lo que respecta al uso del software.

a. Mejoras en los sistemas informáticos.

Se recomienda a la entidad financiera contratar los servicios de un profesional a tiempo completo para que este familiarizado con los trabajadores de la cooperativa y el mismo brinde capacitaciones sobre el uso y manejo de los sistemas informáticos en los que se refiere al software para brindar un soporte eficiente en los programas y aplicaciones que se maneja a diario, con el fin de que el profesional encargado tecnología de información TI elabore un manual de uso sobre el sistema y sea compartido con el personal que trabaja con un ordenador.

b. Conclusiones del Examen Especial.

Al desarrollar el examen especial se pudo evidenciar y de esta manera planteamos la siguiente recomendación:

- La Cooperativa de Ahorro Y Crédito Santa Rosa de Patután Ltda., no cuenta con un profesional en el área de sistemas y tampoco tiene un departamento de Tecnología de Información y Comunicación, ya que es muy importante que una entidad que se dedica a brindar servicios financieros cuente con un profesional en el área de sistemas, para disminuir la vulnerabilidad y el riesgo a ser atacados por delincuentes informáticos que se dedican realizar robos tanto de información confidencial que maneja la cooperativa y de esta manera evitamos pérdidas financieras a futuro protegiendo los sistemas informáticos.

- La cooperativa no cuenta con un manual o instructivo que este sea la base del desarrollo de todas las actividades que efectúa el personal cuando realizan operaciones dentro del software, tampoco cuenta con una políticas para la seguridad de los sistemas informáticos esto se convierte a lo largo del tiempo en un bache (debilidad) de la cooperativa ante posibles ataques por parte de terceras personas.
- La cooperativa sufrió un intento de fraude por medio de un correo electrónico inmediatamente tomaron las medidas respectivas convirtiéndose en una amenaza por ello creemos pertinente desarrollar un examen especial forense.

c. Recomendaciones del Examen Especial.

- Se recomienda al gerente de la cooperativa hacer uso de un servicio de almacenamiento de datos por medio de una nube ya que estamos salvaguardando y protegiendo la información confidencial de la entidad, y de esta manera evitamos perdidas de información.
- Se recomienda contratar un profesional en el área de sistemas sea este a tiempo completo o parcial por ende se debe implementar el departamento de tecnología de información y comunicación y este sea responsable de dicho departamento.
- Recomendamos al gerente llevar un registro de las personas que tienen acceso a la información de clientes y cuenta habientes que acuden a ocupar todos los servicios que ofrece la cooperativa, por lo tanto debe existir una bitácora indicando quien ingresa la hora y con qué fin acceden a dicha información con este proceso estamos asegurando, protegiendo la información personal de los socios.
- Se recomienda a la cooperativa hacer uso de un corta fuegos (Firewall) para poder bloquear el acceso no autorizado, de esta manera protegemos y brindamos mayor seguridad que controle los elementos de la red a la computadora, de acuerdo a las necesidades de la empresa.

4.3. Análisis forense digital

ANÀLISIS FORENSE
COOPERATIVA DE AHORRO Y CRÈDITO SANTA ROSA DE PATUTÀN LTDA.

a. Identificación y recopilación de la amenaza o causa de riesgo

a.1 Tipo de fraude que se intentaba realizar y término en una amenaza

Intento de fraude mediante correo electrónico.

b.1 Fecha en el cual sucedió la amenaza o causa de riesgo

Mediados de Año 2017, Junio

c.1 Número de amenazas que ha sido víctima la cooperativa

1 (uno) primera vez durante su existencia

d.1 Como se identificó el "fraude" que término en una amenaza que sufrió la empresa

La información que proporcionó la Gerente de la cooperativa con número de oficio 192/2018 G-COAC SRP supo manifestar e indicar que una persona creo un correo cuenta de correo ficticio y de esta manera solicitaba una transferencia con un valor considerable el mismo fue detectado por el personal de la entidad aplicando normas de seguridad para

realizar transacciones (llamadas al socio o cliente), gracias a este proceso que aplico el personal no se logró dar paso a dicha solicitud por parte del delincuente informático, y se dio parte a la Fiscalía General del Estado en la provincia de Cotopaxi – Latacunga (FGE) para que entre en investigaciones que aún está vigente por el momento y dar con el responsable que intento realizar un fraude y que termino en una amenaza para la cooperativa.

e.1 Identificación del responsable

La información que proporcionó la gerente de la cooperativa con número de oficio 192/2018 g-coac srp de acuerdo a lo descrito previamente, al momento el caso se encuentra en investigaciones por parte de la fiscal general del estado en la provincia de Cotopaxi (FGE), por tanto no se ha podido identificar al responsable que intento atacar con el único propósito de realizar un fraude, que gracias al excelente manejo del personal que labora en la entidad se convirtió en una amenaza sin dejar pérdidas económicas nos indica que el caso ingreso a la fiscalía general del estado en la provincia de Cotopaxi – Latacunga (FGE) y a la fecha del examen especial se encuentra en investigaciones.

f.1 Que tipo de acciones correctivas tomo la entidad.

Como medidas precautelares a los clientes, socios y cooperativa se tomaron acciones para brindar seguridad actualizar datos a los clientes con el fin de que deseen realizar cualquier tipo de transacciones sea este con terceras personas (autorización del titular), optar por realizar llamadas telefónicas a números convencionales y ha operadoras (celulares) que se tiene en la base de datos de la entidad, con este tipo de acciones la cooperativa tiene un respaldo ante cualquier incidente que se puede presentar durante la jornada de trabajo.

g.1 Investigación global después de la amenaza presentada.

Después de dar aviso a la Fiscalía General del Estado (FGE), se han realizado diferentes investigaciones con las personas internas y externas de la cooperativa.

h.1 Luego de la amenaza que presento la cooperativa las actividades diarias cambiaron.

Luego de detectar la amenaza que presentaba la entidad financiera se procedió a poner la denuncia correspondiente con la Gerente de la cooperativa.

i.1 Se realizó un análisis integral después de hecho ocurrido.

Luego de colocar dicha denuncia la investigación quedo en manos de la Fiscalía General del Estado para que desarrolle todas las pruebas y de con los responsables del hecho.

j.1 La amenaza que sufrió la cooperativa que tan relevante fue.

Tuvo un grado de relevancia muy alto porque al no conseguir su objetivo el delincuente informático da una señal de alerta a la cooperativa para que esta opte por tener medidas altas de seguridad.

b. Documentos que validen la evidencia, amenaza que presento la cooperativa

La evidencia que tiene la Cooperativa de Ahorro y Crédito Santa Rosa de Patután es requerimiento que se envía por medio de la creación de un correo falso el cual solicita una transferencia de dinero hablamos de una cantidad considerable que si se llevaba a cado se convertía en una pérdida para la entidad fraude cibernético con la ayuda de un computador con internet (piratería informática Hacking).

c. Análisis de la evidencia

Luego del hecho que se presentó en la cooperativa de ahorro y crédito Santa Rosa de Patután Ltda., se obtuvo la información esencial para el desarrollo de nuestra investigación ya que con la agradecida ayuda que facilitaron el personal que labora dentro de la entidad, pudimos verificar físicamente cómo se maneja el personal durante su jornada de trabajo haciendo uso de los sistemas informáticos (software, hardware y personal informático), con el objetivo de detectar errores ante el uso de los sistemas informáticos y de esta manera minimizar el grado de vulnerabilidad en la entidad, el resultado que se obtuvo después de su respectiva verificación podemos resaltar que la cooperativa no cuenta con un servicio para almacenar la información dentro de una nube ya que la información que tiene la entidad de sus clientes tiene un grado de sensibilidad ante alguna ocurrencia que se puede presentar .en la entidad como es la pérdida o robo de información, también detectamos que no cuentan con un firewall o corta fuegos para poder bloquear el acceso no autorizado, a aginas maliciosas que lo único que causan es daño y que es una de las ventajas que toma los delincuentes informáticos para poder acceder a la información confidencial que maneja la cooperativa, de esta manera no se protege y no brindamos seguridad así no existirán control e la red a la computadora.

4.4. Elaboración de la hoja de Hallazgo

HH – 1/64

COOPERATIVA DE AHORRO Y CRÉDITO SANTA ROSA DE PATUTÁN LTDA.

HOJA DE HALLAZGOS

ÁREA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN

AL 31 DE JULIO DEL 2018

Tabla 40

Hoja de Hallazgos

Nº	Nombre del Hallazgo	Ref./ P.T	Condición	Criterio	Causa	Efecto	Recomendación
1	La inexistencia de un profesional con relación de dependencia en el área de sistemas.	CCI – 1/3	La Cooperativa, no cuenta con un profesional con relación de dependencia el área de sistemas dentro de la entidad.	La Cooperativa no cuenta con capacitaciones dirigidas al personal que está dentro de la entidad manejando los sistemas informáticos.	La Gerente de la Cooperativa no considera necesario contratar los servicios de un profesional a tiempo completo.	Al no contar con un Profesional a tiempo completo, cuando ocurra algún tipo de problemas en los sistemas representa una amenaza para la entidad.	Se recomienda a la Gerente de la Cooperativa contar con un profesional en el área con el objetivo de minimizar posibles daños dentro del sistema y así brindamos seguridad y eficiencia en los sistemas.
2	No cuenta con un manual o instructivo para el	CCI - 2/3	La Cooperativa de Ahorro y Crédito Santa Rosa de Patután Ltda. Mediante la	De acuerdo a la vanguardia tecnológica que tenemos hoy en día en lo que	La Cooperativa en cuanto respecta a la vulnerabilidad a ataques	Al no contar con un manual o instructivo sobre el manejo y uso del software informático el	Recomendamos al profesional encargado que maneja y se ocupa de la tecnología de

CONTINÚA

	manejo y uso del software informático		actividad que manejan es necesario contar con un adecuado manual sobre el manejo del software que tiene la entidad.	respecta a al mundo tecnológico toda persona que labora dentro de una entidad deben estar al tanto sobre el uso y manejo de los sistemas.	informáticos, contar con un manual sobre el uso y manejo de los sistemas estamos disminuyendo el grado o nivel de vulnerabilidad.	personal que desempeña diferentes operaciones por medio del mismo puede cometer errores por no contar con un manual y generaría perdidas.	información y comunicación implementar un manual sobre el uso y manejo de los sistemas que tiene la entidad con el fin de tener operaciones eficientes y disminuir el grado de errores que se pueden cometer.
3	La inexistencia de un organigrama con la estructura del área de TIC	CCI - 2/3	La Cooperativa de acuerdo al segmento que pertenece, no cuenta con un organigrama con la estructura en el área de TIC	Referente a lo que nos indica COBIT 4.1 el área de tecnología de información tiene mucha importancia estar dentro de las organizaciones, brindando un mejor desempeño a la organización.	Al no contar con una información que brinde beneficios a la Cooperativa de Ahorro y Crédito Santa Rosa de Patután Ltda., no cuenta con el área de TIC.	El no tener la entidad el área o departamento de TIC el personal que maneja los equipos y sistemas puede tener un alto grado de manejo indebido en el mismo.	Se recomienda a la Gerente de la cooperativa implementar dentro de la estructura organizacional de la cooperativa un departamento o área de Tecnología de Información y Comunicación con el objetivo de tener eficiencia en todas las operaciones que tiene la misma brindando seguridad a los clientes.
4	No cuenta con un servicio para almacenar la información	CCI – 2/3	La cooperativa no cuenta con un programa que realiza la gestión para almacenar la información con la finalidad de evitar	Las aplicaciones obtienen acceso a la información en la nube mediante una Api. Los proveedores ofrecen servicios	No existe inversión para almacenar la información dentro de una nube por falta de conocimiento y	Al no tener un servicio seguro de almacenamiento en la nube hace que nuestros clientes no	Se recomienda al gerente de la cooperativa, conocer e implementar la herramienta de almacenamiento para resguardar la

CONTINÚA

	dentro de una nube		pérdidas de información.	complementarios diseñados para ayudar a recopilar, administrar la información de la empresa	manejo de la herramienta.	obtengan datos actualizados.	información de la misma.
5	No existen informes sobre el rendimiento de los sistemas informáticos	CCI - 1/3	La Cooperativa de Ahorro y Crédito Santa Rosa de Patután Ltda., no cuenta con ningún tipo de informes donde se pueda evidenciar el rendimiento de los sistemas informáticos, debido a que el profesional encargado de la información no presenta ningún informe.	Para seguridad y protección de la información es necesario que la empresa cuente con respaldos necesarios de informes de los sistemas informáticos	El profesional no emite ningún reporte sobre la información del rendimiento de los sistemas informáticos	Al no existir respaldos físicos de los rendimientos de los sistemas de información, ocasiona un control débil de los mismos dentro de la cooperativa.	Se recomienda al gerente de la empresa, solicitar al profesional un reporte del rendimiento de los sistemas informáticos
6	No cuenta con políticas de seguridad para los sistemas informáticos	CCI – 2/3	La cooperativa de Ahorro y Crédito Santa Rosa de Patután Ltda, no posee con políticas de seguridad para los sistemas informáticos	Las políticas de seguridad requieren un alto compromiso con la empresa, para gestionar adecuadamente la seguridad de la información.	No existe políticas de seguridad por falta de cultura en la seguridad informática	El no tener una política de seguridad genera el riesgo de robo de información sensible y confidencial de la cooperativa	Se recomienda al gerente implementar un manual de políticas para preservar y proteger la confidencialidad, e integridad de la información
7	No existe restricciones	CCI – 3/3	La Cooperativa de Ahorro y Crédito	Los medios sociales	La Cooperativa de Ahorro y	A través de páginas maliciosas la	Se recomienda a la cooperativa crear un

CONTINÚA

	para el acceso a redes sociales	Santa Rosa de Patután Ltda., no cuenta con restricciones debido a que los empleados pueden hacer uso de las redes sociales por ser una herramienta de marketing para la utilización de publicidad y promocionar los servicios de la cooperativa	actualmente tienen una gran repercusión en la sociedad, y el avance tecnológico hace que la empresa debe contar con software de protección de datos	Crédito Santa Rosa de Patután Ltda., no posee con ninguna restricción para bloquear enlaces o sitios web maliciosos y evitar la divulgación de información confidencial de la empresa.	información de la empresa puede sufrir ataques informáticos frecuentemente	programa informático para mayor seguridad que controle los elementos de la red a la computadora, de acuerdo a las necesidades de la empresa.

4.1. Informe de Auditoria Informática

INFORME DE AUDITORÌA INFORMÀTICA

COOPERATIVA DE AHORRO Y CRÉDITO SANTA ROSA DE PATUTÀN LTDA.

UNIVERSIDAD DE LAS FUERZAS ARMADAS

ESPE EXTENSION LATACUNGA

INFORME DE AUDITORÌA

1. Identificación del informe

Auditoría física a los sistemas informáticos (software, hardware y personal informático).

2. Identificación del área auditada

Área de Tecnología de Información y Comunicación (TIC)

3. Identificación de la entidad Auditada

Cooperativa de Ahorro y Crédito Santa Rosa de Patután Ltda.

4. Objetivos de la auditoria

- Evaluar la gestión de tecnología de información (TI).
- Determinar la vulnerabilidad de los sistemas informáticos de la Cooperativa de Ahorro y Crédito Santa Rosa de Patután LTDA.
- Evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

5. Marco referencial

Auditoría Informática

Según (Escuela Administracion Consultorio Contable , 2007, pág. 1) El COBIT es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso.

Es de mucha importancia COBIT cuando vamos aplicar una auditoría con el fin de conseguir una evaluación de los objetivos de control en lo que respecta a tecnología de información y comunicación, su ámbito de aplicación se enfatiza en todas las empresas sin importar a su actividad económica donde intervienen los administrador de tecnología de información, usuarios y auditores que se engloban en el proceso.

Evaluamos la seguridad y la calidad que brindan los sistemas informáticos (software, hardware y personal informático), en el cual nosotros evaluamos los procesos que se llevan a cabo dentro de la organización.

En su publicación de COBIT 4ta edición nos indica que cuenta con 34 procesos que deben ser llevados a cabo con un enfoque práctico para el desarrollo de todos los procesos que tiene una entidad: planificación y organización, adquisición e implementación, estrega y soporte, supervisión y evaluación estos son los cuatro dominios que COBIT indica con lo que en cada dominio cubren 210 objetivos de vigilancia.

Criterios de información de COBIT

Efectividad: se enfoque en la información proporcionada sea de manera correcta y que siempre sea relevante en lo que respecta a los procesos de la entidad en nuestro caso de la Cooperativa de Ahorro y Crédito.

Eficiencia: la información que se entrega siempre debe ser generada con el adecuado empleo de los recursos que tiene la entidad de una manera optimizando los recursos con los que cuenta la misma.

Confidencialidad: la protección de la información que posee la entidad con lo cual estamos resguardando y brindamos confianza a los socios, y no tengan ningún tipo de inconvenientes ante posibles amenazas de una revelación de información por parte de terceros con el fin de dañar la imagen de la entidad.

Cumplimiento: regir en todo lo que los organismos de control nos obligan a cumplir con leyes, reglamentos que está comprometida la entidad.

Integridad: hace referencia a lo preciso de la información siempre que tenga un marco completo de validez, importancia en lo que respecta las expectativas que mantiene la entidad.

Disponibilidad: fácil accesibilidad de la información cuando sea pertinente en cada proceso que mantiene la entidad en cualquier momento que sea necesario, también tiene un enfoque en la protección de los recursos.

Confiabilidad: la entrega de la información debe ser válida y verdadera con el objetivo de que se tomen las mejores decisiones por parte de la entidad y cumplir con todas las responsabilidades que mantiene la misma.

La integridad está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.

6. Hallazgos potenciales

- La inexistencia de un profesional con relación de dependencia en el área de sistemas.
- No cuenta con un manual o instructivo para el manejo y uso del software informático
- La inexistencia de un organigrama con la estructura del área de TIC
- No cuenta con un servicio para almacenar la información dentro de una nube.
- No existen informes sobre el rendimiento de los sistemas informáticos.
- No cuenta con políticas de seguridad para los sistemas informáticos.
- No existe restricciones para el acceso a redes sociales.

7. Alcance de la Auditoría

La auditoría se llevó a cabo en la Cooperativa de Ahorro y Crédito Santa Rosa de Patután Ltda., y se ha realizado especialmente al área de tecnologías de información y comunicación (TIC), evaluando los sistemas informáticos (software, hardware y personal informático) la seguridad física, lógica, respaldo de datos, la documentación general utilizada en la cooperativa, la seguridad de la red y de esta manera se comprobó generalmente utilizando la información obtenida en la aplicación del cuestionario de control interno y mediante la observación.

8. Periodo de ejecución

La auditoría comprende el período del 1 de enero del 2017 al 30 de julio del 2018, donde se realizó un examen especial a los sistemas informáticos mediante el cual se va a determinar el grado de seguridad, confiabilidad y la eficiencia de los sistema informático que maneja la cooperativa, como también al departamento/área de tecnología de información de la Cooperativa de Ahorro y Crédito Santa Rosa de Patután LTDA.

9. Grupo de Trabajo

- Ing. Luis Alfonzo Lema Cerda (Director del Proyecto de Investigación)
- Sr. Ángel Alejandro Rosero Chávez (Investigador)
- Srta. Erica Maribel Valverde Soto (Investigador)

10. Conclusiones del Informe de Auditoria Informática

- La Cooperativa de Ahorro Y Crédito Santa Rosa de Patután Ltda., no cuenta con un profesional que labore a tiempo completo en la entidad, con lo que se convierte en una desventaja al momento de que se pueda presentar un problema en el sistema informático.
- Con el resultado de la investigación podemos afirmar que la entidad no cuenta con una política de confidencialidad con el personal que tiene acceso a la información de los socios y a las cuentas de los mismos, sin contar con una política puede haber fuga de información por parte del personal que labora dentro de la entidad.
- Por parte del profesional del área de tecnología de información y comunicación (TIC) no brinda capacitaciones al personal que hace uso de los sistemas informáticos (hardware, software y personal informático) por lo que podemos decir que el personal no está entrenado o capacitado para el uso y manejo de los sistemas.
- La cooperativa no cuenta con un manual sobre el manejo de los sistemas informáticos, por lo tanto el profesional que está al frente de las TIC debe implementar dicho manual.

11. Recomendaciones al Informe de Auditoria Informática

- Las recomendaciones que se plantearon en la hoja de hallazgos son los más importantes de acuerdo a nuestra auditoria informática dichas recomendaciones son con el único fin de obtener un mejoramiento de los sistemas informáticos y de esta manera la cooperativa por medio del gerente debe tomar mucho en cuenta las siguientes recomendaciones:

- Se recomienda al gerente de la cooperativa contar con un profesional en el área con el objetivo de minimizar posibles daños dentro del sistema y así brindamos seguridad y eficiencia en el mismo.
- Se recomienda al profesional encargado que maneja y se ocupa de la tecnología de información y comunicación implementar un manual sobre el uso y manejo de los sistemas que tiene la cooperativa con el fin de tener operaciones eficientes y disminuir el grado de errores que se pueden cometer.
- Se recomienda al gerente de la cooperativa implementar dentro de la estructura organizacional de la cooperativa un departamento o área de Tecnología de Información y Comunicación con el fin de tener eficiencia en todas las operaciones que tiene la misma brindando seguridad a los clientes.
- Se recomienda al gerente de la empresa, solicitar al profesional un reporte mensual sobre el rendimiento de los sistemas informáticos
- Se recomienda al gerente implementar un manual de políticas para preservar y proteger la confidencialidad, e integridad de la información
- Se recomienda a la cooperativa hacer uso de un corta fuegos (Firewall) para poder bloquear el acceso no autorizado, de esta manera protegemos y brindamos mayor seguridad que controle los elementos de la red a la computadora, de acuerdo a las necesidades de la empresa.
- Se recomienda a la alta gerencia de la cooperativa contratar el servicio de almacenamiento por medio de una nube aumentando la facilidad y velocidad de acceso por medio de internet con el objetivo de resguardar la información que posee la entidad y de esta manera estamos minimizando el riesgo de pérdida o que se borre la información.

12. Fecha del Informe

	PLANTEAMIENTO	EJECUCION	INFORME
FECHA	08 DE MAYO DE 2018	15 DE MAYO DE 2018	29 DE MAYO DE 2018

13. Identificación Y Firma Del Auditor

Ángel Alejandro Rosero Chaves

CI: 050343629-7

Erica Maribel Valverde Soto

CI: 050357927-8

4.2. Resultado de la investigación

4.2.3. Codificación de la Información.

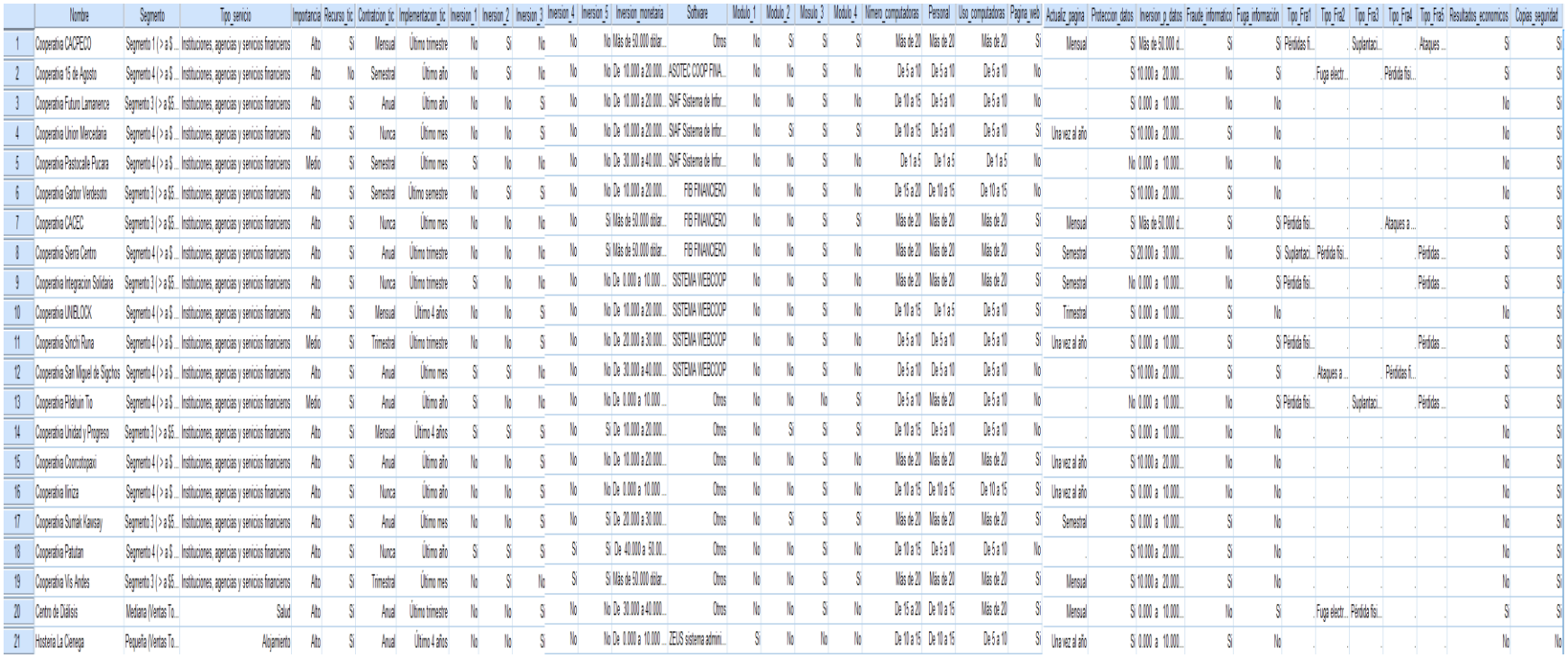
	Nombre	Tipo	Anchura	Decimales	Etiqueta	Valores	Perdidos	Columnas	Alineación	Medida	Rol
1	Nombre	Cadena	60	0	Empresa	Ninguno	Ninguno	23	Izquierda	Nominal	Entrada
2	Segmento	Numérico	8	0	1.¿A que segm...	{1, Segment...	Ninguno	14	Derecha	Ordinal	Entrada
3	Tipo_servicio	Numérico	8	0	2.¿A que activi...	{1, Servicios...	Ninguno	29	Derecha	Nominal	Entrada
4	Importancia	Numérico	8	0	3.¿Desde su p...	{1, Alto}...	Ninguno	7	Derecha	Ordinal	Entrada
5	Recurso_tic	Numérico	8	0	4.¿Considera u...	{1, Si}...	Ninguno	8	Derecha	Nominal	Entrada
6	Contratcion...	Numérico	8	0	5.¿Con què fre...	{1, Mensual...	Ninguno	10	Derecha	Ordinal	Entrada
7	Implementa...	Numérico	8	0	6. ¿Ha implem...	{1, Último m...	Ninguno	13	Derecha	Ordinal	Entrada
8	Inversion_1	Numérico	8	0	Mantenimiento ...	{1, Si}...	Ninguno	7	Derecha	Nominal	Entrada
9	Inversion_2	Numérico	8	0	Compra de equi...	{1, Si}...	Ninguno	8	Derecha	Nominal	Entrada
10	Inversion_3	Numérico	8	0	Compra de soft...	{1, Si}...	Ninguno	8	Derecha	Nominal	Entrada
11	Inversion_4	Numérico	8	0	Capacitación d...	{1, Si}...	Ninguno	8	Derecha	Nominal	Entrada
12	Inversion_5	Numérico	8	0	Licencias y pat...	{1, Si}...	Ninguno	8	Derecha	Nominal	Entrada
13	Inversion_m...	Numérico	8	0	8. ¿Cuánto esti...	{1, De 0.00...	Ninguno	14	Derecha	Ordinal	Entrada
14	Software	Numérico	8	0	9.- ¿Qué tipo d...	{1, MILENIU...	Ninguno	15	Derecha	Nominal	Entrada
15	Modulo_1	Numérico	8	0	ERP (Planificac...	{1, Si}...	Ninguno	8	Derecha	Nominal	Entrada
16	Modulo_2	Numérico	8	0	CRM (Gestión ...	{1, Si}...	Ninguno	8	Derecha	Nominal	Entrada

CONTINÚA

17	Mosulo_3	Numérico	8	0	SIAF (Sistema...	{1, Si}...	Ninguno	8	Derecha	Nominal	Entrada
18	Modulo_4	Numérico	8	0	SAP (Sistemas...	{1, Si}...	Ninguno	8	Derecha	Nominal	Entrada
19	Nímero_co...	Numérico	8	0	11. ¿Cuántas c...	{1, De 1 a 5...	Ninguno	15	Derecha	Ordinal	Entrada
20	Personal	Numérico	8	0	12. ¿Cuántas p...	{1, De 1 a 5...	Ninguno	8	Derecha	Ordinal	Entrada
21	Uso_compu...	Numérico	8	0	13. ¿Cuál es el...	{1, De 1 a 5...	Ninguno	13	Derecha	Ordinal	Entrada
22	Pagina_web	Numérico	8	0	14. ¿Dispone s...	{1, Si}...	Ninguno	8	Derecha	Nominal	Entrada
23	Actualiz_pa...	Numérico	8	0	15. ¿Con que fr...	{1, Cada qui...	Ninguno	11	Derecha	Ordinal	Entrada
24	Proteccion_...	Numérico	8	0	16. ¿Está su e...	{1, Si}...	Ninguno	12	Derecha	Nominal	Entrada
25	Inversion_p_...	Numérico	8	0	17. ¿Hasta cuá...	{1, 0.000 a ...	Ninguno	12	Derecha	Ordinal	Entrada
26	Fraude_infor...	Numérico	8	0	18. ¿Considera...	{1, Si}...	Ninguno	12	Derecha	Nominal	Entrada
27	Fuga_inform...	Numérico	8	0	19. ¿En los últi...	{1, Si}...	Ninguno	12	Derecha	Nominal	Entrada
28	Tipo_Fra1	Numérico	8	0	20. ¿Qué tipo d...	{1, Pérdida f...	Ninguno	8	Derecha	Nominal	Entrada
29	Tipo_Fra2	Numérico	8	0	20. ¿Qué tipo d...	{1, Pérdida f...	Ninguno	8	Derecha	Nominal	Entrada
30	Tipo_Fra3	Numérico	8	0	20. ¿Qué tipo d...	{1, Pérdida f...	Ninguno	8	Derecha	Nominal	Entrada
31	Tipo_Fra4	Numérico	8	0	20. ¿Qué tipo d...	{1, Pérdida f...	Ninguno	8	Derecha	Nominal	Entrada
32	Tipo_Fra5	Numérico	8	0	20. ¿Qué tipo d...	{1, Pérdida f...	Ninguno	7	Derecha	Nominal	Entrada
33	Resultados...	Numérico	8	0	21. Consideran...	{1, Si}...	Ninguno	16	Derecha	Nominal	Entrada
34	Copias_seg...	Numérico	8	0	22. ¿Realiza co...	{1, Si}...	Ninguno	13	Derecha	Nominal	Entrada

Figura 26. Ingreso de datos de las variables

4.2.4. Codificación de la Información.



	Nombre	Segmento	Tipo_servicio	Importancia	Recurso_tic	Contratacion_tic	Implementacion_tic	Inversion_1	Inversion_2	Inversion_3	Inversion_4	Inversion_5	Inversion_monetaria	Software	Modulo_1	Modulo_2	Mesulo_3	Modulo_4	Numero_computadoras	Personal	Uso_computadoras	Pagina_web	Actualiz_pagina	Proteccion_datos	Inversion_y_datos	Fraude_informatico	Fuga_información	Tipo_Fris1	Tipo_Fris2	Tipo_Fris3	Tipo_Fris4	Tipo_Fris5	Resultados_economicos	Copias_seguridad
1	Cooperativa CACPECO	Segmento 1 (> a $...	Instituciones, agencias y servicios financieros	Alto	Si	Mensual	Último trimestre	No	Si	No	No	No	Más de 50.000 dólar...	Otros	No	Si	Si	Si	Más de 20	Más de 20	Más de 20	Si	Mensual	Si	Más de 50.000 d...	Si	Si	Pérdidas fi...		Suplantaci...		Ataques ...	Si	Si
2	Cooperativa 15 de Agosto	Segmento 4 (> a $ ...	Instituciones, agencias y servicios financieros	Alto	No	Semestral	Último año	No	Si	No	No	No	De 10.000 a 20.000...	ASOTEC COOP FINA...	No	No	Si	No	De 5 a 10	De 5 a 10	De 5 a 10	No		Si	10.000 a 20.000...	No	Si		Fuga electr...		Pérdida fisi...		Si	Si
3	Cooperativa Futuro Lamanence	Segmento 3 (> a $5...	Instituciones, agencias y servicios financieros	Alto	Si	Anual	Último año	No	No	Si	No	No	De 10.000 a 20.000...	SAF Sistema de Infor...	No	No	Si	No	De 10 a 15	De 5 a 10	De 5 a 10	No		Si	0.000 a 10.000...	No	No						No	Si
4	Cooperativa Union Mercedaria	Segmento 4 (> a $ ...	Instituciones, agencias y servicios financieros	Alto	Si	Nunca	Último mes	No	No	Si	No	No	De 10.000 a 20.000...	SAF Sistema de Infor...	No	Si	Si	Si	De 10 a 15	De 5 a 10	De 5 a 10	Si	Una vez al año	Si	10.000 a 20.000...	Si	No						No	Si
5	Cooperativa Pastocalle Pucara	Segmento 4 (> a $ ...	Instituciones, agencias y servicios financieros	Medio	Si	Semestral	Último mes	Si	No	No	No	No	De 30.000 a 40.000...	SAF Sistema de Infor...	No	No	Si	No	De 1 a 5	De 1 a 5	De 1 a 5	No		No	0.000 a 10.000...	No	No						No	Si
6	Cooperativa Garbor Verbesito	Segmento 3 (> a $5...	Instituciones, agencias y servicios financieros	Alto	Si	Semestral	Último semestre	No	Si	Si	No	No	De 10.000 a 20.000...	FIB FINANCIERO	No	No	Si	No	De 15 a 20	De 10 a 15	De 10 a 15	No		Si	10.000 a 20.000...	Si	No						No	Si
7	Cooperativa CACEC	Segmento 3 (> a $5...	Instituciones, agencias y servicios financieros	Alto	Si	Nunca	Último mes	No	No	No	Si	Más de 50.000 dólar...		FIB FINANCIERO	No	No	Si	Si	Más de 20	Más de 20	Más de 20	Si	Mensual	Si	Más de 50.000 d...	Si	Si	Pérdida fisi...			Ataques a ...		Si	Si
8	Cooperativa Sierra Centro	Segmento 4 (> a $ ...	Instituciones, agencias y servicios financieros	Alto	Si	Anual	Último trimestre	No	No	No	Si	Más de 50.000 dólar...		FIB FINANCIERO	No	No	Si	No	Más de 20	Más de 20	Más de 20	Si	Semestral	Si	20.000 a 30.000...	No	Si	Suplantaci...	Pérdida fisi...			Pérdidas ...	Si	Si
9	Cooperativa Integracion Solidaria	Segmento 3 (> a $5...	Instituciones, agencias y servicios financieros	Alto	Si	Nunca	Último trimestre	Si	No	No	No	No	De 0.000 a 10.000 ...	SISTEMA WEBCOOP	No	No	Si	No	Más de 20	Más de 20	Más de 20	Si	Semestral	No	0.000 a 10.000...	No	Si	Pérdida fisi...				Pérdidas ...	Si	Si
10	Cooperativa UNBLOCK	Segmento 4 (> a $ ...	Instituciones, agencias y servicios financieros	Alto	Si	Mensual	Último 4 años	No	No	Si	No	No	De 10.000 a 20.000...	SISTEMA WEBCOOP	No	No	Si	No	De 10 a 15	De 1 a 5	De 5 a 10	Si	Trimestral	Si	0.000 a 10.000...	Si	No						No	Si
11	Cooperativa Sinchi Runa	Segmento 4 (> a $ ...	Instituciones, agencias y servicios financieros	Medio	Si	Trimestral	Último trimestre	No	No	Si	No	No	De 20.000 a 30.000...	SISTEMA WEBCOOP	No	No	Si	No	De 5 a 10	De 5 a 10	De 5 a 10	Si	Una vez al año	Si	0.000 a 10.000...	Si	Si	Pérdida fisi...				Pérdidas ...	Si	Si
12	Cooperativa San Miguel de Sigchos	Segmento 4 (> a $ ...	Instituciones, agencias y servicios financieros	Alto	Si	Anual	Último mes	Si	Si	No	No	No	De 30.000 a 40.000...	SISTEMA WEBCOOP	No	No	Si	No	De 5 a 10	De 5 a 10	De 5 a 10	No		Si	10.000 a 20.000...	Si	Si		Ataques a ...		Pérdidas fi...		Si	Si
13	Cooperativa Pilahuin Tio	Segmento 4 (> a $ ...	Instituciones, agencias y servicios financieros	Medio	Si	Anual	Último año	Si	No	No	No	No	De 0.000 a 10.000 ...	Otros	No	No	No	Si	De 5 a 10	Más de 20	De 5 a 10	No		No	0.000 a 10.000...	No	Si	Pérdida fisi...		Suplantaci...		Pérdidas ...	Si	Si
14	Cooperativa Unidad y Progreso	Segmento 3 (> a $5...	Instituciones, agencias y servicios financieros	Alto	Si	Mensual	Último 4 años	Si	Si	Si	No	Si	De 10.000 a 20.000...	Otros	No	Si	Si	Si	De 10 a 15	De 5 a 10	De 5 a 10	No		Si	0.000 a 10.000...	No	No						No	Si
15	Cooperativa Cooncotopaxi	Segmento 4 (> a $ ...	Instituciones, agencias y servicios financieros	Alto	Si	Anual	Último año	No	No	Si	No	No	De 10.000 a 20.000...	Otros	No	No	Si	No	Más de 20	Más de 20	Más de 20	Si	Una vez al año	Si	10.000 a 20.000...	No	No						No	Si
16	Cooperativa Ilinca	Segmento 4 (> a $ ...	Instituciones, agencias y servicios financieros	Alto	Si	Nunca	Último año	No	No	Si	No	No	De 0.000 a 10.000...	Otros	No	No	Si	No	De 10 a 15	De 10 a 15	De 10 a 15	Si	Una vez al año	Si	0.000 a 10.000...	No	No						No	Si
17	Cooperativa Sumak Kawsay	Segmento 3 (> a $5...	Instituciones, agencias y servicios financieros	Alto	Si	Anual	Último mes	No	No	Si	No	Si	De 20.000 a 30.000...	Otros	No	Si	Si	Si	Más de 20	Más de 20	Más de 20	Si	Semestral	Si	0.000 a 10.000...	Si	No						No	Si
18	Cooperativa Patutan	Segmento 4 (> a $ ...	Instituciones, agencias y servicios financieros	Alto	Si	Nunca	Último año	Si	Si	Si	Si	Si	De 40.000 a 50.00...	Otros	No	No	Si	No	De 10 a 15	De 5 a 10	De 5 a 10	No		Si	10.000 a 20.000...	Si	No						No	Si
19	Cooperativa Vis Andas	Segmento 3 (> a $5...	Instituciones, agencias y servicios financieros	Alto	Si	Trimestral	Último mes	No	Si	No	Si	Si	Más de 50.000 dólar...	Otros	No	No	Si	Si	Más de 20	Más de 20	Más de 20	Si	Mensual	Si	10.000 a 20.000...	Si	No						No	Si
20	Centro de Diálisis	Mediana (Ventas To...	Salud	Alto	Si	Anual	Último trimestre	No	No	Si	No	No	De 30.000 a 40.000...	Otros	No	No	Si	No	De 15 a 20	De 10 a 15	Más de 20	Si	Mensual	Si	0.000 a 10.000...	No	Si	Fuga electr...	Pérdida fisi...				Si	Si
21	Hostería La Ciénega	Pequeña (Ventas To...	Alojamiento	Alto	Si	Anual	Último 4 años	No	No	Si	No	No	De 0.000 a 10.000 ...	ZEUS sistema admini...	Si	No	No	No	De 10 a 15	De 10 a 15	De 5 a 10	Si	Una vez al año	Si	0.000 a 10.000...	Si	No						No	No

Figura 27. Ingreso del resultado de las variables

Para realizar la tabulación de la encuesta y el cruce de variables optamos por utilizar el programa SPSS, con esta herramienta muy importante realizamos un proceso efectivo y rápido.

4.3. Análisis de los resultados

Prueba de hipótesis

Al desarrollar la tabulación de las encuestas aplicadas a las entidades financieras reguladas por la Superintendencia de Compañías y la Superintendencia de Economía Popular y Solidaria (SEPS), ocupamos la herramienta del SPSS, es un software estadístico que nos permite analizar los datos obtenidos. Al comprobar la hipótesis se afirma que los fraudes informáticos no tienen ninguna incidencia en los resultados económicos en las empresas del sector servicios financieros en la provincia de Cotopaxi.

4.4. Comprobación de hipótesis

Para comprobar la hipótesis utilizamos el estadístico CHI CUADRADO que permite verificar sobre la proporcionalidad de las variables, en el sentido de la igualdad en proporciones para las variables tanto independientes como dependientes en la tabla de contingencia (prueba de independencia).

4.4.1. Planteamiento de hipótesis.

Hipótesis nula

Los fraudes informáticos no inciden en los resultados económicos financieros de las empresas del sector de servicios reguladas por la Superintendencia de Economía Popular y solidaria y la Superintendencia Compañías de la Provincia de Cotopaxi

Hipótesis Alternativa

Los fraudes informáticos inciden en los resultados económicos financieros de las empresas del sector de servicios reguladas por la Superintendencia de Economía Popular y solidaria y la Superintendencia de Compañías de la Provincia de Cotopaxi.

a. Nivel de Significancia.

Se elige un nivel de significancia (α) del 5% esto significa tener la probabilidad del 0,05 de cometer el ERROR TIPO I, es decir “Rechazar la hipótesis alternativa siendo esta verdadera” por tal razón como esta probabilidad es pequeña es muy difícil rechazar. Los fraudes informáticos inciden en los resultados económicos financieros de las empresas siendo esto verdadero.

Se aplica el estadístico chi-cuadrado tomando los resultados de la encuesta según la pregunta 20. ¿Qué tipo de fraude informático ha sufrido su empresa? Y la pregunta 21. ¿Considerando la respuesta que usted dio en la pregunta anterior, los fraudes informáticos afectan a los resultados económicos financieros de la empresa?

Grados de libertad= (número de filas menos uno) *(número de columnas menos uno)

Grados de libertad = (5-1)*(2-1) = 4 el estadístico que delimita la zona de aceptación y rechazo es para aceptar o rechazar la hipótesis nula:

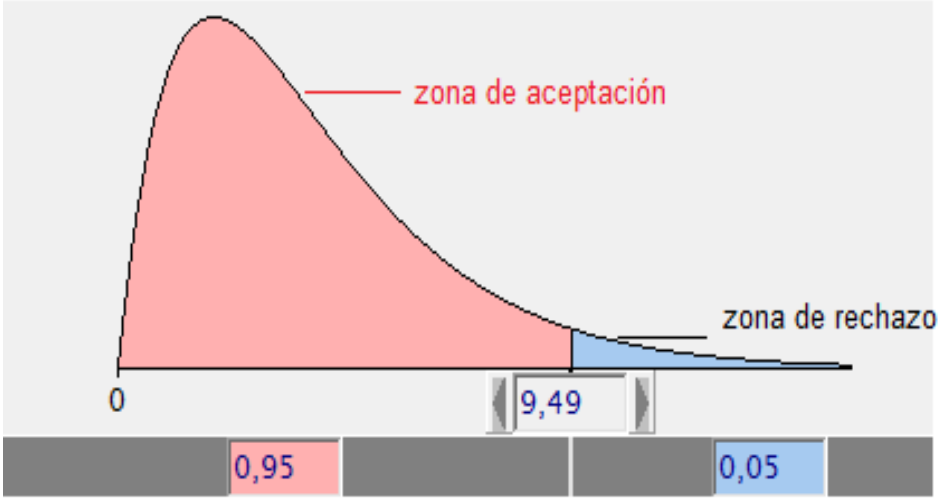


Figura 28. Comprobación de Hipótesis

Fuente: Tabla ji-cuadrado

Tabla 41

JI CUADRADO

Grados de	**Probabilidad**										
Libertad	0,95	0,90	0,80	0,70	0,50	0,30	0,20	0,10	0,05	0,01	0,001
1	0,004	0,02	0,06	0,15	0,46	1,07	1,64	2,71	3,84	6,84	10,83
2	0,1	0,21	0,45	0,71	1,39	2,41	3,22	4,6	5,99	8,21	13,82
3	0,35	0,58	1,01	1,42	2,37	3,66	4,64	6,25	7,82	11,34	16,27
4	0,71	1,06	1,65	2.20	3,36	4,88	5,99	7,78	9,49	13,28	18,47
5	1,14	1,61	2,34	3	4,35	6,06	7,23	9,24	11,07	15,09	20,52
6	1,63	2,2	3,07	3,83	5,35	7,23	8,38	10,64	12,59	16.81	22,46
7	2,17	2,83	3,82	4,67	6,35	8,38	9,8	12,02	14,07	18,48	24,32
8	2,73	3,49	4,59	5,53	7,34	9,52	11,03	13,36	15,51	20,09	26,12
9	3,32	4,17	5,38	6,39	8,34	10,66	12,24	14,68	16,92	21,67	27,88
10	3,94	4,86	6,18	7,27	9,34	11,78	13,44	15,99	18,31	23,21	29,59
			No significativo							Significativo	

Fuente: (Webster, 2000)

b. Determinación Del Estadístico mediante SPSS.

fo: frecuencias observadas

fe: frecuencias esperadas

Tabla 42

Resultados obtenidos de las frecuencias observadas y esperadas

			Los fraudes informáticos afectan a los resultados económicos financieros de la empresa		Total
			Si	No	
Fraude informático	Pérdida física de dispositivos o medios que contengan datos	Recuento	7	14	21
		Recuento esperado	4	17	21
	Fuga electrónica de datos de los sistemas internos	Recuento	2	19	21
		Recuento esperado	4	17	21
	Suplantación de identidad/ ingeniería social en cuentas	Recuento	3	18	21
		Recuento esperado	4	17	21
	Ataques a servicios bancarios en línea	Recuento	3	18	21
		Recuento esperado	4	17	21
	Pérdidas financieras debidas a ataques en cajeros	Recuento	6	15	21
		Recuento esperado	4	17	21
Total		Recuento	21	84	105
		Recuento esperado	21	84	105
Pruebas de chi-cuadrado					

CONTINÚA

	Valor	gl	Significación asintótica (bilateral)
Chi 2 de Pearson	5,60	4	0,23
N°- de casos válidos	21		

Fuente: Encuestas

c. Decisión.

Como 5,60 es menor a 9,49 zona de aceptación por tanto acepto la hipótesis nula y rechazo la hipótesis alternativa.

d. Conclusión

Con un nivel de significancia del 5% podemos afirmar que: Los fraudes informáticos no inciden en los resultados económicos financieros de las empresas del sector de servicios reguladas por la Superintendencia de Compañías de la Provincia de Cotopaxi.

4.5. Tendencia de fraudes Informáticos

De acuerdo a publicaciones emitidas por ecuavisa (Jesuarez, 2015) “En el país, de enero a octubre de 2015, la Fiscalía General del Estado registra 1.254 denuncias de delitos informáticos y las provincias con mayor número de casos son Guayas (406) y Pichincha (388)”.

En el Ecuador a lo largo del tiempo ha tenido un aumento en ataques informáticos esto con respecto al crecimiento económico que ha generado el país por lo que para los ciberdelincuentes se convierte en una ventaja “Hay hackers que atacan desde Perú, Colombia o Europa occidental a los bancos ecuatorianos, lo que antes no sucedía, pues se trata es un delito importado”, indica (El Universo, 2014)

El delito más cometido es la apropiación fraudulenta de dinero o información por medios electrónicos, tipificado en el artículo 190 del Código Orgánico Integral Penal (COIP), y que registra 800 casos. Según indica (Jesuarez, 2015)

Podemos concluir que debido a las ventajas que son presentadas por los delincuentes informáticos hace que se convierta en una debilidad para las empresas ecuatorianas a ser atacadas por algún tipo de fraude dejando como resultados pérdidas económicas ya que los sistemas informáticos que usan las empresas de servicios son vulnerables a hackers.

Según (El comercio , 2014) indica que “Los ataques informáticos se han convertido en una industria global que alcanza ya cerca de los USD 500 000 millones y sigue creciendo”

También nos indica el (El comercio, 2015) “El 98,5 % de los riesgos bancarios en América Latina y el Caribe son digitales o informáticos, según un estudio de la Federación Latinoamericana de Bancos (Felaban)”

Esto nos quiere decir que los ataques o daños informáticos que sufren las empresas son a nivel mundial generando grandes pérdidas económicas lo que implica que es un tema difícil de tratar y de controlar ya que atacan de diferentes partes del mundo intentando lograr su objetivo que es el robo de información y de dinero. El avance de la tecnología tiene mucho que ver en lo que respecta a los servicios financieros en línea ya que este se convierte en una puerta de entrada para que los hackers cometan sus fechorías, y los usuarios o socios que tienen dinero en instituciones financieras no se acerquen a los bancos y todo se realice mediante un teléfono inteligente según las necesidades o requerimientos del mismo.

4.6. Tendencia de inversión en tecnología de información y comunicación (TIC) en las empresas del sector servicios en la provincia de Cotopaxi periodo 2012 – 2016

La información acerca de las empresas del sector servicios nos facilitaron la Superintendencia de compañías SUPERCIAS y la Superintendencia de economía popular y solidaria SEPS con los balances generales que nos entregaron nosotros como investigadores podemos observamos y verificamos la inversión que tiene cada empresa en la cuenta Equipo de Cómputo y Software por lo que con estos montos que tiene cada entidad nosotros procedemos a ver la tendencia que tienen en los últimos cuatro años 2012 - 2016.

Tabla 43

Monto de Inversión en los segmento del 1 al 4 reguladas bajo la SEPS

RAZÓN SOCIAL	2012	2012	2013	2015	2016
EDUCADORES PRIMARIOS DEL COTOPAXI	$ 39.544,05	$ 39.544,05	$ 75.530,24	$ 90.913,86	$ 111.877,61
DE LA PEQUEÑA EMPRESA DE COTOPAXI LTDA	$712.961,97	$873.331,25	$955.776,76	$1.032.230,38	$1.234.952,88
SAN MIGUEL DE SIGCHOS	$ 7.052,04	$ 7.052,04	$ 9.163,04	$ 3.820,71	$ 3.065,30
UNION MERCEDARIA LTDA	$ 14.166,32	$ 14.166,32	$ 16.864,92	$ 17.812,71	$ 17.117,04
FUTURO LAMANENSE	$ 31.349,31	$ 31.349,31	$ 40.747,08	$ 52.607,82	$ 58.730,43
SUMAK KAWSAY LTDA	$ 33.715,83	$ 33.715,83	$ 45.114,78	$ 56.289,57	$ 66.002,49
PILAHUIN	$ 20.556,15	$ 20.556,15	$ 28.270,84	$ 29.781,72	$ 29.781,72
15 DE AGOSTO DE PILACOTO	$ 14.740,36	$ 14.740,36	$ 19.216,70	$ 16.374,70	$ 16.754,70
ILINIZA LTDA	$ 17.435,69	$ 17.435,69	$ 26.207,52	$ 26.738,77	$ 30.104,16
UNIBLOCK Y SERVICIOS LTDA	$ 8.955,86	$ 8.955,86	$ 8.955,86	$ 9.939,93	$ 11.560,43
COORCOTOPAXI LTDA	$ 18.513,18	$ 18.513,18	$ 19.985,03	$ 19.985,03	$ 22.515,46
PUCARA LTDA	$ 5.720,90	$ 5.720,90	$ 7.952,90	$ 9.083,30	$ 11.283,90
SINCHI RUNA LTDA	$ 9.098,08	$ 9.098,08	$ 12.294,55	$ 13.700,55	$ 15.031,06
SANTA ROSA DE PATUTAN LTDA	$ 9.954,31	$ 9.954,31	$ 10.514,31	$ 10.514,31	$ 9.733,07

CONTINÚA

INTEGRACION SOLIDARIA LTDA	$ 28.571,77	$ 28.571,77	$ 31.244,77	$ 32.463,73	$ 48.968,50
SIERRA CENTRO LTDA	$116.793,15	$ 116.793,15	$ 125.579,15	$ 131.863,72	$ 138.358,50
VISION DE LOS ANDES VISANDES	$ 32.851,17	$ 32.851,17	$ 66.458,18	$ 92.695,26	$ 111.638,68
UNIDAD Y PROGRESO	$ 12.900,89	$ 12.900,89	$ 13.721,87	$ 20.291,05	$ 22.770,86
HERMES GAIBOR VERDESOTO	$ 21.960,84	$ 21.960,84	$ 31.338,92	$ 37.841,14	$ 25.419,62

4.7. Evaluación de los resultados obtenidos durante la investigación

4.7.1. Cruce de variables de la investigación.

El cruce de variables es una herramienta muy importante que nos permite realizar un análisis de datos de nuestra investigación se lo realizan a algunas preguntas que están direccionadas con la investigación y nos facilitan la recolección de información que nos ayudan a ampliar, determinar la correlación que tienen las variables.

4.8. Evaluación de los resultados

Tabla 44

Cruce de Variable N° 1

			8. ¿Cuánto estima usted que ha invertido en Tecnología de Información y Comunicación (TIC) durante el periodo 2012 - 2016?						
			De 0.000 a 10.000 dólares	**De 10.000 a 20.000 dólares**	**De 20.000 a 30.000 dólares**	**De 30.000 a 40.000 dólares**	**De 40.000 a 50.000 dólares**	**Más de 50.000 dólares**	Total
1. ¿A qué segmento pertenece la entidad financiera?	Segmento 1 (> a $ 80.000.000)	Recuento	0	0	0	0	0	1	1
		% dentro de 1	0,0%	0,0%	0,0%	0,0%	0,0%	100,0%	100,0%
	Segmento 3 (> a $5.000.000 hasta $20.000.000)	Recuento	1	3	1	0	0	2	7
		% dentro de 1	14,3%	42,9%	14,3%	0,0%	0,0%	28,6%	100,0%
	Segmento 4 (> a $ 1.000.000 hasta $5.000.000)	Recuento	2	4	1	2	1	1	11
		% dentro de 1	18,2%	36,4%	9,1%	18,2%	9,1%	9,1%	100,0%
	Pequeña (Ventas Totales: $100.001-$1.000.000)	Recuento	1	0	0	0	0	0	1
		% dentro de 1	100,0%	0,0%	0,0%	0,0%	0,0%	0,0%	100,0%

CONTINÚA

	Mediana (Ventas Totales: $ 1.000.001-$5.000.000)	Recuento	0	0	0	1	0	0	1
		% dentro de 1	0,0%	0,0%	0,0%	100,0%	0,0%	0,0%	100,0%
Total		Recuento	4	7	2	3	1	4	21
		% dentro de 1	19,0%	33,3%	9,5%	14,3%	4,8%	19,0%	100,0%

Interpretación:

De acuerdo a las preguntas seleccionadas podemos decir que con respecto a cada segmento en el cual se encuentra cada cooperativa tiene su nivel de inversión en TIC por lo tanto en el cuadro de cruce de variables tenemos en el segmento tres y cuatro que tienen inversión considerable con respecto a la tecnología de información y comunicación en el segmento tres con un 42.9%, en cuanto al segmento cuatro tenemos 36.4% en un rango de inversión de $ 10.000 a $20.000 dólares, por lo que en estos dos segmentos existe un número considerable de cooperativas, en lo que se puede decir en cuanto a las pequeñas y medianas empresas tiene un nivel de inversión de $0.00 a $40.000 dólares esto con respecto a su actividad económica dentro se los servicios por lo que es indispensable tener una inversión considerable en TIC. La inversión en tecnología de información y comunicación a las empresas de servicios tiene un gran impacto en lo que se refiere a servicios de acceso de información, proceso de datos que desee el usuario, crear canales de información y el almacenamiento de información en grandes cantidades por lo que nos permite el manejo rápido y fácil de la información en cualquier lugar que nos encontremos.

Tabla 45

Cruce de Variable N° 2

			9.- ¿Qué tipo de software contable maneja la entidad?						
			ASOTEC COOP FINANCIAL	**SIAF Sistema de Información y Adm. Financiera**	**FIB FINANCIERO**	**SISTEMA WEBCOOP**	**Otros**	**ZEUS sistema administrativo**	Total
2. ¿A qué actividad de servicios se dedica su empresa?	Salud	Recuento	0	0	0	0	1	0	1
		% del total	0,0%	0,0%	0,0%	0,0%	4,8%	0,0%	4,8%
	Instituciones, agencias y servicios financieros	Recuento	1	3	3	4	8	0	19
		% del total	4,8%	14,3%	14,3%	19,0%	38,1%	0,0%	90,5%
	Alojamiento	Recuento	0	0	0	0	0	1	1
		% del total	0,0%	0,0%	0,0%	0,0%	0,0%	4,8%	4,8%
Total		Recuento	1	3	3	4	9	1	21
		% del total	4,8%	14,3%	14,3%	19,0%	42,9%	4,8%	100,0%

Interpretación:

De acuerdo a las preguntas que tenemos en el siguiente cruce de información podemos distinguir en el sector servicios con mayor número en este caso es el de servicios financieros por lo que las entidades de este sector deben manejar un

software contable eficiente y seguro con el propósito de no tener ningún tipo de problemas en el desarrollo de las actividades diarias que existen día a día, por lo cual podemos identificar que con un porcentaje de 4.8% manejan el software ASOTEC COOP FINANCIAL ya que este tipo de software es muy usado por algunas cooperativas ya que cuenta con un servicio adecuado a las necesidades de la entidades de servicios financieros, con un 14.3% utilizan los servicios del software SIAF (Sistema de Información y Adm. Financiera) y FIB FINANCIERO estos resultados de acuerdo al monto de inversión que cada cooperativa tiene las condiciones de implementar en el paquete de servicios que tiene cada software por lo que en consideración se puede afirmar que esto va en relación al segmento y montos de inversión de acuerdo a la información recolectada en nuestra investigación nos indicaban que cada entidad financiera tiene sus requerimientos y necesidades dependiendo sus montos de inversión que tiene cada una de ellas, esto también con respecto al nivel de socio y todo tipo transacciones que solicitan los clientes, con un 38.1% manejan otros tipos de software.

En lo que respecta a las empresas del sector servicios reguladas por la Superintendencia de Compañías tenemos salud mantiene un software de otro tipo con diferentes servicios de acuerdo a sus necesidades por lo que en alojamiento (hostería) utilizan el software ZEUS Sistema Administrativo esto va direccionado a empresas que tiene el servicio de alojamiento.

Tabla 46

Cruce de Variable N° 3

			20. ¿Qué tipo de fraude informático ha sufrido su empresa?					Total
			Pérdida física de dispositivos o medios que contengan datos	Fuga electrónica de datos de los sistemas internos	Suplantación de identidad/ ingeniería social en cuentas	Ataques a servicios bancarios en línea	Pérdidas financieras debidas a ataques en cajeros automáticos	
2. ¿A qué actividad de servicios se dedica su empresa?	Salud	Recuento	1	1	0	0	0	1
		% dentro de $A	14,3%	50,0%	0,0%	0,0%	0,0%	
		% del total	11,1%	11,1%	0,0%	0,0%	0,0%	11,1%
	Instituciones, agencias y servicios financieros	Recuento	6	1	3	3	6	8
		% dentro de $A	85,7%	50,0%	100,0%	100,0%	100,0%	
		% del total	66,7%	11,1%	33,3%	33,3%	66,7%	88,9%
Total		Recuento	7	2	3	3	6	9
		% del total	77,8%	22,2%	33,3%	33,3%	66,7%	100,0%

Interpretación:

Este tipo de cruce de variables está dirigida en el tipo de fraudes informáticos que ha sufrido las empresas con el tipo de actividad que mantienen las empresas de servicios de salud e Instituciones, agencias y servicios financieros.

Después de conocer los niveles de inversión que tiene cada empresa o cooperativa nos dirigimos directamente a la pregunta que tiene que ver con los tipos de fraudes informáticos que han sido víctimas las cooperativas como empresas que brindan servicios a la sociedad por lo que se puede decir que durante la investigación las entidades en el sector servicios financieros son más vulnerables a sufrir este tipo de fraudes por lo que manejan grandes cantidades de dólares.

Con porcentajes mayores de 66.7% han sufrido pérdida física de dispositivos o medios que contengan datos y pérdidas financieras debidas a ataques en cajeros automáticos por lo que estos ataques son frecuentes en las cooperativas, ya que las mismas manejan niveles de seguridad como medida precautelar dentro de los sistemas informáticos de esta manera brindan seguridad a los clientes y socios para no crear pérdidas económicas. Con el 33.3% son atacados con suplantación de identidad/ ingeniería social en cuentas y ataques a servicios bancarios en línea este tipo de ataques son creados con el fin de realizar retiros y transacciones con valores considerables. Por lo que en nuestro campo de investigación se encuentra la Cooperativa de Ahorro y Crédito Santa Rosa de Patutan Ltda., ya que ella sufrió un ataque dejando como resultado de su excelente desempeño se convirtió en amenaza por lo que no pudieron lograr el objetivo propuesto por el delincuente informático.

Estos tipos de fraudes están direccionado a todo tipos de empresas sean grandes, medianas, pequeñas y microempresas ya que para los delincuentes informáticos su único fin es robar todo tipo de información relevante que pueda ser necesario para cometer sus objetivos delincuenciales por lo que toda empresa por diferente que sea se sector deben contar con normas de seguridad y contando excelentes software que brinden seguridad y confidencialidad en la información que manejan las mismas.

Tabla 47

Cruce de Variable N° 4

			20. ¿Qué tipo de fraude informático ha sufrido su empresa?					
			Pérdida física de dispositivos o medios que contengan datos	Fuga electrónica de datos de los sistemas internos	Suplantación de identidad/ ingeniería social en cuentas	Ataques a servicios bancarios en línea	Pérdidas financieras debidas a ataques en cajeros automáticos	Total
1. ¿A qué segmento pertenece la entidad financiera?	Segmento 1 (> a $ 80.000.000)	Recuento	0	0	1	1	1	1
		% dentro de $A	0,0%	0,0%	33,3%	33,3%	16,7%	
		% del total	0,0%	0,0%	11,1%	11,1%	11,1%	11,1%
	Segmento 3 (> a $5.000.000 hasta $20.000.000)	Recuento	2	0	0	1	1	2
		% dentro de $A	28,6%	0,0%	0,0%	33,3%	16,7%	
		% del total	22,2%	0,0%	0,0%	11,1%	11,1%	22,2%
	Segmento 4 (> a $ 1.000.000 hasta $5.000.000)	Recuento	4	1	2	1	4	5
		% dentro de $A	57,1%	50,0%	66,7%	33,3%	66,7%	
		% del total	44,4%	11,1%	22,2%	11,1%	44,4%	55,6%
		Recuento	1	1	0	0	0	1

CONTINÚA

	Mediana (Ventas Totales: $ 1.000.001-$5.000.000)	% dentro de $A	14,3%	50,0%	0,0%	0,0%	0,0%	
		% del total	11,1%	11,1%	0,0%	0,0%	0,0%	11,1%
Total		Recuento	7	2	3	3	6	9
		% del total	77,8%	22,2%	33,3%	33,3%	66,7%	100,0%

Interpretación:

El cruce de variables está enfocada en el segmento que se encuentran las cooperativas y al tipo de fraudes informáticos que ha sufrido las empresas de servicios financieros.

En el segmento uno (> a $ 80.000.000 dólares) han sufrido suplantación de identidad/ ingeniería social en cuentas, ataques a servicios bancarios en línea y pérdidas financieras debidas a ataques en cajeros automáticos. Con un número de uno por cada tipo de fraude señalado en este párrafo. En el segmento tres (> $5.000.000 a $20.000.000) fueron atacados con el fraude pérdida física de dispositivos o medios que contengan datos en dos cooperativas, con un tipo de fraude por cooperativa, ataque a servicios bancarios en línea y pérdidas financieras debidas a ataques en cajeros automáticos. En el segmento cuatro (> $1.000.000 a $5.000.000) tenemos a dos cooperativas que sufrieron un ataque de pérdida física de dispositivos o medios que contengan datos y fuga electrónica de datos de los sistemas internos al igual que las empresas reguladas por la Superintendencia de Compañías fueron víctimas de estos tipos de fraudes informáticos.

Podemos decir que las empresas del sector financieros son más vulnerables a ser atacadas por la información que manejan tienen una debilidad que se convierte en una ventaja para los delincuentes informáticos.

Según (It User Tech & Business, 2017)

> La mayor parte de los casos de estafa que se denuncian ante los tribunales son archivados al no ser posible identificar al responsable del delito por falta de pruebas suficientes. En aquellos casos en los que la vía penal se cierra, el afectado suele buscar una reclamación civil contra la entidad financiera, si bien, legislativamente hablando, ambas vías pueden seguirse de manera independiente.

Tabla 48

Cruce de Variable N° 5

			21. Considerando la respuesta que usted dio en la pregunta anterior, los fraudes informáticos afectan a los resultados económicos financieros de la empresa?		Total
			Si	No	
16. ¿Está su empresa interesada en poner en marcha un sistema informático de protección de datos o actualizarlos?	Si	Recuento	7	11	18
		% del total	33,3%	52,4%	85,7%
	No	Recuento	2	1	3
		% del total	9,5%	4,8%	14,3%
Total		Recuento	9	12	21
		% del total	42,9%	57,1%	100,0%

Interpretación:

En este cruce de variables es muy importante indicar que las empresa con un porcentaje de 85.7% está de acuerdo en poner en marcha un sistema informático de protección de datos esto indica que es de gran aporte a las empresas tener una seguridad apropiada en la entidad para resguardar toda la información que poseen y de esta manera dar confianza y seguridad al usuario, mientras que un 14.3% no están interesados en este tipo de servicio por lo que su nivel de ingresos no están representativo y se encuentran en la clasificación de pequeñas empresa.

En lo que respecta a que los fraudes informáticos afectan a los resultados económicos financieros de la empresa con un 57.1 % indican que no afectan a los resultados económicos financieros de la entidad cuando ocurre algún tipo de fraude, en cambio con un 42.9% manifiestan que si afectan esto puede ser que cuando fueron atacados por algún tipo de delito o fraude tuvieron como resultados pérdidas económicas. Este cruce de variables es muy importante porque podemos decir que las empresas que sufrieron algún tipo de fraude están de acuerdo en poner en marcha un sistema informático de protección de datos esto como medida de seguridad ante un posible ataque a futuro que puede estar expuesta cualquier empresa.

En tanto las empresas que no han sufrido ningún tipo de ataque podemos decir que no tienen ningún problema en sus sistemas informáticos ya que jamás fueron víctimas de un ataque o si fueron no tuvieron ninguna pérdida económica esto se convierte en una amenaza a los sistemas informáticos dentro de la empresa.

CAPITULO V

PROPUESTA DE LA INVESTIGACIÓN

5.1. Diagnóstico de los fraudes informáticos en el Ecuador

El uso de la tecnología se ha desarrollado de acuerdo al paso de los años a nivel mundial día a día se está innovando productos y servicios, la globalización ha hecho que todos los países estén a la vanguardia aportando mucho más al desarrollo tecnológico de esta manera países como el nuestro cuentan con centros tecnológicos de primera categoría ya que al contar con este tipo de ventaja tecnológica tienen un alto grado de productividad las empresas se vuelven competitivas ofreciendo los mejores servicios y productos.

Una de las desventajas que se presentan en el uso de la tecnología es que estamos expuestos a sufrir algún tipo de fraude, delito que son ocasionados por hackers o delincuentes cibernéticos que su único objetivo es acceder, ingresar saltando niveles de seguridad de un sistema informático o cuenta en línea sin tener ningún tipo de autorización, dentro de la misma estos realizan robos, estafas aprovechándose de la información personal del usuario. (Steven Whitner, 2011) Nos indica una de las maneras que “los hackers pueden utilizar los sitios web hackeados para difundir software malicioso, malware, incluyendo virus, gusanos o troyanos (malware disfrazado como código útil)”.

> Según (Fiscalía General del Estado, 2015) menciona que: La Dirección de Política Criminal de la Fiscalía General del Estado registró 626 denuncias por delitos informáticos desde el 10 de agosto del 2014 -cuando entró en vigencia el Código Orgánico Integral Penal (COIP)- hasta el 31 de mayo del 2015. A partir del COIP se tipifica este tipo de delitos. En el COIP se sancionan los delitos

informáticos, cuyos actos se comenten con el uso de tecnología para violentar la confidencialidad y la disponibilidad de datos personales.

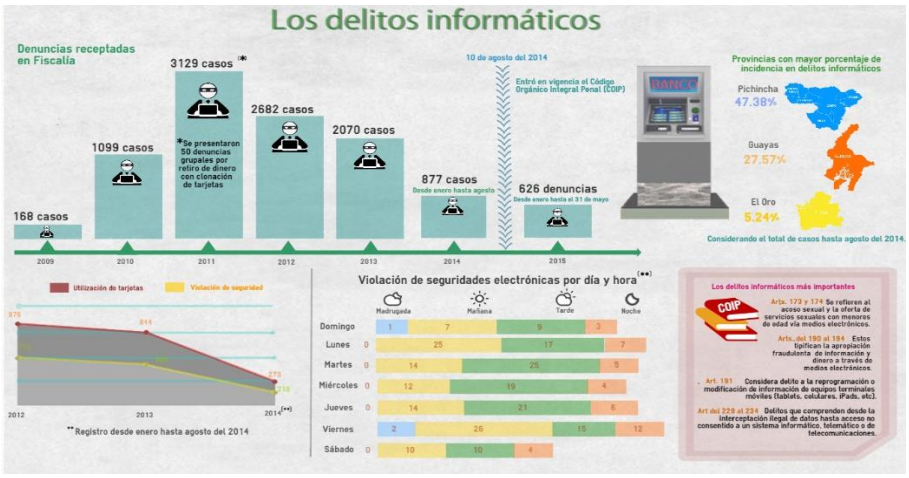


Figura 29. Los delitos informáticos

Fuente: (Fiscalía General del Estado, 2015)

Según la Revista Líderes en un estudio realizado sobre el delito informático, otra inquietud de las empresas en Ecuador menciona que: Cuando se trata de fraudes y robos de información, las pequeñas y medianas empresas (pymes) suelen ser las más vulnerables. Esto se debe a que no siempre cuentan con presupuestos o el equipo para poder enfrentar estos retos de seguridad. Las plataformas de pago, los correos en servidores compartidos o las conexiones a Internet gratuito son algunas de las brechas de entrada que facilitan los crímenes de cibernéticos. (Revista Líderes, 2016)

Según (El Telegrafo, 2016) en un estudio realizado sobre los fraudes Delitos Informáticos en el Ecuador manifiesta que: “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”

5.2. Elaboración de una Guía de Buenas Prácticas de control de vulnerabilidades en fraudes informáticos para las empresas de servicios de la Provincia de Cotopaxi.

GUÍA DE BUENAS PRÁCTICAS

PARA EL CONTROL DE LOS

DELITOS INFORMÁTICOS

AUTORES:

ANGEL ALEJANDRO ROSERO CHAVES

ERICA MARIBEL VALVERDE SOTO

2018

a) Prologo

La presente Guía de Buenas Prácticas en Tecnología de Información y Comunicación (TIC), se enfoca en un conjunto de herramientas que nos permiten desarrollar de una manera eficiente las operaciones de un sistema informático de esta manera disminuiremos errores que se cometen en el transcurso del día, el objetivo de esta guía es brindar soluciones a los usuarios que hacen uso de un sistema y que los mismos son vulnerables a un ataque informático ya que al sector que nosotros realizamos la presente investigación sector servicios regulada por la Superintendencia de Economía Popular y Solidaria y Superintendencia de Compañías en la provincia de Cotopaxi, tiene un grado alto hacer atacados por parte de un ciberdelincuente o Hackers, la globalización ha sido de gran ayuda para la sociedad y poder acceder al internet siendo una herramienta de gran importancia en los últimos años brindando un desarrollo a las empresas con el fin de desarrollar todo tipo de actividades que se presentan día a día.

La característica más importante de en lo que respecta a Tecnología de Información y Comunicación (TIC) dentro de las empresas del sector servicios es contar con un departamento en TIC´s que se encarguen de impulsar valores agregados a las diferentes actividades operacionales y de gestión dentro de la misma ya que se convierten en ventajas hacia las demás entidades. Al hacer uso de los medios de información que tiene cada entidad nos ayudan almacenar, procesar y difundir cualquier tipo de información dentro de la entidad a diferentes áreas que lo necesiten con el objetivo de mejorar los procesos efectuados.

La seguridad en los sistemas informáticos que manejan las empresas de servicios debe ser controlada y monitoreada de forma eficiente y eficaz para evitar ser atacados por ciberdelincuentes y de esta forma estamos preparados ante cualquier tipo de amenaza que puede presentarse en cualquier momento.

b) Introducción

Internet es quizás la invención tecnológica más influyente de la actualidad y continúa cambiando la vida cotidiana de prácticamente todos en la Tierra. Millones de personas están conectadas al ciberespacio y miles más ingresan al mundo en línea todos los días. Internet no solo ha revolucionado la forma en que interactuamos con otros y aprendemos, sino que ha cambiado para siempre la forma en que vivimos. A medida que las tecnologías de Internet e informática continúan prosperando; los delincuentes han encontrado formas de utilizar estas tecnologías como una herramienta para sus actos desviados (Acurio del Pino, 2013).

Los delitos informáticos son una nueva clase de delito que se perpetran usando computadoras, o que están relacionadas con ellos. El delito informático es diferente y más atroz que el delito convencional, ya que el delito se comete a través de un medio electrónico que dificulta el seguimiento e identificación del delincuente. Los tipos más comunes de delito informático incluyen el fraude informático, la difamación, la piratería, la intimidación y el phishing (Acurio del Pino, 2013).

El delito informático tiene el potencial de afectar las actividades diarias de todos. La sociedad depende en gran medida de la tecnología informática para casi todo en la vida. El uso de la tecnología informática abarca desde las ventas individuales de los consumidores hasta el procesamiento de miles de millones de dólares en las industrias bancaria y financiera. El rápido desarrollo de la tecnología también está aumentando la dependencia de los sistemas informáticos. Hoy en día, los delincuentes informáticos están utilizando esta mayor dependencia como una oportunidad significativa para participar en comportamientos ilícitos o delincuentes (Alestuey, 2013).

c) Secciones en la Guía de Buenas Practicas en TIC

La siguiente guía de buenas prácticas consta de las siguientes secciones:

- Sección 1
    - Fundamentos teóricos

    - Política seguridad Informática
    - Sistema de Información
    - Confidencialidad
    - Riesgo
    - Manipulación de datos de entrada
- Sección 2
    - Política de seguridad Informática
    - Marco de Gestión de Seguridad Informática
    - Roles y responsabilidades
    - Sensibilidad y clasificación de la seguridad
    - Seguridad Informática
    - Controles para la administración de la Seguridad
    - Controles de seguridad lógica y física.
    - Software malicioso
- Sección 3
    - Medidas técnicas para la prevención de fraudes informáticos
    - Prevención
    - Detección de sistemas de intrusos
    - Recuperación: Copias de seguridad
    - Técnicas de análisis Forense

LA GUÍA DE BUENAS PRÁCTICAS

SE ENCUENTRA ANEXADA A LA INVESTIGACIÓN.

CONCLUSIONES

- A lo largo del desarrollo de nuestra investigación como base principal fue investigar, analizar e indagar a todas las empresas del sector servicios que se encuentran en la provincia de Cotopaxi con la finalidad de estudiar el grado de vulnerabilidad que presentan en los sistemas informáticos, determinando que las empresas financieras reguladas por la Superintendencia de Economía Popular y Solidaria pertenecientes al segmento 3 y 4 tienen un alto grado de vulnerabilidad a recibir un ataque informático por parte de hackers o delincuentes informáticos, debido a que no cuentan con un departamento en Tecnología de Información y Comunicación (TIC) con la finalidad de que todas las operaciones sean controladas y monitoreadas por el mismo.
- Dentro de la investigación de nuestro estudio que fue direccionado a las empresas del sector servicios se encuentran con mayor población las entidades de intermediación financiera reguladas por la Superintendencia de Economía Popular y Solidaria (SEPS) y la Superintendencia de Compañías, enfocamos en la inversión que tiene cada entidad en la cuenta Equipo de Cómputo y Software que pertenece a Propiedad Planta y Equipo basados en sus balances generales con el fin de determinar montos relevantes para nuestro estudio y de esta manera aplicar instrumentos de recopilación de información y datos
- En nuestro estudio aplicamos diferentes herramientas como la encuesta el cuestionario de control interno de esta manera llegamos a obtener información precisa que conllevo a realizar una auditoría informática y forense de acuerdo a los resultados obtenidos, de esta manera podemos decir que las entidades de intermediación financiera no cuenta con un adecuado manejo en lo que se

refiere a sistemas informáticos software, hardware y personal informático ya que se convierten en una desventaja para la entidad y una ventaja para los ciberdelincuentes para cometer algún tipo de fraude o delito informático.

- Con la aplicación de la encuesta La Cooperativa de Ahorro y Crédito Santa Rosa de Patutan Ltda., se pudo identificar que sufrió un fraude informático con un resultado final convertido en una amenaza que en la actualidad se encuentra en investigaciones. La misma que fue aplicado un cuestionario de control interno obteniendo como resultado un nivel de confianza de 27,59 (Bajo) y su nivel de riesgo de 72,41 (Alto) con respecto a la seguridad; por lo que podemos decir que por inexistencia de un control adecuado en los sistemas informáticos (hardware, software y personal informático) dentro de la cooperativa obtuvimos un resultado bajo en nivel de confianza y alto en respecto al nivel de riesgo, lo que se convierte la cooperativa en tener un alto grado de vulnerabilidad ante un ataque informático, por lo que se dio paso a la aplicación de una auditoria informática.
- La Cooperativa de Ahorro Y Crédito Santa Rosa de Patután Ltda., no cuenta con un profesional en el área de sistemas y tampoco tiene un departamento de Tecnología de Información y Comunicación, ya que es muy importante que una entidad que se dedica a brindar servicios financieros cuente con un profesional en el área de sistemas, para disminuir la vulnerabilidad y el riesgo a ser atacados por delincuentes informáticos que se dedican realizar robos tanto de información confidencial que maneja la cooperativa y de esta manera evitamos pérdidas financieras a futuro protegiendo los sistemas informáticos.
- La cooperativa no cuenta con un manual o instructivo que este sea la base del desarrollo de todas las actividades que efectúa el personal cuando realizan operaciones dentro del software, tampoco cuenta con una políticas para la seguridad de los sistemas informáticos esto se convierte a lo largo del tiempo en un bache (debilidad) de la cooperativa ante posibles ataques por parte de terceras personas, la cual sufrió un intento de fraude por medio de un correo

electrónico inmediatamente tomaron las medidas respectivas convirtiéndose en una amenaza por ello realizamos un examen especial forense.

- Al concluir con la investigación se afirma que las empresas del sector servicios reguladas por las Superintendencia de Economía Popular y Solidaria (SEPS) y Superintendencia de Compañías no cuentan con un manual o guía de buenas prácticas referente al manejo de sistemas informáticos y seguridad informática con el propósito de brindar mayor confianza a los socios y clientes dentro de las operaciones de la entidad.

RECOMENDACIONES

- A las empresas del sector servicios reguladas por la Superintendencia de Economía Popular y Solidaria (SEPS) y Superintendencia de Compañías tener una inversión más representativa en lo que respecta Propiedad Planta y Equipo la cuenta Equipo de Cómputo y software con la finalidad de contar con un sistema informático adecuado con el desarrollo de acorde a las actividades económicas que realizan dichas entidades de intermediación financiera, alojamiento y salud. De esta manera proteger y precautelar los sistemas informáticos.
- Los proveedores de sistemas y programas informáticos deben contar con los servicios específicos acorde a las necesidades de las empresas o entidades ya que cada organización tiene su actividad económica diferente esto hace que sea una diferente de otra por lo que se aconseja tener una amplia gama en lo que se refiere a servicios en sistemas y programas informáticos con el fin de tener un excelente manejo del mismo.
- Las empresas del sector servicios deben estar preparadas ante posibles ataques informáticos de esta forma disminuiremos el grado de vulnerabilidad ante un posible riesgo por parte de hackers o delincuentes informáticos, las entidades deben capacitar, educar e instruir al personal que labora dentro de la misma con la finalidad de saber actuar o manejar una posible situación que puede suceder en cualquier momento, optando por la compra o contratar los servicios de una excelente firma proveedora de sistemas informáticos que cuide y garantice la seguridad de la empresa.
- Se recomienda a las entidades hacer uso de un servicio de almacenamiento de datos por medio de una nube ya que estamos salvaguardando y protegiendo la información confidencial de la entidad, y de esta manera evitamos perdidas de información, a su vez contratar un profesional en el área de sistemas sea este a tiempo completo o parcial por ende se debe implementar el departamento de

tecnología de información y comunicación y este sea responsable de dicho departamento.

- Llevar un registro de las personas que tienen acceso a la información de clientes y cuenta habientes que acuden a ocupar todos los servicios que ofrece la cooperativa, por lo tanto debe existir una bitácora indicando quien ingresa la hora y con qué fin acceden a dicha información con este proceso estamos asegurando, protegiendo la información personal de los socios. Hacer uso de un corta fuegos (Firewall) para poder bloquear el acceso no autorizado, de esta manera protegemos y brindamos mayor seguridad que controle los elementos de la red a la computadora, de acuerdo a las necesidades de la empresa.
- Implementar dentro de la estructura organizacional de las empresas de servicios un departamento o área de Tecnología de Información y Comunicación con el fin de tener eficiencia en todas las operaciones que tiene la misma brindando seguridad y confiabilidad a socios y clientes.
- Se recomienda adoptar una cultura organizacional con un enfoque en el manejo, guía de buenas prácticas en lo que se refiere a Tecnología de Información y Comunicación (TIC) que está desarrollada por los investigadores de este proyecto con el propósito de que se lleve una excelente administración y manejo de la tecnología de información de esta manera aplicaremos herramientas para controlar, disminuir y evitar posibles ataques por ciberdelincuentes que están conectados en la red.

REFERENCIAS BIBLIOGRÁFICAS

(s.f.).

Alatrista Gironzini, M. A. (7 de Diciembre de 2016). *Aspectos clave para el DIseño de programs de Información Financiera*. Recuperado el 04-08-2017. Obtenido de https://auditool.org/blog/auditoria-externa/2028-programa-de-auditoria

Alatrista Gironzini, M. A. (07 de Diciembre de 2016). *Auditool*. Recuperado el 04-08-2017. Obtenido de Auditoria: https://www.auditool.org/blog/auditoria-externa/2028-programa-de-auditoria

Arens, A., Randal, E., & Beasley, M. (2012). *Auditoría un enfoque integral.* México D.F.: Pearson Educatión de México.

Arias Fidias G. (2012). *El proyecto de investigacion Introducción a la metodología científica.* Caracas: Episteme, C.A.

Baca Urbina Gabriel. (2016). *Seguridad Informática.* Méxco: Patria.

Baena Guillermina. (1985). *Manual para elaborar trabajos de investigación documental.* México.

Banco Interamericano de Desarrollo. (14 de Mayo de 2016). *BID y OEA instan a América Latina y Caribe a mayores esfuerzos en ciberseguridad*. Recuperado el 04-08-2017. Obtenido de http://www.iadb.org/es/noticias/comunicados-de-prensa/2016-03-14/informe-sobre-ciberseguridad-en-america-latina,11420.html

Beatriz, S. (s.f.). *Gestion.Org*. Obtenido de https://www.gestion.org/economia-empresa/creacion-de-empresas/3985/clasificacion-de-las-empresas/

Carrasquel Meneses Dorela: Méndez Aray, A. C. (s.f.). *Seguridad Informatica*. Recuperado el 11-08-2017. Obtenido de https://carrmen.jimdo.com/riesgo-informatico/

Chavarría, J., & Roldán, M. (2014). *Auditoría Forense.* México D.F.: Euned.

Chavarría, J., & Roldán, M. (s.f.). *Auditoría Forense.*

CIBERTEC . (s.f.). Obtenido de https://www.cibertec.edu.pe/extension-profesional/certificaciones-internacionales/cursos-cobit/que-es-cobit/

Código Organico Integral Penal Delitos contra la información Art.22. (2014). *Deltos Informaticos.* Ecuador.

Constitución de la República del Ecuador. (2008). *Comunicación e Informcación.*

Constitución de la República del Ecuador, Garantías constitucionales Capitulo VIII Articulo 16. (2011). *Derechos de Proteccion.* Ecuador.

Constitución de la Republica del Ecuador. Art. 308. (2008). *Sistema Financiero.* Montecristi.

Constitución Política. (2008). *Comunicación e Informcación.*

Davara Rodriguez Miguel Angel. (1993). *Manual de Derecho Informatico.* Aranzadi Pamplona.

Díaz Lazo, J., Pérez Guitiérrez, A., & Florido Bacallao, R. (Marzo de 2011). *Impacto de las Tecnologías de la Información y las Comunicaciones (TIC) para disminuir la brecha degital en la Sociedad Actual*. Recuperado el 20-08-2017. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0258-59362011000100009

E General - Definista. (8 de Noviembre de 2008). *Concepto de definición*. Recuperado el 20-08-2017. Obtenido de http://conceptodefinicion.de/empresa-de-servicios/

Echenique Garcia Jose Antonio. (2001). En G. J. Echenique, *Auditoria Informatica.* México: Mc,Graw-Hill/Interamericana Editores.

Ecured. (Octubre de 2017). *Auditoría Administrativa*. Recuperado el 03-09-2017. Obtenido de https://www.ecured.cu/Auditor%C3%ADa_Administrativa

El comercio . (09 de 06 de 2014). Recuperado el 03-09-2017. Obtenido de http://www.elcomercio.com/actualidad/delitos-informaticos-economia-seguridad.html

El comercio. (15 de 10 de 2015). Recuperado el 03-09-2017. Obtenido de http://www.elcomercio.com/actualidad/estudio-riesgosbancarios-americalatina-delitosinformaticos.html

El diario. es. (16 de Mayo de 2013). *Grandes robos informáticos de la historia*. Recuperado el 10-09-2017. Obtenido de http://www.eldiario.es/turing/Grandes-robos-informaticos-historia_0_132986921.html

El Telegrafo. (16 de Agosto de 2016). Obtenido de En Ecuador, el 85% de los delitos informáticos ocurre por descuido del usuario

El Telegrafo. (16 de 08 de 2016). *El Telegrafo. Recuperado el 10-09-2017.* Obtenido de El Telegrafo: https://www.eltelegrafo.com.ec/noticias/judicial/1/en-ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario

El Universo. (17 de 11 de 2014). Recuperado el 15-09-2017. Obtenido de https://www.eluniverso.com/noticias/2014/11/17/nota/4226966/ataques-web-podrian-aumentar

Enciclopedia Financiera. (s.f.). *Sistemas de Información*. Recuperado el 15-09-2017. Obtenido de http://www.enciclopediafinanciera.com/definicion-sistemas-de-informacion.html

Enrique Bejamin, F. F. (2007). Auditoria Administrativa, Gestion Estrategica Del Cambio. En F. F. Enrique Bejamin. México.

Escuela Administracion Consultorio Contable . (10 de Mayo de 2007). Recuperado el 20-09-2017.Obtenido de http://www.eafit.edu.co/escuelas/administracion/consultorio-contable/Documents/boletines/auditoria-control/b13.pdf

Estupiñán Gaitán Rodrigo. (2006). *Control Interno y Fraudes con base en los ciclos transaccionales analisis de informe COSO I y II.* Bogotá: Ecoe Ediciones.

Estupiñan Gaitan Rodrigo. (2015). *Control interno y fraudes Coso I, II, III.* Bogotá.

Evangelina, F. T. (s.f.). *Foro de Profesionales Latinoamericanos de Seguridad*. Recuperado el 20-09-2017. Obtenido de La Auditoria Forense es una técnica que

integra conocimientos criminalísticos, contables, jurídicos, procesales y financieros para la lucha contra el fraude: http://www.forodeseguridad.com/artic/discipl/4166.htm

Falella Santa: Martins Feliberto. (2012). *Metodología de la investigación.* Caracas : Fedupel.

Fayad Omar. (27 de 10 de 2015). *Ley Federal para prevenir y sancionar los delitos Informáticos*. Recuperado el 25-09-2017. Obtenido de http://www.senado.gob.mx/sgsp/gaceta/63/1/2015-10-27-1/assets/documentos/Inic_PRI_Ley_Delitos_Informaticos.pdf

Fidias Arias G. (2006). *Metodologia de la Investigacion.* Caracas, Venezuela: Episteme.

Fiscalía General del Estado. (13 de 06 de 2015). *Fiscalía General del Estado.* Recuperado el 25-09-2017. Obtenido de Fiscalía General del Estado: https://www.fiscalia.gob.ec/los-delitos-informaticos-van-desde-el-fraude-hasta-el-espionaje/

Fiscalía General del Estado. (13 de Junio de 2015). *Los delitos informáticos van desde el fraude hasta el espionaje*. Recuperado el 25-09-2017. . Obtenido de http://fiscalia.gob.ec/index.php/sala-de-prensa/boletines/151-2015/junio-2015/4208-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje

Fontán Tapia María Evangelina, F. (s.f.). *La Auditoria Forense es una técnica que integra conocimientos criminalísticos, contables, jurídicos, procesales y financieros para la lucha contra el fraude*. Recuperado el 30-09-2017. Obtenido de http://www.forodeseguridad.com/artic/discipl/4166.htm

García Alfonso: Hurtado Cervigón: Alegre Ramos María Del Pilar. (2011). *Seguridad Informatica.* Madrid: Ediciones Paraninfo, SA.

García Córdoba Fernando. (2004). *El cuestionario.* México: Limusa.

González Cruz Maité. (22 de Marzo de 2011). *Gestiopolis*. Recuperado el 07-10-2017.. Obtenido de Impacto de las TIC en los sistemas educativos: https://www.gestiopolis.com/impacto-de-las-tic-en-los-sistemas-educativos/

Hall Andrés. (s.f.). *Los tipos de delitos informáticos reconocidos por Naciones Unidas.* Recuperado el 15-10-2017. Obtenido de Los tipos de delitos informáticos reconocidos por Naciones Unidas: http://www.forodeseguridad.com/artic/discipl/disc_4016.htm

Hernandez Hernandez Enrique. (1996). *Un enfoque metodologico.* México: Continental, S.A DEC.V.

Hernandez Jesus. (2 de Marzo de 2016). *Delitos Informaticos*. Recuperado el 20-10-2017. Obtenido de http://losdelitosinformaticoslegislacion.blogspot.com/

ISO 19011. (2015). *Como gestionar un programa de Auditoría*. Recuperado el 25-10-2017. Obtenido de https://www.123aprende.com/2015/11/norma-iso-19011-programa-auditoria/?c=cee236228e9a

It User Tech & Business. (09 de 03 de 2017). Recuperado el 04-11-2017. Obtenido de Content Marketing: http://www.ituser.es/content-marketing/2017/03/tecnologia-para-hacer-frente-al-fraude-financiero

Jesuarez. (17 de 12 de 2015). *Ecuavisa* . Recuperado el 09-11-2017. Obtenido de http://www.ecuavisa.com/articulo/televistazo/noticias/124448-guayas-pichincha-registran-mayor-numero-delitos-informaticos

Juarez Edgar, J. (26 de Julio de 2017). *El economista*. Recuperado el 09-11-2017. Obtenido de https://www.eleconomista.com.mx/finanzaspersonales/Conozca-cuales-son-los-principales-fraudes-financieros-20170726-0139.html

Kotler, Philip. (2010). *Direccion de Mercadotecnia.* España: Prentice.

Kuna Horacio. (2006). *Asistente para la Realización de Auditorías de Sistemas en Organismos públicos y privados.* Recuperado el 12-11-2017. Obtenido de Tesis

de Magister en Ingeniería del Software: http://laboratorios.fi.uba.ar/lsi/rgm/tesistas/kuna-tesisdemagister.pdf

La Contraloria General del Estado. (s.f.). Recuperado el 04-11-2017. Obtenido de https://apps.contraloria.gob.pe/packanticorrupcion/control_interno.html

La investigación de campo. Bogotá: E-Cultura Group. (23 de abril de 2016). *El Pasante*. Obtenido de https://educacion.elpensante.com/la-investigacion-de-campo/

Laudon Kanneth & Laudon Jane. (2006). *Administración de los Sistemas de Información.* New York: Charles.

Leiva, R. E. (2007). *Intermediacion Financiera.* Costa Rica: Universidad Estatal a Distancia San Jose.

Ley Comercio Electrónico, Código Organico IntegralPenal Art. 353. (2014). *Falsificacion Electronica.* Ecuador.

Ley Comercio Electrónico, Código Organico IntegralPenal Art. 552. (2014). *Apropiacion Ilicita.* Ecuador.

Ley Comercio Electrónico, Código Organico IntegralPenal Art. 415. (2014). *Daños Informaticos.* Ecuador.

Ley General de Instituciones del Sistema Financiero. (10 de Enero de 2001). Recuperado el 12-11-2017. Obtenido de https://www.oas.org/juridico/mla/sp/ecu/sp_ecu-mla-law-finance.html

López Aguilera Purificacion. (2010). *Seguridad informática.* Editex.

López López, M. L. (2010 de 2010). *La auditoría Administrativa para evaluar el nivel de eficacia de una Empres*. Recuperado el 17-11-2017. Obtenido de http://www.eumed.net/libros-gratis/2010e/804/Concepto%20de%20Auditoria%20Administrativa.htm

Lybrand Coopers. (1997). *Los nuevos conceptos del control interno (Informe COSO).* España: Diaz de Santo.

Martinez Catherine. (28 de abril de 2017). *lifeder.com*. Recuperado el 17-11-2017 Obtenido de https://www.lifeder.com/investigacion-documental/

Martínez, Y., Blanco, B., & Loy Marichal, L. (28 de Julio de 2012). *Auditoría con Informática a Sistemas Contables.* Recuperado el 17-11-2017. Obtenido de http://www.redalyc.org/html/1939/193924743004/

Mendez Carlos. (199). *Metodología Diseño y Desarrollo del Proceso de Investigación.*

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (Enero de 2014). *Tecnologías de la Información y Comunicaciones para el Desarrollo.* Recuperado el 16-11-2017. Obtenido de http://www.industrias.ec/archivos/CIG/file/CARTELERA/MINTEL-TIC%20para%20el%20Desarrollo.pdf

Ministerio de Telecomunicaciones y de la la Sociedad de la Información. (Enero de 2014). *Tecnologías de la Información y Comunicación para el Desarrollo. Recuperado el 19-11-2017.* Obtenido de http://www.industrias.ec/archivos/CIG/file/CARTELERA/MINTEL-TIC%20para%20el%20Desarrollo.pdf

Moncayo Carolina. (16 de Septiembre de 2016). *Instituto Nacional de Contadores Publicos de Colombia*. Obtenido de https://www.incp.org.co/tipos-de-fraudes/

Montilla Galvis, O. d., & Herrera Marchena, L. G. (2006). *Estudios Gerenciales*. *Recuperado el 19-11-2017..* Obtenido de Auditoría: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-59232006000100004

Moreno Bayardo María Guadalupe. (s.f.). *Introducción a las metodología de la investigación educativa.*

Muñoz Razo Carlos. (2002). *Auditoría en Sistemas Computacionales.* México: Camara Nacional de la industria Editorial Mexicana .

Ojeda Pérez Jorge Eliécer: Arias Flórez Miguel Eugenio. (Enero de 2010). *Delitos Informáticos y entorno jurídico vigente en Colombia*. Obtenido de file:///C:/Users/Pato/Downloads/Dialnet-DelitosInformaticosYEntornoJuridicoVigenteEnColomb-3643404.pdf

Osores Melisa. (Julio de 2014). *TechTarget*. *Recuperado el 26-11-2017.* Obtenido de https://searchdatacenter.techtarget.com/es/cronica/Principios-de-COBIT-5-para-el-gobierno-efectivo-de-TI

Pérez Porto Julián. (2008). *Definición de empresa*. Obtenido de https://definicion.de/empresa/

Piattini Velthius Mario Gerardo: Del Peso Navarro Emilio. (2004). *Auditoria Informatica Un enfoque practico.* Madrid España: Alfaomega Grupo Editor.

Plan Nacional del Buen Vivir. (2013). *Plan Nacional del Buen Vivir. Recuperado el 26-11-2017.* 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

Plan Nacional del Buen Vivir. (2013). *Plan Nacional del Buen Vivir. Recuperado el 26-11-2017.* 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

Policía Nacional del Ecuador. (2 de Septiembre de 2015). *Delitos informáticos o ciberdelitos*. Obtenido de http://www.policiaecuador.gob.ec/delitos-informaticos-o-ciberdelitos/

QuestionPro. (s.f.). *Recuperado el 19-11-2017.* Obtenido de https://www.questionpro.com/blog/es/tipos-de-muestreo-para-investigaciones-sociales/

Quintuña Rodriguez, V. (2012). *Auditoría Informática a la Superintendencia de Telecomunicaciones. Recuperado el 30-11-2017.* Obtenido de http://dspace.ucuenca.edu.ec/bitstream/123456789/652/1/ts205.pdf

Revista Líderes. (10 de Octubre de 2016). *El delito informático, otra inquietud de las empresas*. *Recuperado el 30-11-2017.* Obtenido de http://www.revistalideres.ec/lideres/delito-tecnologia-internet-empresas-fraude.html

Revista Líderes. (10 de 10 de 2016). *Revista Líderes.* Obtenido de Revista Líderes: http://www.revistalideres.ec/lideres/delito-tecnologia-internet-empresas-fraude.html

Rincón Rodríguez, F., Ojeda Pérez, J. E., Arias Flórez, M. E., & Daza Martínez, L. A. (23 de Mayo de 2010). *Delitos informáticos y entorno jurídico vigente en colombia. Cuadernos de Contabilidad. Recuperado el 30-11-2017.* Obtenido de file:///C:/Users/Pato/Downloads/Dialnet-DelitosInformaticosYEntornoJuridicoVigenteEnColomb-3643404.pdf

Rivas, G. A. (1989). Auditoria Informatica. En G. A. Rivas, *Auditoria Informatica* (págs. 39-40). Madrid.

Rizo José Mario. (3 de Enero de 2007). *Auditoría Forense ¿ Qué es y cuál es su metodología?* Obtenido de http://elconta.com/2017/01/03/auditoria-forense-que-es-y-su-metodologia/

Rodriguez U Manuel Luis. (19 de Noviembre de 2010). *METODOLOGÍAS DE LA INVESTIGACIÓN*. *Recuperado el 08-12-2017.* Obtenido de https://metodologiasdelainvestigacion.wordpress.com/2010/11/19/la-tecnica-de-la-encuesta/

Rodriguez, L. Y. (s.f.). *Auditoría Administrativa*. *Recuperado el 08-12-2017. Recuperado el 08-12-2017.* Obtenido de http://scholar.googleusercontent.com/scholar?q=cache:SQbZe_Ddx5UJ:scholar.google.com/+alcance+en+auditoria&hl=es&as_sdt=0,5

Roldán. (11 de Marzo de 2018). *Nicanor Aniorte Hernández*. *Recuperado el 08-12-2017.* Obtenido de http://www.aniorte-nic.net/apunt_metod_investigac4_4.htm

Sistema Financiero del Ecuador. (s.f.). *Recuperado el 17-12-2017.* Obtenido de https://www.educacionfinanciera.com.ec/sistema-financiero-del-ecuador

Steven Whitner. (16 de 03 de 2011). *Techlandia*. *Recuperado el 17-12-2017.* Obtenido de https://techlandia.com/objetivos-hackers-info_291023/

Tamayo Mario. (1997). *El proceso de la Investigacion Cientifica.* México: Limusa S.A.

Tamayo Mario. (1997). *El proceso de la investigación científica.* México: Limusa S.A.

Tapia Iturriaga, C. K., Guevara Rojas, E. D., Castillo Prieto, S., Rojas Tamayo, M., & Salomón Doroteo, L. (s.f.). *o.* México.

Tapia Iturriaga, C. K., Guevara Rojas, E. D., Castillo Prieto, S., Rojas Tamayo, M., & Salomón Doroteo, L. (s.f.). *Tapia Iturriaga, Carmen Karina; Guevara Rojas, Eloy David; Castillo Prieto, Salvador; Rojas Tamayo , Martín; Salomón Doroteo, Leonardo.* México.

Téllez Valdés Julio. (1996). *Derecho Informático. 2ª. edición.* México: Mc Graw Hill.

Temperini Marcelo. (2014). *Delitos Informáticos en latinoamérica: Un estudio de derecho comparado. 2da Parte. Recuperado el 17-12-2017.* Obtenido de http://43jaiio.sadio.org.ar/proceedings/SID/13.pdf

Terán Perez David Moises. (2014). *Administración Estratégias de la Función Informátiva.* México: Alfaomega.

Tesis de Investigadores. (31 de Mayo de 2011). *Blogspot.com*. *Recuperado el 17-12-2017.* Obtenido de http://tesisdeinvestig.blogspot.com/2011/05/tipos-de-investigacion.html

Universidad Nacional Autonoma de Mexico. (s.f.). *Seguridad Informática*. *Recuperado el 20-12-2017.* Obtenido de Seguridad Informática: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/Definiciones.php

Vega Alfredo. (2013). Buenos Aires : La bruja.

Velázquez Labrada Yadira, S. B. (Junio de 2015). *Programa de auditoría contable*. *Recuperado el 20-12-2017.* Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2306-91552015000100003

Villa Irene. (9 de Diciembre de 2017). *EAE Business School*. Obtenido de https://retos-directivos.eae.es/empresas-de-servicios-tipos-y-caracteristicas/

Webster, A. (2000). *Estadistica Aplicada a los Negocios y a la Economía.* México: Mc Graw- Hill.

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. Ángel Alejandro Rosero Chaves y la Srta. Erica Maribel Valverde Soto en la cuidad de Latacunga a los 02 días del mes de Agosto de 2018.

Ing. Luis Alfonso Lema Cerda
DIRECTOR

Aprobado por:

Eco. Alisva Cárdenas Pérez
DIRECTORA DE LA CARRERA

Dr. Freddy Jaramillo Checa
SECRETARIO ACADÉMICO