

UNIVERSIDAD TÉCNICA DE AMBATO



FACULTAD DE CONTABILIDAD Y AUDITORÍA

MAESTRÍA DE CONTABILIDAD Y AUDITORÍA

Tema:

LA ADMINISTRACIÓN DE LOS RIEGOS Y LA AUDITORÍA
INFORMÁTICA EN EL SECTOR COOPERATIVO SEGMENTO 1 DE
LA CIUDAD DE AMBATO.

Trabajo de investigación, previo a la obtención del Grado Académico de
Magister en Contabilidad y Auditoría

Autor: Ingeniero Kléver Alfonso Pilamunga Yansapanta

Director: Doctor Joselito Ricardo Naranjo Santamaría Magister

Ambato – Ecuador

2018

A la Unidad Académica de Titulación de la Facultad de Contabilidad y Auditoría.

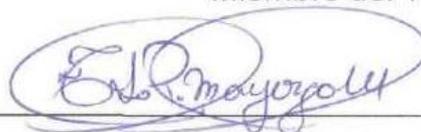
El Tribunal receptor del Trabajo de Investigación presidido por el Economista Telmo Diego Proaño Córdova Magister, e integrado por los señores Doctora Patricia Paola Jiménez Estrella Magister, Doctor Tito Patricio Mayorga Morales Magister, y Doctora Cecilia Catalina Toscano Morales Magister, designados por la Unidad Académica de Titulación de la Universidad Técnica de Ambato, para receptor el Trabajo de Investigación con el tema: "La Administración de los Riegos y la Auditoría Informática en el sector cooperativo segmento 1 de la ciudad de Ambato", elaborado y presentado por el señor Ingeniero Kléver Alfonso Pilamunga Yansapanta, para optar por el Grado Académico de Magister en Contabilidad y Auditoría; una vez escuchada la defensa oral del Trabajo de Investigación el Tribunal aprueba y remite el trabajo para uso de custodia en las bibliotecas de la UTA.



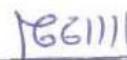
Econ. Telmo Diego Proaño Córdova Mg.
Presidente del Tribunal



Dra. Patricia Paola Jiménez Estrella Mg.
Miembro del Tribunal



Dr. Tito Patricio Mayorga Morales Mg.
Miembro del Tribunal



Dra. Cecilia Catalina Toscano Morales Mg.
Miembro del Tribunal

AUTORÍA DEL TRABAJO DE INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Investigación presentado con el tema: "La Administración de los Riegos y la Auditoría Informática en el sector cooperativo segmento 1 de la ciudad de Ambato", le corresponde exclusivamente a: Ingeniero Kléver Alfonso Pilamunga Yansapanta, Autor bajo la Dirección del Doctor Joselito Ricardo Naranjo Santamaría, Magister, Director del Trabajo de Investigación; y el patrimonio intelectual a la Universidad Técnica de Ambato.



Ing. Kléver Alfonso Pilamunga Yansapanta
C.C. 1804477790
AUTOR



Dr. Joselito Ricardo Naranjo Santamaría Mg.
C.C. 1802621241
DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Investigación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.



Ing. Kléver Alfonso Pilamunga Yansapanta
C.C. 1804477790

ÍNDICE GENERAL DE CONTENIDOS

| | |
|--|-----------|
| Portada | i |
| A la Unidad Académica de Titulación | ii |
| Autoría del Trabajo de Investigación..... | iii |
| Derechos de Autor | iv |
| Índice General de Contenidos..... | v |
| Índice General de Tablas | vii |
| Índice General de Gráficos | viii |
| Agradecimiento | ix |
| Dedicatoria..... | x |
| Resumen Ejecutivo | xi |
| Executive Summary | xiii |
| Introducción | 1 |
| CAPÍTULO I..... | 3 |
| EL PROBLEMA DE INVESTIGACIÓN..... | 3 |
| 1.1. Tema de investigación | 3 |
| 1.2. Planteamiento del Problema | 3 |
| 1.3. Justificación..... | 12 |
| 1.4. Objetivos | 14 |
| CAPÍTULO II..... | 15 |
| MARCO TEÓRICO | 15 |
| 2.1. Antecedentes Investigativos..... | 15 |
| 2.2. Fundamentación Filosófica | 18 |
| 2.3. Fundamentación Legal..... | 19 |
| 2.4. Categorías Fundamentales | 21 |
| 2.5. Hipótesis | 39 |
| 2.6. Señalamiento de variables | 39 |
| CAPÍTULO III..... | 40 |
| METODOLOGÍA..... | 40 |
| 3.1. Enfoque..... | 40 |
| 3.2. Modalidad básica de la investigación..... | 40 |

| | | |
|------|---|------------|
| 3.3. | Nivel o tipo de Investigación..... | 41 |
| 3.4. | Población y Muestra..... | 42 |
| 3.5. | Operacionalización de Variables..... | 42 |
| 3.6. | Recolección de Información | 45 |
| 3.7. | Procesamiento y Análisis | 46 |
| | CAPÍTULO IV | 48 |
| | ANÁLISIS DE RESULTADOS..... | 48 |
| 4.1. | Análisis de e interpretación de resultados..... | 48 |
| 4.2. | Comprobación de Hipótesis | 70 |
| | CAPÍTULO V | 75 |
| | CONCLUSIONES Y RECOMENDACIONES..... | 75 |
| 5.1. | Conclusiones..... | 75 |
| 5.2. | Recomendaciones | 76 |
| | CAPÍTULO VI | 77 |
| | PROPUESTA..... | 77 |
| 6.1. | Datos Informativos | 77 |
| 6.2. | Antecedentes | 78 |
| 6.3. | Justificación..... | 80 |
| 6.4. | Objetivos | 81 |
| 6.5. | Análisis de Factibilidad..... | 81 |
| 6.6. | Fundamentación | 83 |
| 6.7. | Modelo Operativo | 85 |
| | Bibliografía | 122 |
| | Anexos | 127 |

ÍNDICE DE TABLAS

| | |
|--|----|
| Tabla No. 1.1 Cooperativas | 5 |
| Tabla No. 1.2 Cooperativas segmento 1 | 6 |
| Tabla No. 1.3. Cooperativas segmento 1 – Ambato | 8 |
| Tabla No. 3.1. Población..... | 42 |
| Tabla No. 3.2. Administración de riesgos | 43 |
| Tabla No. 3.3. Auditoría informática | 44 |
| Tabla No. 3.4. Recolección de la información..... | 45 |
| Tabla No. 4.1. Productos y servicios..... | 50 |
| Tabla No. 4.2. PED | 51 |
| Tabla No. 4.3. SIC | 52 |
| Tabla No. 4.4. Licencias SIC | 53 |
| Tabla No. 4.5. Conocimiento informática | 55 |
| Tabla No. 4.6. Riesgos claros | 56 |
| Tabla No. 4.7. Administración de riesgos | 57 |
| Tabla No. 4.8. Mitigación de riesgos..... | 58 |
| Tabla No. 4.9. Procedimientos - administración riesgos | 59 |
| Tabla No. 4.10. Importancia administración de riesgos | 60 |
| Tabla No. 4.11. Normativa | 61 |
| Tabla No. 4.12. Unidad de auditoría informática | 62 |
| Tabla No. 4.13. Auditoría informática | 63 |
| Tabla No. 4.14. Sistemas de información | 64 |
| Tabla No. 4.15. Accesos no autorizados | 65 |
| Tabla No. 4.16. Riesgos SEPS | 66 |
| Tabla No. 4.17. Mitigación | 67 |
| Tabla No. 4.18. Organigrama | 68 |
| Tabla No. 4.19. Cálculo t Student | 72 |

ÍNDICE DE GRÁFICOS

| | |
|--|----|
| Gráfico No. 1.1. Árbol del problema..... | 8 |
| Gráfico No. 2.1 Red de inclusiones conceptuales..... | 21 |
| Gráfico No. 2.2. Constelación de ideas..... | 22 |
| Gráfico No. 4.1. Productos y servicios | 51 |
| Gráfico No. 4.2. PED | 52 |
| Gráfico No. 4.3 SIC..... | 53 |
| Gráfico No. 4.4. Licencias SIC | 54 |
| Gráfico No. 4.5. Conocimiento informática | 55 |
| Gráfico No. 4.6. Riesgos claros | 56 |
| Gráfico No. 4.7. Administración de riesgos..... | 57 |
| Gráfico No. 4.8. Mitigación de riesgos | 58 |
| Gráfico No. 4.9. Procedimientos - riegos | 59 |
| Gráfico No. 4.10. Importancia administración de riesgos..... | 60 |
| Gráfico No. 4.11. Normativa | 61 |
| Gráfico No. 4.12. Unidad de auditoría informática | 62 |
| Gráfico No. 4.13. Auditoría informática | 63 |
| Gráfico No. 4.14. Sistemas de información..... | 64 |
| Gráfico No. 4.15. Accesos no autorizados..... | 65 |
| Gráfico No. 4.16. Riesgos SEPS | 66 |
| Gráfico No. 4.17. Mitigación..... | 67 |
| Gráfico No. 4.18. Organigrama | 69 |
| Gráfico No. 4.25. T student..... | 72 |

AGRADECIMIENTO

Mis más sinceros agradecimientos a quienes con su ayuda, apoyo y comprensión me alentaron para lograr esta hermosa y anhelada realidad.

A mis padres, quienes siempre me han apoyado en todos los aspectos de mi vida y han sido un ejemplo a seguir; a mi esposa por su apoyo constante en el día a día, a mis hijos quienes son y será la fuente de inspiración y perseverancia para nuevos objetivos, a la Facultad de Contabilidad y Auditoría de la Universidad Técnica de Ambato que, a través de sus docentes nos han sabido guiar y compartir sus conocimientos; en especial, al Dr. Joselito Naranjo por su dirección, conocimiento y apoyo en la culminación del presente trabajo.

Fonsi

DEDICATORIA

El presente trabajo investigativo está dedicado a Dios, quien me otorgó la sabiduría y fortaleza necesarias para continuar y seguir adelante con mis sueños.

A mis padres, a mis hermanos, a mi esposa y a mis queridos hijos, les dedico con mucho amor y cariño todo mi esfuerzo y trabajo puesto para llegar a finalizar una meta tan importante.

Fonsi

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE CONTABILIDAD Y AUDITORÍA
MAESTRÍA DE CONTABILIDAD Y AUDITORÍA

TEMA:

LA ADMINISTRACIÓN DE LOS RIEGOS Y LA AUDITORÍA
INFORMÁTICA EN EL SECTOR COOPERATIVO SEGMENTO 1 DE LA
CIUDAD DE AMBATO

AUTOR: Ingeniero Kléver Alfonso Pilamunga Yansapanta

DIRECTOR: Doctor Joselito Ricardo Naranjo Santamaría Magister

FECHA: 06 de marzo de 2018

RESUMEN EJECUTIVO

El trabajo investigativo tiene como propósito fundamental determinar la incidencia que tiene la administración de riesgos operativos y la auditoría informática en el sector Cooperativo segmento 1 de la ciudad de Ambato, con el fin de dar alternativas de solución en caso de ser necesario y así mejorar el mejoramiento del control interno.

Para dar cumplimiento al objetivo establecido se procedió a realizar la investigación basada en un estudio documental y de campo, aplicando encuestas de carácter objetivo a la población determinada, esto es a los auditores de las cooperativas pertenecientes al segmento 1 de la ciudad de Ambato.

Tomando en cuenta que el avance tecnológico va aumentando día a día, y por ende, nuestro ambiente común son los computadores, teléfonos inteligentes, tablets, etc., medios por los cuales se puede utilizar productos o servicios financieros que las cooperativas de ahorro y crédito

segmento 1 de la ciudad de Ambato brindan o pueden brindar en el futuro, esto de acuerdo a las políticas nacionales o para satisfacer necesidades de los clientes, se ha realizado la presente investigación y se trabajó con cinco cooperativas de ahorro y crédito segmento 1 de la ciudad de Ambato, en específico, con sus auditores, quienes afirman ser de gran importancia la Administración de Riesgos, y en específico del Riesgo Operativo, ya que no existe normativa expedida por el ente de control, el este caso de la Superintendencia de Economía Popular y Solidaria, en el cual se aborden los factores del riesgo, para de esta manera realizar procesos y procedimiento para evaluar, prevenir y mitigar el riesgo operativo, por lo que posteriormente a la investigación, demostrando la hipótesis, se propone una alternativa de solución la misma que es formular normativa de obligatoriedad de contar con una Unidad de Auditoría informática en el Organigrama estructural de las Cooperativas de Ahorro y Crédito segmento 1, de la ciudad de Ambato, para el fortalecimiento de la Administración de Riesgos Operativos de los Sistemas de Información y comunicación.

Descriptor: Administración del riesgo operativo, auditor informático, auditoría informática, control interno, evaluación del riesgo, factores de riesgo operativo, fraude externo, impacto del riesgo, nivel de riesgo operativo, probabilidad de ocurrencia, riesgo operativo.

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE CONTABILIDAD Y AUDITORÍA
MAESTRÍA DE CONTABILIDAD Y AUDITORÍA

THEME:

THE ADMINISTRATION OF OPERATIONAL RISKS AND COMPUTER
AUDITING IN THE SECTOR COOPERATIVE SEGMENT 1 OF THE CITY
OF AMBATO

AUTHOR: Ingeniero Kléver Alfonso Pilamunga Yansapanta

DIRECTED BY: Doctor Joselito Ricardo Naranjo Santamaría Magister

DATE: March 6th, 2018

EXECUTIVE SUMMARY

The fundamental purpose of the research work is to determine the impact of the administration of operational risks and the computer auditing in the sector Cooperative segment 1 of the city of Ambato, in order to provide alternative solutions if necessary and thus improve the improvement of internal control.

In order to comply with the established objective, we proceeded to carry out the research based on a documentary and field study, applying objective surveys to the determined population, that is to the auditors of the cooperatives belonging to segment 1 of the city of Ambato.

Taking into account that technological progress is increasing day by day, and therefore, our common environment are computers, smart phones, tablets, etc., means by which you can use financial products or services that credit unions segment 1 of the city of Ambato provide or may provide in the future, this according to national policies or to meet customer needs, this research has been conducted and worked with five savings and credit

cooperatives segment 1 of the City of Ambato, specifically, with its auditors, who claim to be of great importance the Risk Management, and specifically Operational Risk, since there is no regulation issued by the control body, this case of the Superintendence of Popular Economy and Solidarity, in which the risk factors are addressed, in order to carry out processes and procedures to evaluate, prevent and mitigate the operational risk, so that after the investigation, demonstrating the hypothesis, an alternative solution is proposed, which is to formulate compulsory regulations for having a Computer Audit Unit in the structural Organigram of the Savings and Credit Cooperatives segment 1 , of the city of Ambato, for the strengthening of the Operational Risk Management of the Information and Communication Systems.

Keywords: Operational risk management, IT auditor, IT audit, internal control, risk assessment, operational risk factors, external fraud, risk impact, level of operational risk, probability of occurrence, operational risk.

INTRODUCCIÓN

El presente trabajo de investigación tiene como tema: “LA ADMINISTRACIÓN DE LOS RIEGOS Y LA AUDITORÍA INFORMÁTICA EN EL SECTOR COOPERATIVO SEGMENTO 1 DE LA CIUDAD DE AMBATO”, el mismo que consta de seis Capítulos, los cuales se encuentran desarrollados de acuerdo a la norma establecida por la Facultad de Contabilidad y Auditoría; y, está estructurado por los siguientes capítulos:

Capítulo I, denominado: El Problema, contiene el planteamiento del problema, Contextualizaciones Macro, Meso y Micro, Análisis Crítico, Prognosis, Formulación del Problema, Delimitación del objeto de investigación, la Justificación, Los Objetivos, Objetivo General y tres Objetivos Específicos.

Capítulo II, denominado: Marco Teórico, que contiene Antecedentes Investigativos, Fundamentaciones, Categorías Fundamentales, Hipótesis, Variable Independiente y Variable Dependiente.

Capítulo III, titulado: Metodología, que contiene el Nivel o Tipo de Investigación, la Población y Muestra, Operacionalización de cada una de las variables, plan de recolección de datos, y plan de Procesamiento de la información.

Capítulo IV, llamado: Análisis e Interpretación de Resultados, que contiene: el Análisis de los Resultados, Interpretación de datos y la Verificación de la Hipótesis.

Capítulo V, llamado: Conclusiones y Recomendaciones, que se han llegado en base a las encuestas y del trabajo investigativo.

Capítulo VI, llamado: Propuesta, contiene: Datos Informativos, Antecedentes de la Propuesta, Justificación, Objetivos, Análisis de Factibilidad, Fundamentación y Modelo Operativo.

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1. TEMA DE INVESTIGACIÓN

“La Administración de los Riegos y la Auditoría Informática en el sector Cooperativo Segmento 1 de la ciudad de Ambato.”

1.2. PLANTEAMIENTO DEL PROBLEMA

1.2.1. Contextualización

1.2.1.1. Contexto macro

En el Ecuador y el mundo, el desarrollo de la Tecnología ha evolucionado de una manera significativa desde 1939, fecha en la que se creó la primera computadora electrónica en la actual Iowa State University (USA), (Coello Coello, 2003); hasta la actualidad, y más aún en el ámbito de los servicios financieros, es así, que hoy en día encontramos la banca virtual para acceso a computadores con internet y la banca móvil para acceso a teléfonos inteligentes a través de las diferentes aplicaciones, que dan acceso a todos sus usuarios para realizar transacciones bancarias, pagos de servicios básicos, tarjetas de crédito, préstamos bancarios, etc., pero la mayoría de usuarios realizan dichas operaciones con desconfianza, ya que es común escuchar sobre los fraudes o delitos informáticos que han sufrido los usuarios del sistema financiero a nivel mundial. Es así que, según el diario El Tiempo (2014), en su noticia manifiesta que “se capturó a 12 integrantes de una red de ‘hackers’ que, vulnerando los sistemas de pago en internet, robó más de 10.000 millones de pesos afectando a más

de 15.000 usuarios de diferentes entidades bancarias”, dentro de las instituciones afectadas por este hecho se encuentran: Davivienda, Bancolombia, Banco del Occidente, Av-villas, Caja Social, Banco Popular, bancos que son reconocidos en el País de Colombia. El evento más reciente es el que sufrió la compañía Apple, en la cual, un software malicioso, simulaba ser una aplicación real de la compañía, pero dicho software estaba programado para recolectar información sobre los dispositivos infectados, información como contraseñas y datos para el acceso a la banca on line, por el alcance de la tecnología de dicha empresa, todo el mundo se ve afectado. (EL PAÍS, 2015), así mismo, en el Ecuador según el diario EL UNIVERSO (2014) manifiesta que los delitos informáticos podrían aumentar en el País, debido al crecimiento económico, por no contar con una adecuada administración de riesgos, por lo acarrea a ser un blanco ideal para los cyber-delincuentes y hackers del mundo entero.

Según la Fiscalía General Del Estado (2015), a partir del 10 de agosto de 2014, fecha en la cual entró en vigencia del nuevo Código Orgánico Integral Penal hasta el 31 de mayo de 2015, se ha recibido 626 denuncias por delitos informáticos, debido a que el nuevo código ya tipifica dichos delitos, entre las denuncias realizadas se encuentran las siguientes: Transferencia ilícita de dinero, apropiación fraudulenta de datos personales, interceptación ilegal de datos, violación de las seguridades, etc., aspectos que son de relevancia y deberían ser tratados por Auditoría.

Por ende, la mala administración de los Riesgos puede ocasionar que se produzcan los delitos informáticos a diferentes escalas, perjudicando así a las Instituciones Financieras y por consecuencia a los usuarios que mantienen su dinero en dichas instituciones, esto a la vez refleja que el resultado de las auditorías informáticas no son confiables, o estos temas no los topa las Auditorías tradicionales (financieras).

Es importante mencionar que en el Ecuador según el Boletín Financiero de la Superintendencia De Economía Popular Y Solidaria (2015) al 30 de junio de 2015 existen 908 cooperativas de ahorro y crédito bajo su control, divididos en segmentos de acuerdo a ciertas características, las mismas que pueden sufrir ataques de los hacker y ser víctima de los delitos informáticos debido a una mala Administración de los Riesgos y en el presente estudio de Riesgos Operativos en cuanto a las tecnologías de la información y comunicación. Las cooperativas por segmentos pertenecientes a todo el país se detallan a continuación:

TABLA 1.1 COOPERATIVAS

| SEGMENTO | REQUISITOS - ACTIVOS (USD) | NÚMERO DE COOPERATIVAS |
|-----------------|---|-------------------------------|
| 1 | Mayor a 80'000.000,00 | 25 cooperativas |
| 2 | Mayor a 20'000.000,00 hasta 80'000.000,00 | 36 cooperativas |
| 3 | Mayor a 5'000.000,00 hasta 20'000.000,00 | 88 cooperativas |
| 4 | Mayor a 1'000.000,00 hasta 5'000.000,00 | 194 cooperativas |
| 5 | Hasta 1'000.000,00 | 565 cooperativas |
| TOTAL | | 908 cooperativas |

Fuente: Superintendencia de Economía Popular y Solidaria (2015)

1.2.1.2. Contexto meso

En la provincia de Tungurahua, por ser una de las provincias más comerciales, se hace frecuente el uso de los servicios financieros a través de las Instituciones Financieras, por tal razón, es más propensa a sufrir ataques de Cyber-delincuentes, y por ende, verse afectado por cualquier delito informático, en consecuencia pérdida de los recursos financieros y económicos de las Cooperativas de Ahorro y Crédito, esto por incurrir en proporcionar nuevos servicios a sus clientes, casos que ya han sucedido en países desarrollados y que tienen procedimientos de control para estos casos, es decir, mantienen una adecuada administración de los riesgos a través de procedimientos de auditoría, como por ejemplo: las transferencias bancarias sin consentimiento de su titular, en las cuales se

vieron afectados cinco ciudades de Europa: Valladolid, Lora del Río en Almería, Badajoz, Alicante y Parla en Madrid según la página de Delitos Informáticos (2015).

Del total de cooperativas en el Ecuador, se tomó en cuenta para el presente trabajo de investigación las que se encuentran categorizadas en el Segmento 1, es decir, las cooperativas que tengan en sus activos una cantidad mayor a ochenta millones de dólares americanos según lo determina la Resolución Nro. 038-2014-F de la Junta de Política y Regulación Monetaria y Financiera, las mismas que corresponden a 25 cooperativas de acuerdo al Boletín Financiero de la SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (2015), cada una con sus respectivas sucursales en los diferentes cantones de la provincia, las cooperativas en mención son:

TABLA 1.2. COOPERATIVAS SEGMENTO 1

| No. | RUC | RAZÓN SOCIAL |
|-----|---------------|--|
| 1 | 0190115798001 | COOPERATIVA DE AHORRO Y CREDITO JUVENTUD ECUATORIANA PROGRESISTA LTDA. |
| 2 | 0190155722001 | COOPERATIVA DE AHORRO Y CREDITO JARDIN AZUAYO LTDA. |
| 3 | 1790567699001 | COOPERATIVA DE AHORRO Y CREDITO 29 DE OCTUBRE LTDA. |
| 4 | 1790451801001 | COOPERATIVA DE AHORRO Y CREDITO COOPROGRESO LTDA. |
| 5 | 1190068389001 | COOPERATIVA DE AHORRO Y CREDITO VICENTINA MANUEL ESTEBAN GODOY ORTEGA LTDA. |
| 6 | 0690045389001 | COOPERATIVA DE AHORRO Y CREDITO RIOBAMBA LTDA. |
| 7 | 1890001323001 | COOPERATIVA DE AHORRO Y CREDITO OSCUS LTDA |
| 8 | 1890003628001 | COOPERATIVA DE AHORRO Y CREDITO SAN FRANCISCO LTDA |
| 9 | 0590052000001 | COOPERATIVA DE AHORRO Y CREDITO DE LA PEQUEÑA EMPRESA DE COTOPAXI LTDA. |
| 10 | 1790325083001 | COOPERATIVA DE AHORRO Y CREDITO ANDALUCIA LTDA. |
| 11 | 1890141877001 | COOPERATIVA DE AHORRO Y CREDITO MUSHUC RUNA LTDA |
| 12 | 1890037646001 | COOPERATIVA DE AHORRO Y CREDITO EL SAGRARIO LTDA |
| 13 | 1790093204001 | COOPERATIVA DE AHORRO Y CREDITO 23 DE JULIO LTDA |
| 14 | 1090033456001 | COOPERATIVA DE AHORRO Y CREDITO ATUNTAQUI LTDA |
| 15 | 1790501469001 | COOPERATIVA DE AHORRO Y CREDITO ALIANZA DEL VALLE LTDA. |
| 16 | 1890080967001 | COOPERATIVA DE AHORRO Y CREDITO CAMARA DE COMERCIO DE AMBATO LTDA. |
| 17 | 0790024656001 | COOPERATIVA DE AHORRO Y CREDITO SANTA ROSA LTDA |
| 18 | 0490001883001 | COOPERATIVA DE AHORRO Y CREDITO PABLO MUÑOZ VEGA LTDA. |
| 19 | 0390027923001 | COOPERATIVA DE AHORRO Y CREDITO DE LA PEQUEÑA EMPRESA BIBLIAN LTDA. |
| 20 | 1790979016001 | COOPERATIVA DE AHORRO Y CREDITO DE LOS SERVIDORES PUBLICOS DEL MINISTERIO DE EDUCACION Y CULTURA |
| 21 | 1790866084001 | COOPERATIVA DE AHORRO Y CREDITO POLICIA NACIONAL LTDA. |
| 22 | 1091720902001 | COOPERATIVA DE AHORRO Y CREDITO PILAHUIN TIO LTDA |
| 23 | 0490002669001 | COOPERATIVA DE AHORRO Y CREDITO TULCAN LTDA. |
| 24 | 0290003288001 | COOPERATIVA DE AHORRO Y CREDITO SAN JOSE LTDA |
| 25 | 1791708040001 | CAJA CENTRAL FINANCOOP |

Fuente: Superintendencia de Economía Popular y Solidaria (2015)

1.2.1.3. Contexto micro

En la ciudad de Ambato, se encuentran la mayor cantidad de empresas del comercio, como carroceras, plantas industriales de alimentos, fábricas de calzado, jean, ropa deportiva, etc., los mismos que usan frecuentemente los sistemas financieros, y se ven en la necesidad de utilizar el internet, o, en ciertos casos aplicaciones para teléfonos inteligentes y con estas herramientas realizar transacciones financieras, para ahorrar tiempo, ya que el proceso normal tomarían horas realizarlo y costaría mucho más que hacerlo por medios electrónicos, con este avance de la tecnología el cheque va perdiendo acogida, es por ésta razón que las cooperativas de ahorro y crédito, para diversificar sus servicios, buscan ofrecer los mismos productos que los Bancos, es decir, transferencias bancarias, emisión de tarjetas de crédito y debito, pagos de servicios básicos, etc., a través de medios electrónicos, los mismos ayudarían a agilizar las operaciones comerciales, pero nunca hay que dejar de lado, la adecuada Administración de los Riesgos y más los Operativos los mismos que abarcan los sistema de información y comunicación de cada una de las cooperativas de ahorro y crédito, así como, la confianza de los socios y socias, ya que, existe la incertidumbre al escuchar que pueden ser víctimas de las delincuencia informática.

De acuerdo al Boletín Mensual del Segmento 1 correspondiente al mes de noviembre, de la SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (2015)son 5 las cooperativas en el cantón Ambato que corresponden a éste segmento y al cual va dirigido la investigación, y son las siguientes:

TABLA 1.3. COOPERATIVAS SEGMENTO 1 – AMBATO

| RUC | RAZÓN SOCIAL |
|---------------|--|
| 1890001323001 | COOPERATIVA DE AHORRO Y CREDITO OSCUS LTDA |
| 1890003628001 | COOPERATIVA DE AHORRO Y CREDITO SAN FRANCISCO LTDA |
| 1890141877001 | COOPERATIVA DE AHORRO Y CREDITO MUSHUC RUNA LTDA |
| 1890037646001 | COOPERATIVA DE AHORRO Y CREDITO EL SAGRARIO LTDA |
| 1890080967001 | COOPERATIVA DE AHORRO Y CREDITO CAMARA DE COMERCIO DE AMBATO LTDA. |

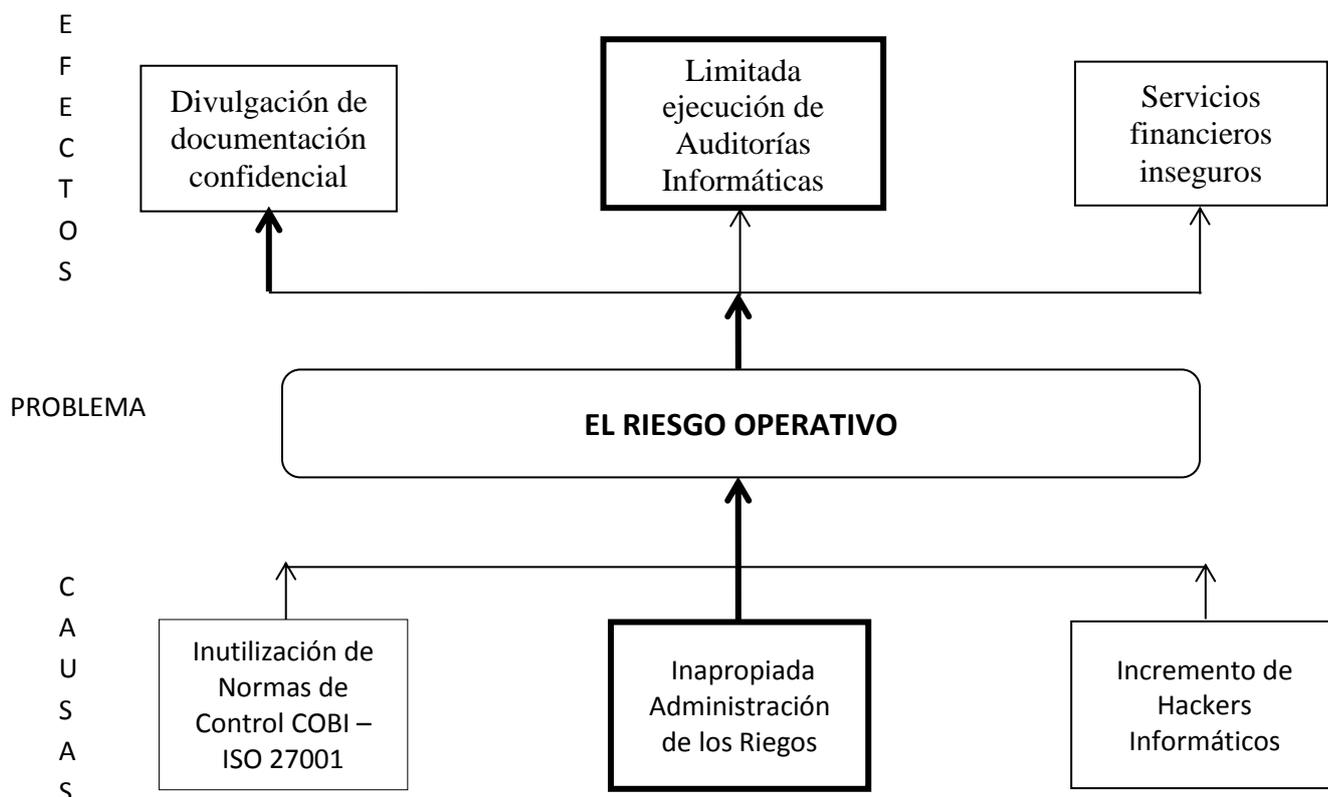
Elaborado por: Pilamunga, Alfonso (2017)

Fuente: Superintendencia de Economía Popular y Solidaria (2015)

1.2.2. Análisis crítico

Árbol del problema

GRÁFICO 1.1. ÁRBOL DEL PROBLEMA



Elaborado por: Pilamunga, Alfonso (2017)

Fuente: Elaboración propia (2017)

Relación causa-efecto

En avance de la tecnología a nivel mundial y en el Ecuador ha sido muy vertiginoso, por tal razón las cooperativas de ahorro y crédito correspondientes al segmento 1 en la ciudad de Ambato, se encuentran proporcionando servicios financieros que agilitan la vida comercial de las empresas y de las personas, causando así el problema de la inapropiada administración de los Riesgos Operativos de las tecnologías de la información y comunicación.

En este sentido, al ser relativamente nuevo los servicios financieros que proporcionan las Cooperativas de Ahorro y Crédito el problema planteado se da por la inutilización de las Normas de Control COBI – ISO 27001, sin la adecuada utilización, esto puede generar la ocurrencia de la divulgación de documentación confidencial para las cooperativas, lo que no garantiza a sus clientes la confiabilidad de sus datos personales y financieros, de la misma manera, se incurriría en la prestación de servicios financieros inseguros, ya que no se tiene la certeza de que las transacciones realizadas utilizando los sistemas de información puedan ser intersectadas por los Cyber – delincuentes, y ser víctimas de transferencias sin el consentimiento del titular, y; también, se incurriría en una limitada ejecución de auditorías informáticas, ya que no se encuentran previstos los factores de riesgo que se deberían evaluar.

Otra causa por la cual se genera el problema, es por la inapropiada Administración de los Riesgos Operativos en cuento a las tecnologías de la información y comunicación, las mismas que ayudan a los sistemas integrados de información a tener un mejor control interno, a través de la detección de riesgos inherentes con su respectivo tratamiento, pero, al no aplicarlos, ocasionaría que exista fuga de información confidencial, por ende, la divulgación de información, como datos de crédito, valores en las cuentas de ahorro, número de tarjetas, etc., en consecuencia, se tendría

un servicio financiero inseguro utilizado por los clientes, llegando así a la limitada ejecución de auditorías informáticas, ya que se vería aumentado el riesgo de detección al no tener el planteamiento claro de los factores de riesgos, y más aún al no contar con una unidad de Auditoría Informática para las Cooperativas de Ahorro y Crédito, esto podría no detectar ciertas irregularidades que se estén presentando en las aplicaciones para brindar servicios financieros.

Con relación a los efectos que la mala Administración de los Riesgos Operativos con respecto de los sistemas de información, en primer plano se encuentra la divulgación de la información confidencial, ya que, con dicha información se puede acceder a cuentas, transferencias bancarias, pagos de servicios de otras personas, etc., y caer así, en una limitada ejecución de las auditorías informáticas, por no tener lineamientos claros, ya que los hacker aprovechan la tecnología para ingresar a datos confidenciales de otras personas y hacer de las suyas, como interferir en las transferencias bancarias, apropiación de claves de acceso, direccionamiento de transferencias, etc., desde cualquier parte del mundo.

1.2.3. Prognosis

Actualmente, los servicios financieros prestado por los bancos se encuentran ganando territorio, y dejándole en segundo plano a las Cooperativas de Ahorro y Crédito, por tal razón, todas las cooperativas categorizadas en el segmento 1 se suman a las nuevas tecnologías de información y comunicación en diferentes escalas, para tratar de brindar servicios financieros ágiles, que optimicen el tiempo, para ello, se utiliza los sistemas de información y comunicación, y de esta manera, poder competir con los servicios financieros brindado por otras instituciones, en éste proceso se debe tener muy en cuenta, la apropiada Administración de los Riesgos Operativos de los sistemas de información y

comunicación. Al no tomar en cuenta este aspecto, los sistemas de información de las cooperativas serán vulnerables a cualquier ataque de los hackers, de este modo serán víctimas de los delitos informáticos, y ocasionarían pérdidas económicas por valores considerables, como ya ha sucedido en otros lugares, lo que también causaría que la reputación de las cooperativas de ahorro y crédito bajen, por ende que la aceptación en la sociedad y clientes sea menor debido a la desconfianza en los servicios financieros.

1.2.4. Formulación del problema

¿Es un componente relevante la Administración de Riesgos en las Auditorías informáticas en el sector cooperativo, Segmento 1 de la Ciudad de Ambato?

1.2.5. Preguntas directrices

- ¿Los procedimientos para la administración de los riesgos operativos con respecto a la utilización de las tecnologías de la información y comunicación en la Cooperativa son los adecuados?
- ¿Cree usted que es importante la realización de Auditorías informáticas en las Cooperativas?
- ¿Cree usted que la Administración de Riesgos Operativos con relación a las Tecnologías de Información y comunicación mejoraría con una Normativa que obligue la creación de una Unidad de Auditoría informática en el Organigrama estructural de las Cooperativas de Ahorro y Crédito segmento 1 de la ciudad de Ambato?

1.2.6. Delimitación del objeto de investigación

La investigación se encuentra enmarcada en la siguiente delimitación que contiene:

- **Campo:**
Auditoría.
- **Área:**
Auditoría Informática.
- **Aspecto:**
Riesgos Operativos.
- **Delimitación Espacial:**
Cantón Ambato, perteneciente a la Provincia de Tungurahua.
- **Delimitación Temporal:**
Está previsto realizar el trabajo de investigación en el segundo semestre del año 2017.
- **Delimitación Poblacional:**
Sector Cooperativo, Segmento 1.

1.3. JUSTIFICACIÓN

En el país no existe evidencia de estudios de post grado acerca de la Administración de Riesgos Operativos de Sistemas de Información y comunicación, específicamente en la ciudad de Ambato para el sector cooperativo correspondiente al Segmento 1, por lo que el presente trabajo de investigación surge como pionero en el tema; y, de esta forma

proporcionar información valiosa acerca de la Administración de Riesgos Operativos de Sistemas de Información y comunicación y su influencia en los resultados de las Auditorías Informáticas a todas las cooperativas que incurrieren en los servicios financieros a través de las nuevas tecnologías de información y comunicación; indagación, que en lo posterior servirá como base sólida para otras futuras investigaciones, como lo determina (Shuttleworth, 2008); así como, para la elaboración de técnicas o metodologías de control interno para los sistemas de información.

Con los antecedentes mencionados, el presente tema de investigación es factible, por la trascendencia que se tiene para la sociedad, por cuanto, las empresas o personas naturales dedicadas al comercio pudieran realizar sus transacciones financieras sin riesgos, ya que se contaría con una adecuada Administración de Riesgos Operativos a los sistemas de información, en consecuencia, una mayor demanda de los servicios financieros, con un alto grado de aceptación y confianza en la imagen institucional cooperativista, esto concuerda con el pensamiento de Torralba (2013) que manifiesta: “es necesaria la confianza en las instituciones: porque sin confianza no habrá eficacia, o esta será precaria; porque reduce el grado de incertidumbre, tan elevado en estos momentos; porque supone un ahorro en normas, reglamentos y protocolos; porque fomenta la cooperación y los acuerdos”.

Así mismo, es importante mencionar que, el presente estudio es factible, por cuanto, existe información actualizada acerca del sector cooperativo, es decir, la información provendrá del ente de control de las cooperativas, en este caso de la Superintendencia de Economía Popular y Solidaria, así como del Instituto de estadísticas y censo; y, otras entidades relacionadas al sector cooperativo, de la misma manera, por cuanto el investigador posee el recurso económico, humano y de tiempo para realizar la presente investigación.

1.4. OBJETIVOS

1.4.1. Objetivo general

Demostrar la influencia de la Administración de los Riesgos Operativos en las Auditorías Informáticas del sector Cooperativo Segmento 1 de la ciudad de Ambato para el mejoramiento del control interno.

1.4.2. Objetivos específicos

- Identificar los Riesgos Operativos en el Sector Cooperativo Segmento 1 de la ciudad de Ambato para una adecuada administración de riesgos de los sistemas de Información y Comunicación.
- Identificar la importancia de las Auditorías Informáticas en las Cooperativas de Ahorro y Crédito Segmento 1 de la ciudad de Ambato, para atribuir responsables de dichas auditorías.
- Proponer una Normativa de obligatoriedad de contar con una Unidad de Auditoría informática en el Organigrama estructural de las Cooperativas de Ahorro y Crédito segmento 1, para el fortalecimiento de la Administración de Riesgos Operativos de los Sistemas de Información y comunicación.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes Investigativos

En base a los estudios efectuados a los trabajos investigativos de similares características que se relacionan con el tema a investigar se resumen los siguientes:

En el Trabajo de Investigación de Bravo, Oswaldo (2010, pág. 139) con el tema de: “La Auditoría Informática como un factor de éxito en el cumplimiento de Objetivos Empresariales”, el autor establece las siguientes conclusiones: “Si dividimos por sectores podemos afirmar que las empresas industriales y comerciales, si bien tienen clara la necesidad de que sus procesos soportados por herramientas tecnológicas sea probados y revisados, no han incluido dentro de su estructura la función de auditoría de sistemas, el 100% de las empresas entrevistadas de esos sectores no cuentan con un auditor de sistemas”, así mismo hace incapié en las instituciones financieras con la siguiente conclusión: “En el caso de las instituciones financieras y empresas de telecomunicaciones sobre todo las internacionales, tienen en su área de auditoría un responsable para la parte de sistemas y esto es comprensible; ya que en el primer caso es una exigencia de su ente de control la Superintendencia de Bancos y Seguros, y la segunda por exigencia de su casa matriz y de la velocidad de desarrollo de la tecnología en éste sector”, conclusión muy acertada, ahora, al existir otro segmento denominado de economía popular y solidaria al cual pertenecen las Cooperativas y por el avance tecnológico muy creciente, se hace necesario el presente trabajo de investigación con la finalidad de fortalecer el sector cooperativo a través de la creación de la Unidad de Auditoría Informática.

En el Trabajo de Investigación denominado “Auditoría informática al departamento de Tecnologías de la Información (T.I.) de Hidropaute”, elaborado por Analuisa & Erazo (2007, pág. 156), los Autores plantean los siguientes objetivos: “Identificar si la empresa Hidropaute Mantiene un control adecuado de su área de T.I., en comparación con los estándares establecidos por la metodología COBIT, Identificar si la empresa Hidropaute se encuentra utilizando metodologías estándares para el área de T.I., y Efectuar recomendaciones para mejorar los controles” además al finalizar el trabajo se han determinado las siguientes conclusiones, las cuales se han considerado importantes: “Para realizar de forma más efectiva la auditoría utilizando el modelo COBIT, se recomienda que las personas que vayan a realizar el trabajo, revisen principalmente los siguientes documentos en secuencia: Cobit Framework, Directrices de Auditoría, Guía de Administración y Herramientas de Administración”, “Para cualquier empresa que quiera iniciar o mantener un proceso de control, el primer paso es la capacitación del personal involucrado, por lo que se recomienda, formar un grupo de personas especializadas, las cuales podrán posteriormente replicar sus conocimientos y técnicas hacia los demás participantes de la empresa”.

En el artículo científico de tema: “Auditoría con Informática a Sistemas Contables” publicado en la Revista de Arquitectura e Ingeniería, de Martínez, Briseida, & Marichal (2012, pág. 14), los autores en sus conclusiones establecen la importancia de la Auditoría Informática y las determinan así: “Se realizó un estudio de los conceptos teóricos relacionados con la auditoría, el control interno y la auditoría informática, destacando la importancia que tiene esta última en la aplicación a los sistemas contables”. “Se describió la acción de principales pruebas (de cumplimiento de controles y sustantivas), con la intervención de un auditor informático y el empleo de las herramientas WinIdea y ACL para la realización de auditorías a los sistemas contables, que permitirán que la auditoría financiera opere en un ambiente de eficiencia y mayor

confiabilidad”, por lo que se hace totalmente necesario un auditor informático en las instituciones financieras controladas por la Superintendencia de Economía Popular y Solidaria, para llegar a altos niveles de eficiencia y confiabilidad.

La conclusión para las transferencias electrónicas en el artículo científico denominado: “Aplicación de la norma COBIT en el monitoreo de transferencias electrónicas de datos contable-financieros” de Graterol & Hernández (2011, pág. 40) es: “La ejecución de la revisión del proceso de monitoreo de las transferencias electrónicas de datos contable-financieros de la Unidad de Contraloría y Administración de la Región Occidente del Grupo Lácteos Los Andes aplicando las normas COBIT ha permitido, entre otros aspectos, evaluar la adecuación de los controles establecidos, detectar algunas debilidades y riesgos potenciales en el funcionamiento del mismo. A partir de la definición de los aspectos anteriores se puede estar en capacidad de realizar un análisis exhaustivo de los objetivos de control que son necesarios para garantizar el correcto funcionamiento, la operatividad continua y calidad de resultados. Siguiendo el modelo de madurez COBIT, el proceso está definido de manera formal por la Gerencia TICs y se han desarrollado políticas y procedimientos de evaluación y reportes, incluyendo programas de adiestramiento de usuarios responsables del proceso. Sin embargo, se requiere una mayor integración del sistema de control informático interno con el resto de los procesos relacionados con el área contable-financiera”.

Con los antecedentes mencionados, se puede decir que el presente trabajo de investigación se encuentra enmarcado dentro de una temática de gran interés local, nacional e internacional en los últimos tiempos, por lo tanto, cuenta con el respaldo de trabajos de investigación, los cuales van a aportar información valiosa a ésta investigación, facilitando así su desarrollo y ejecución.

2.2. FUNDAMENTACIÓN FILOSÓFICA

La presente investigación se encuentra alineada con el Paradigma Crítico-Propositivo; crítico por cuanto estudia y debate la realidad en cuanto a la mala Administración de Riesgos Operativos de las Tecnologías de la Información; y, Propositivo porque a través de él se busca plantear una alternativa de solución a la problemática en estudio.

De acuerdo con Herrera, Medina, & Naranjo (2010, pág. 20): “Este enfoque privilegia la interpretación, comprensión y explicación de los fenómenos sociales en perspectiva de totalidad”, por lo tanto el paradigma crítico propositivo constituye la mejor opción para la presente investigación, para una adecuada comprensión del tema tratado.

Fundamentación Epistemológica

Para Cerda, H. (1998, pág. 42) la epistemología es “aquella filosofía o teoría de la ciencia que estudia críticamente los principios, las hipótesis y los resultados de las diversas ciencias, con el propósito de determinar su origen y estructura, su valor y alcance objetivo”, en este contexto, el fundamento epistemológico para el presente trabajo se enfoca en una investigación sistemática, controlada y empírica, ya que los datos obtenidos deben ser procesados para la comprobación científica a través de un método estadístico.

En consecuencia, el presente trabajo de investigación además de solucionar el problema planteado, contribuirá en la generación de nuevo conocimiento y servirá como base para futuras investigaciones, además de ayudar al sector cooperativo.

Fundamentación Ontológica

En términos de Gilson E. (1962, pág. 132) la ontología es: “Aquella ciencia del ser como tal y de las propiedades que le pertenecen, estudia el ser en general, es decir el fundamento de todo lo que es”, es decir, la razón de ser para el presente trabajo de investigación es el estudio de los factores que crearon el problema para de ésta manera recomendar una posible solución. En efecto, se estudiará las causas que originan la mala Administración de los Riesgos Operativos de los sistemas de información del sector cooperativo, en especial, al segmento 1, para determinar una solución adecuada que genere beneficios al sector.

Fundamentación Axiológica

La presente investigación estará apegada a los valores propios de la fundamentación axiológica, conjuntamente con los valores del investigador que son: disciplina, respeto, rectitud, la honestidad científica y la verdad concluyente sea cual fuere sus resultados, de esta manera se podrá garantizar una investigación que contribuya al descubrimiento de la verdad de los hechos, proporcionando así conocimientos válidos, confiables y razonables sobre la temática de estudio.

2.3. FUNDAMENTACIÓN LEGAL

Según la constitución de la República del Ecuador (Asamblea Nacional, Constitución de la República del Ecuador, 2015), en el numeral 2 del Art. 16.- relacionado a que todas las personas, en forma individual o colectiva, tienen derecho a: “El acceso universal a las tecnologías de información y comunicación”.

Así mismo es menester hacer referencia al Art. 18 ibídem.

Art. 18.-Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior.

2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley.

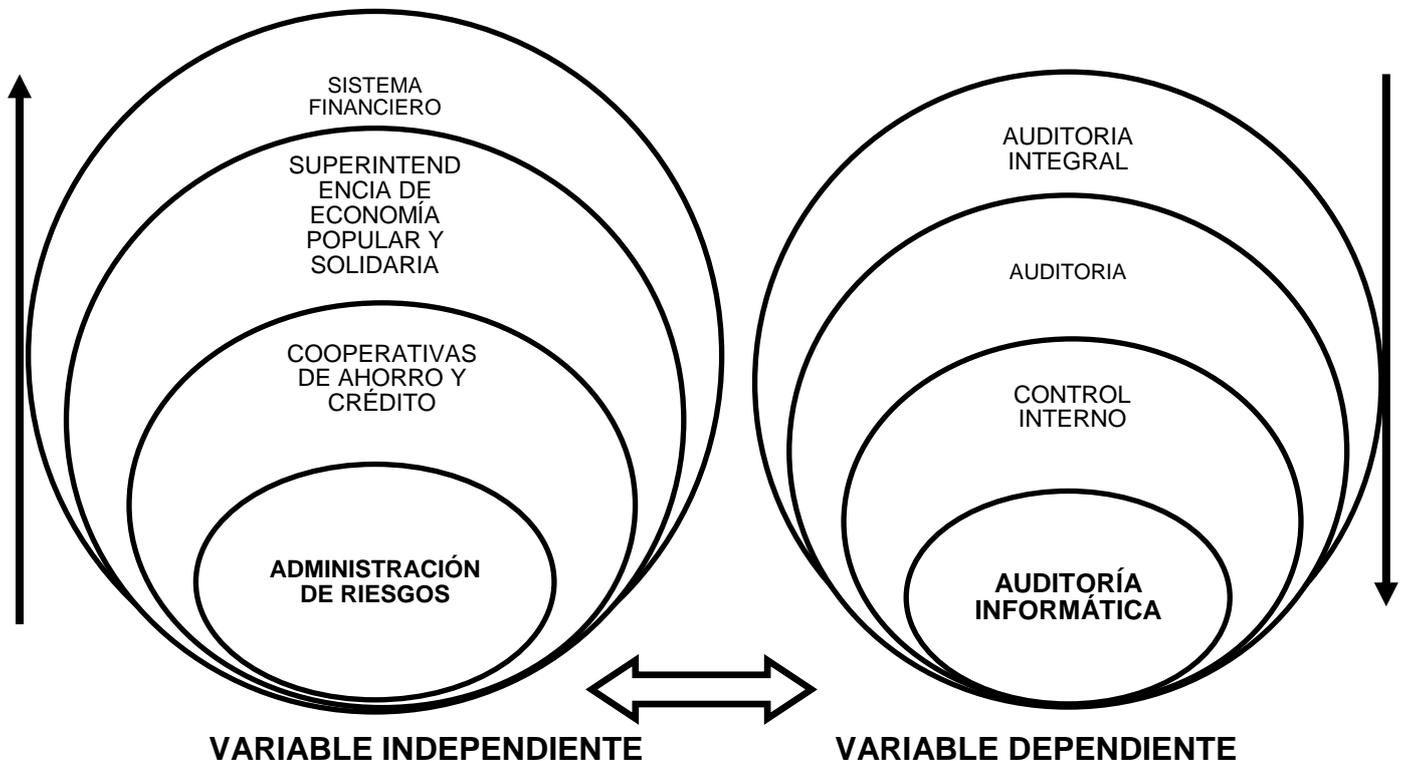
Es importante mencionar que las personas que mantienen cuentas en las cooperativas tienen derecho a recibir un servicio de calidad y no engañosa conforme lo manifiesta el Art. 52 ibídem, “Las personas tienen derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a una información precisa y no engañosa sobre su contenido y características”.

Según el Capítulo III acerca del Control, del Reglamento de la Ley Orgánica del Sistema de Economía Popular y Solidaria (2012) en su Art. 154. Atribuciones de la Superintendencia de Economía Popular y Solidaria en el Numeral 6 tenemos: “Revisar los informes de auditorías para su aceptación o formulación de observaciones”, es decir, que todas las Cooperativas Reguladas por la Superintendencia deberán presentar los informes de auditoría para la revisión respectiva por su ente de control, cuestión por la cual, el presente trabajo de investigación se realiza sobre la premisa de la Auditoría de Sistemas, ya que las cooperativas especialmente las categorizadas en el Segmento 1 se encuentran en la etapa de sistematización de todos sus servicios.

Según la Resolución 128-2015-F de la Junta de Política y Regulación Monetaria y Financiera se emite las Normas para la Administración Integral de Riesgos en las Cooperativas de Ahorro y Crédito y Cajas Centrales, en las cuales se establecen los tipos de riesgos, para el caso del presente trabajo investigativo se tomará en cuenta los Riesgos Operativos, contemplados en el Art. 15.

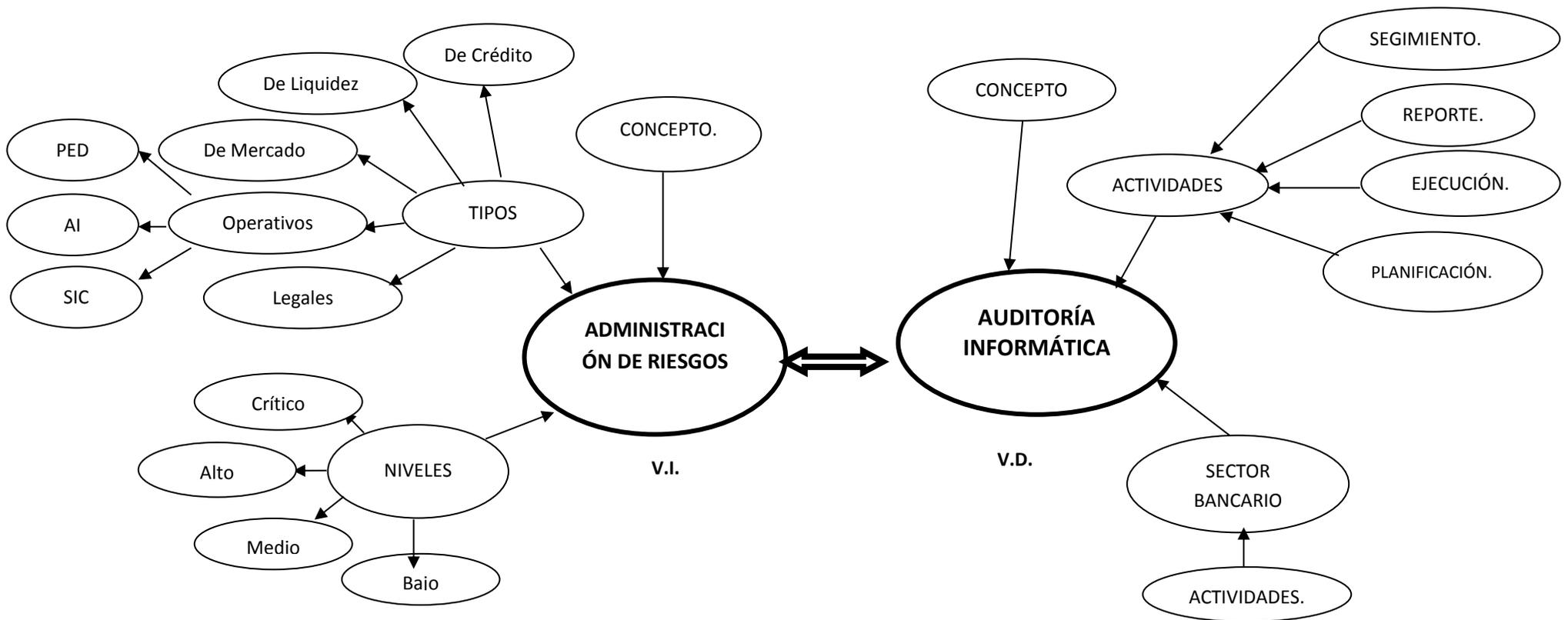
2.4. Categorías Fundamentales

GRÁFICO 2.1. RED DE INCLUSIONES CONCEPTUALES



Elaborado por: Pilamunga, Alfonso (2017)
 Fuente: Elaboración propia (2017)

GRÁFICO 2.2. CONSTELACIÓN DE IDEAS



Elaborado por: Pilamunga, Alfonso (2017)
Fuente: Elaboración propia (2017).

2.4.1. Marco Conceptual Variable Independiente

Sistema Financiero

Según Chiriboga, Luis (2010, pág. 6) el Sistema Financiero “Constituye uno de los sectores más importantes de la economía, que permite proveer de servicio de pagos, movilizar el ahorro y asignar crédito, además de limitar, valorar, aunar e intercambiar los riesgos resultantes de esas actividades. Diversas instituciones (Bancos, Sociedades Financieras, Mutualistas, Cooperativas de Ahorro y Crédito, Compañías de Seguros, Casas de Valores, Almacenes, etc.) prestan estos servicios, que son utilizados en diferentes combinaciones por unidades familiares, empresas y gobierno, mediante toda una serie de instrumentos (dinero, tarjetas de crédito, bonos, acciones, seguros, etc.).”

Para (Tus Finanzas, 20015) El sistema financiero es “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 del país haciendo que los fondos lleguen desde las personas que tienen recursos monetarios excedentes hacia las personas que necesitan estos recursos. Los intermediarios financieros se encargan de captar depósitos del público (ahorros), y, prestarlos a los demandantes de recursos (créditos).”.

Superintendencia de Economía Popular y Solidaria

Según la (SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA, 2015) la institución es: “una entidad técnica de supervisión y control de las organizaciones de la economía popular y solidaria, con personalidad jurídica de derecho público y autonomía administrativa y financiera, que busca el desarrollo, estabilidad, solidez y correcto funcionamiento del sector económico popular y solidario.” De la misma

manera tiene como objeto en concordancia con la Constitución de la República del Ecuador (Asamblea Nacional, Constitución de la República del Ecuador, 2015) en su Art. 283 las siguientes:

“Reconocer a las organizaciones de la economía popular y solidaria como motor del desarrollo del país; Promover los principios de la cooperación, democracia, reciprocidad y solidaridad en las actividades económicas que realizan las organizaciones de la EPS; Velar por la estabilidad, solidez y correcto funcionamiento de las organizaciones de la EPS; Establecer mecanismos de rendición de cuentas de los directivos hacia los socios y miembros de las organizaciones de la economía popular y solidaria; Impulsar la participación activa de los socios y miembros en el control y toma de decisiones dentro de sus organizaciones, a diferencia de las actividades económicas privadas; Identificar nuevos desafíos para el diseño de políticas públicas que beneficien, fortalezcan y consoliden al sector económico popular y solidario; Fortalecer la gestión de las organizaciones en beneficio de sus integrantes y la comunidad.”.

Cooperativas de Ahorro y Crédito

Para (Mi banco me Enseña, Banco del Pacífico, 2015) las Cooperativas de Ahorro y Crédito son “asociaciones autónomas de personas que se reúnen de forma voluntaria para satisfacer sus necesidades y aspiraciones económicas, sociales y culturales, mediante una empresa de propiedad conjunta y gestión sin fines de lucro.

Según Chiriboga, Luis (2010, pág. 9) las Cooperativas de Ahorro y Crédito son “Sociedades financieras de derecho privado, formadas por personas naturales o jurídicas, que sin perseguir finalidades de lucro, tienen por objeto planificar y realizar actividades de trabajo en beneficio social o colectivo, a través de una empresa manejada en común y formada con la aportación económica, intelectual y moral de sus miembros.”.

Administración de Riesgos

Según la Resolución No. 128-2015-F de la Junta de la Política y Regulación Monetaria y Financiera (2015), en su Art. 3 la Administración de Riesgos es “el proceso mediante el cual las entidades identifican, miden, priorizan, controlan, mitigan, monitorean y comunican los riesgos a los cuales se encuentran expuestas”.

Tipos de Riesgos

Dentro de la normativa antes citada, por ser la de regulación nacional, se toma en cuenta lo descrito en el Art. 15, que describe los tipos de riesgos de acuerdo al siguiente detalle:

- a) Riesgo de Crédito: es la probabilidad de pérdida que asume la entidad como consecuencia del incumplimiento de las obligaciones contractuales asumidas por la contraparte.
- b) Riesgo de Liquidez: es la probabilidad de que una entidad no disponga de los recursos líquidos necesarios para cumplir a tiempo sus obligaciones y que, por tanto, se ve forzada a limitar sus operaciones, incurrir en pasivos con costo o vender sus activos en condiciones desfavorables;
- c) Riesgo de Mercado: es la probabilidad de pérdida en que una entidad puede incurrir por cambios en precios de activos financieros, tasas de interés y tipos de cambio que afecten el valor de las posiciones activas y pasivas;
- d) Riesgo Operativo: es la posibilidad que se produzca pérdidas para la entidad, debido a fallas o insuficiencias originadas en procesos, personas, tecnología de la información y eventos externos; y
- e) Riesgo Legal: es la probabilidad de que una entidad incurra en pérdidas debido a la inobservancia e incorrecta aplicación de

disposiciones legales e instrucciones emanadas por organismos de control; aplicación de sentencias o resoluciones judiciales o administrativas adversas; deficiente redacción de textos; formalización o ejecución de actos, contratos o transacciones o porque los derechos de las partes contratantes no han sido debidamente estipuladas.

Procesamiento electrónico de datos (PED)

Este apartado hace referencia a la utilización de métodos automatizados para procesar grandes volúmenes de datos comerciales, financieros, etc., a través de un computador electrónico, así como lo describe Langenbach Robert G. (1976, pág. 145) que manifiesta “Cuando un sistema ha de procesar grandes volúmenes de datos a velocidades muy elevadas y con un alto grado de exactitud, entra en funciones el ordenador electrónico, que puede suministrar a la dirección más información con mayor rapidez y a un costo inferior por unidad de información”.

Ambiente Informático (AI)

El presente hace referencia, a que el auditor debe estar suficientemente preparado en conocimientos de auditoría, control, informática y actividades que desarrolla la empresa a la cual se va a auditar, ya que ese será su ambiente informático, es así que Delgado Xiomar (2015, pág. 56) lo describe de la siguiente manera “un auditor informático, con una base fundamental de auditoría se sustenta también en la solidez que se requiere en lo que se refiere a control, y de los específicos que deben ser los conocimientos de la informática para realizar la evaluación del ambiente informático de una empresa determinada”.

Sistemas de información computarizada (SIC)

Es cuando se diseñan nuevos sistemas de información a través del computador, los mismos deberán elaborarse con la colaboración de un auditor informático, así como lo manifiesta Galán Leonor 32 (1996, pág. 32).

Niveles de Riesgo

Según la Resolución No. 128-2015-F de la Junta de la Política y Regulación Monetaria y Financiera (2015), en el Art. 18, se establecen los siguientes niveles de riesgo:

- a) Riesgo Crítico: cuando el riesgo representa una probabilidad de pérdida alta que puede afectar gravemente a la continuidad del negocio e incluso llevar a la liquidación de la entidad y que, por lo tanto, requiere acciones inmediatas por parte del consejo de Administración y la Gerencia;
- b) Riesgo Alto: cuando el riesgo representa una probabilidad de pérdida alta, que puede afectar el funcionamiento normal de ciertos procesos de la entidad, y que requiere la atención del Consejo de Administración y la Gerencia;
- c) Riesgo Medio: cuando el riesgo representa una probabilidad de pérdida moderada, que afecta a ciertos procesos de la entidad, y que requiere la atención de la Gerencia y de mandos medios; y,
- d) Riesgo Bajo: cuando el riesgo representa una probabilidad de pérdida baja, que no afecta significativamente a los procesos de la entidad, y que se administran con controles y procedimientos rutinarios.

2.4.2. Marco Conceptual Variable Dependiente

Auditoría Integral

Para Yanel Blanco (2015, pág. 5) la auditoría integral es “un modelo de cobertura global y por lo tanto no se trata de una suma de auditorías, pero se puede estructurar con base en normas de auditoría y aseguramiento de general aceptación”, esto implicaría, que la ejecución de un trabajo de auditoría integral incluirá la de auditoría financiera, de cumplimiento, de control interno financiero y de gestión, etc.

Auditoría

Según (Piattini & Del Peso , pág. 4) manifiesta que la Auditoría es “la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple condicione que le han sido prescritas.

Control Interno

Para Viloría, Norka (2005, p. 88) “el intercambio constante entre los individuos y la organización, establecer un mínimo de reglas que permitan la operatividad organizacional. Este mínimo de normas se conoce como Sistema de Control Interno. Sin embargo, pareciera que las organizaciones se han constituido más por hacer y con base en la experiencia, que por estudios de planes de negocios y diseño organizacional. Esto ocasiona que los sistemas de control interno no respondan a las necesidades organizacionales”, en efecto, algunas organizaciones se han basado en la experiencia y en cubrir ciertas necesidades de las personas a través de los servicios que se puedan ofrecer, y es ahí, cuando se descuida el control interno.

De acuerdo a las SAS No. 1 (Statement on Auditing Standards) (1948), Del Instituto Americano de Contadores Públicos define al control Interno como: “El control interno comprende el plan de organización, todos los métodos coordinados y las medidas adoptadas en el negocio, para proteger sus activos. Verificar la exactitud y confiabilidad de sus datos contables, promover la eficiencia en las operaciones y estimular la adhesión a la práctica ordenada por la gerencia”, en verdad, el control interno es de suma importancia para la protección de los activos, ya que con un adecuado procedimiento, mitigando el riesgo inherente existente se puede llegar a éste objetivo.

Según Cooper & Lybran (1997, pág. 16) “El control Interno es un proceso efectuado por el consejo de administración, la dirección y el resto del personal de la entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías: Eficacia y eficiencia de las operaciones, Fiabilidad de la información financiera y cumplimiento de leyes y normativas aplicables”, es por tal razón, que el control interno no es solo responsabilidad del Auditor, sino de todo el personal, ya que el uso adecuado de los sistemas de información así como de los procedimientos harán que los objetivos institucionales se cumplan, y por lo tanto, la empresa refleje sus valores razonablemente hacia sus socios.

Control Interno Informático

Para Fonseca, Oswaldo (2011, pág. 26) el Control interno Informático esta ayudado por una herramienta denominada “CobiT, (Control Objectives for Information and Related Technology), es una herramienta de Tecnología de Información (TI) para uso de las entidades. A diferencia del modelo de control que preconiza el COSO, el CobiT proporciona buenas prácticas para los procesos de negocios y la información resultante de la aplicación combinada de recursos que requieran ser administrados, apoyados por la

tecnología de la Información. Estas prácticas están enfocadas más al fortalecimiento del control que a su ejecución, siendo una estructura apropiada para la seguridad y el control de la TI”.

De acuerdo con Echenique, José (2006, pág. 16) “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 participan en el procesamiento 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”

Además Pinilla, José (2005, pág. 1) manifiesta que: “El control interno informático puede definirse como el sistema integrado al proceso administrativo, en la planeación, organización, dirección y control de las operaciones con el objeto de asegurar la protección de todos los recursos informáticos y mejorar los índices de economía, eficiencia y efectividad de los procesos operativos computarizados”, esto debido a que la mayoría de empresas a través del avance científico ha automatizado sus procesos a través de sistemas de información o sistemas contables.

Sistemas de Información

En palabras de O’Brien, James (2001, pág. 42) “Un sistema de información depende de los recursos humanos (Usuarios finales y especialistas en SI), hardware (máquinas y medios), software (programas y procedimientos), datos (base de datos y de conocimientos) y redes (medios de comunicación y soporte de redes) para desempeñar actividades de entrada, procesamiento, salida, almacenamiento y control que conviertan los recursos de datos en resultados de información”, lo cual es muy importante en la actualidad, ya que cualquier dato ingresado a un sistema de información para procesado, almacenado y que como

salida se tenga información gerencial para una organización y se pueda tomar decisiones oportunas.

Para Prieto & Martínez (2004, pág. 336) “Los sistemas de información deben estar al servicio de la organización y de esta manera establecer su enfoque o estrategia de negocio, hecho éste en oportunidades ignorado por la gerencia y en muchos casos manipulado para convenimiento de sus intereses. El sistema de información debe ser considerado como uno de los subsistemas que conforman la organización, creado por ella misma para ser utilizado en el logro de sus objetivos, y como dicho sistema sirve de base en la estrategia de negocio puede ser utilizada para lograr ventajas competitivas”, es decir, los sistemas de información están para ayudar a la consecución de objetivos, facilitando el trabajo y haciéndole más rápido el servicio brindado, pero siempre que sea utilizado de una buena manera y bajo los controles respectivos.

Auditoría Informática

Para Martínez, Briseida, & Marichal (2012, pág. 4) la auditoría es: “un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados, cuyo fin consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como establecer si dichos informes se han elaborado observando los principios establecidos para el caso”, por lo tanto, con esto se analizará todo informe o reporte en el cual ha intervenido las tecnologías de la información.

Ahora, según León & Martínez García (1999, pág. 4) la auditoría de sistemas o informática es 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”, por ende, la eficacia y eficiencia están estrechamente relacionadas con los controles internos a los sistemas informáticos.

En palabras de Morilla, Ignacio (2002, pág. 150) la Auditoría de sistemas o informática “aparece como una de las herramientas más útiles, eficientes y con mayor coste / rentabilidad para determinar la vulnerabilidad de los sistemas de información de la empresa”, es decir, a través de la auditoría de sistemas se determinarán los riesgos de los sistemas de información para la respectiva mitigación, dicha auditoría, es de suma importancia en sectores que en la actualidad todo su sistema contable, financiero y de talento humano se encuentran sistematizados.

De acuerdo con la Asociación de Control y Auditoría de Sistemas de Información conocida por sus siglas ISACA (Information Systems Audit and Control Association) (2005) en su Normas generales para la auditoría de sistemas de información dice que:

La auditoría informática deberá comprender no sólo 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 obtención de información” es decir, un examen completo a los sistemas de información, además en las normas nos describen las actividades que se deben realizar en la auditoría informática, las mismas que son:

a. Planificación.

En la planificación de una auditoría informática se deben cumplir con los siguientes aspectos:

El auditor debe planear el alcance de la auditoría informática para cubrir los objetivos planteados y cumplir con las leyes aplicables y las normas profesionales de auditoría.

El auditor debe desarrollar y documentar un enfoque de auditoría basado en riesgos.

El auditor debe desarrollar y documentar un plan de auditoría que detalle la naturaleza y los objetivos de la auditoría, los plazos y alcance, así como los recursos requeridos.

El auditor debe desarrollar un programa y/o plan de auditoría detallando la naturaleza, los plazos y el alcance de los procedimientos requeridos para completar la auditoría.

Para una función de auditoría interna, debe desarrollarse/actualizarse un plan, al menos una vez al año, para las actividades permanentes. El plan debe servir como marco de referencia para las actividades de auditoría y servir para abordar las responsabilidades establecidas por el estatuto de auditoría. El nuevo/actualizado plan debe ser aprobado por un consejo de administración.

Para el caso de una auditoría externa, normalmente debe prepararse un plan para cada una de las tareas, sean o no de auditoría. El plan debe documentar los objetivos de la auditoría.

El auditor debe obtener un entendimiento de la actividad que está siendo auditada. El grado del conocimiento requerido debe ser determinado por la naturaleza de la organización, su entorno y riesgos, y por los objetivos de la auditoría.

El auditor debe realizar una evaluación de riesgos para brindar una garantía razonable de que todos los elementos materiales serán cubiertos adecuadamente durante la auditoría. En este momento, es posible establecer las estrategias de auditoría, los niveles de materialidad y los recursos necesarios.

El programa y/o plan de auditoría puede requerir ajustes durante el desarrollo de la auditoría para abordar las situaciones que surjan (nuevos riesgos, suposiciones incorrectas o hallazgos en los procedimientos ya realizados) durante la auditoría.

b. Ejecución de la Auditoría.

A continuación se enuncian normas que proporcionar asesoría con respecto a la realización de las auditorías:

Supervisión. El personal de auditoría debe ser supervisado para brindar una garantía razonable de que se lograrán los objetivos de la auditoría y que se cumplirán las normas profesionales de auditoría aplicables.

Evidencia. Durante el transcurso de la auditoría, el auditor debe obtener evidencia suficiente, confiable y pertinente para alcanzar los objetivos de auditoría. Los hallazgos y

conclusiones de la auditoría deberán ser soportados mediante un apropiado análisis e interpretación de dicha evidencia.

Documentación. El proceso de auditoría deberá documentarse, describiendo las labores de auditoría realizadas y la evidencia de auditoría que respalda los hallazgos y conclusiones del auditor.

Se deben establecer los roles y responsabilidades del equipo de auditoría al iniciarse la auditoría, y como mínimo deben definirse los roles de decisión, ejecución y revisión.

Las labores realizadas durante la ejecución del trabajo deben organizarse y documentarse siguiendo procedimientos documentados predefinidos. La documentación debe incluir aspectos tales como los objetivos y alcance del trabajo, el programa de auditoría, los pasos de auditoría realizados, la evidencia recogida, los hallazgos, conclusiones y recomendaciones.

La documentación de auditoría debe ser suficiente para permitir que una tercera entidad independiente vuelva a realizar todas las tareas realizadas durante la auditoría para llegar a las mismas conclusiones.

La documentación de auditoría debe incluir detalles de quién realizó cada tarea de auditoría y sus funciones. Como regla general, cada tarea, decisión, paso o resultado de la auditoría realizado por un miembro o grupo de miembros del equipo deberá ser revisado por otra persona del equipo, nombrada de acuerdo con la importancia del elemento considerado.

El auditor debe planificar el uso de la evidencia de auditoría obtenida de manera coherente con la importancia del objetivo de la auditoría y el tiempo y esfuerzo involucrados en obtener la evidencia de auditoría.

La evidencia de auditoría debe ser suficiente, confiable y pertinente para formar una opinión o respaldar los hallazgos y conclusiones del auditor. Si, en opinión del auditor, la evidencia de auditoría obtenida no cumple con estos criterios, el auditor deberá obtener evidencia de auditoría adicional.

c. Reporte de Auditoría

Las siguientes normas establecen y proporcionar asesoría sobre la generación del informe, a fin de que el auditor pueda cumplir con esta responsabilidad para que se presente un documento que sea muy claro para el personal:

El auditor debe suministrar un informe, en un formato apropiado, al finalizar la auditoría. El informe debe

identificar la organización, los destinatarios previstos y respetar cualquier restricción con respecto a su circulación.

El informe de auditoría debe indicar el alcance, los objetivos, el período de cobertura y la naturaleza, plazo y extensión de las labores de auditoría realizadas.

El informe debe indicar los hallazgos, conclusiones y recomendaciones, así como cualquier reserva, calificación o limitación que el auditor tuviese en cuanto al alcance de la auditoría.

El auditor debe tener evidencia de auditoría suficiente y apropiada para respaldar los resultados reportados.

Al emitirse, el informe del auditor debe ser firmado, fechado y distribuido de acuerdo con los términos del estatuto de auditoría o carta de compromiso.

El formato y contenido del informe generalmente varían según el tipo auditoría realizada. Un auditor puede realizar cualquiera de las siguientes acciones:

- Auditoría (de manera directa o como testigo)

- Revisión (de manera directa o como testigo)

- Procedimientos acordados

Cuando se requiera que el auditor proporcione una opinión sobre el entorno de control y exista evidencia de auditoría sobre una debilidad material o significativa, el auditor no deberá concluir que los controles internos son eficaces. El informe del auditor debe describir la debilidad material o significativa y el efecto en el logro de los objetivos de los criterios de control.

El auditor debe comentar el contenido del informe en borrador con la gerencia del área bajo revisión antes de la finalización y divulgación, e incluir los comentarios de la gerencia en el informe final cuando corresponda.

Cuando el auditor encuentre deficiencias significativas en el entorno de control, el auditor debe informar sobre estas deficiencias al comité de auditoría o a la autoridad responsable y comentar en el informe que se han comunicado dichas deficiencias significativas.

Cuando el auditor emita informes separados, el informe final deberá hacer referencia a todos los informes separados.

El auditor debe considerar y evaluar si comunicará a la gerencia acerca de las deficiencias en los controles internos de menor magnitud que las deficiencias significativas. En tales casos, el auditor debe informar al comité de auditoría o a la autoridad responsable que se han comunicado a la gerencia dichas deficiencias del control interno.

El auditor debe solicitar y evaluar la información sobre los hallazgos, las conclusiones y las recomendaciones de informes anteriores a fin de determinar si se han

implementado las acciones apropiadas de manera oportuna.

d. Monitoreo y Control

Las siguientes normas proporcionan asesoría con respecto a las actividades de seguimiento realizadas durante un proceso de auditoría, que deben ser tomadas en cuenta:

Después de informar/reportar sobre los hallazgos y las recomendaciones, el auditor debe solicitar y evaluar la información relevante para concluir si la gerencia tomó las acciones apropiadas de manera oportuna.

Si las acciones propuestas por la gerencia para implementar las recomendaciones notificadas se proporcionaron al auditor, se comentaron con éste, dichas acciones deberán registrarse en el informe final como la respuesta de la gerencia.

La naturaleza, los plazos y la extensión de las actividades de seguimiento deben tener en cuenta la importancia de los hallazgos reportados y el impacto, en caso de no haberse tomado las acciones correctivas. Los plazos de las actividades de seguimiento de una auditoría en relación con el informe original deben basarse en el juicio profesional y depender de una serie de consideraciones tales como la naturaleza o magnitud de los riesgos y costos asociados a la entidad.

La función de auditoría interna debe establecer un proceso de seguimiento para monitorear y asegurar que las acciones de la gerencia efectivamente han sido implementadas o que la gerencia superior ha aceptado el riesgo de no haber tomado la acción pertinente. La responsabilidad por estas actividades de seguimiento puede definirse en el estatuto de auditoría.

Cuando la gerencia proporcione información sobre las acciones tomadas para implementar las recomendaciones y el auditor tenga dudas con respecto a la información suministrada, se deberán llevar a cabo las pruebas apropiadas u otros procedimientos para determinar la posición o estado reales antes de concluir las actividades de seguimiento.

Puede presentarse un informe, sobre el estado de las actividades de seguimiento, que incluya las recomendaciones aceptadas no implementadas, ante el comité de auditoría en caso de que éste se haya establecido, o, como alternativa, al nivel apropiado de la gerencia de la entidad.

Como parte de las actividades de seguimiento, el auditor deberá evaluar si los hallazgos no implementados siguen siendo importantes.

Normas generales que deben ser aplicados y revisados periódicamente para el buen uso, y un desarrollo adecuado del control interno.

Existe también, otras actividades de auditoría, esto, según Rivas Gonzalo (1988, pág. 47) los cuales se pueden obviar en función de las características a auditar, y estos son:

Toma de contacto: La cual se relaciona a recabar toda la información relativa a la empresa a la que se va a auditar, punto de relevancia cuando se trata de auditores externos.

Planificación de la operación: Este punto según el autor es en el cual se desarrolla el plan de trabajo, las áreas que se van a cubrir, es decir, el alcance, además de que en esta etapa el auditor deberá conocer que personas intervienen en los procesos y los procesos en sí.

Fase de diagnóstico: En este punto el auditor analizará e interpretará todos los datos obtenidos de la empresa auditada, con la finalidad de concluir un diagnóstico de la situación real de la empresa.

Presentación de conclusiones: En esta actividad, el auditor debe presentar sus conclusiones suficientemente argumentadas, probadas y documentas para que la empresa no pueda ser refutada.

Formación del plan de mejoras: En este punto, la empresa o el auditor deberán presentar un plan de mejoras, para poder erradicar para próximas auditorias todos los hallazgos encontrados.

Auditoría Informática en el Sector Bancario

Con el avance tecnológico a nivel global, y por ende, en las instituciones financieras se ha creado la función de la auditoría informática recientemente, por lo que Pianttini & Del Peso (2005, pág. 510) manifiesta: “la faceta en la que la participación de auditoria informática en el sector financiero es m{as valiosa la constituye, quizás, la revisión de las aplicaciones informáticas, con el objeto de asegurar que ellas cumplen con los criterios de funcionales y operativos definidos por la entidad financiera. Esta actividad, que forma parte del ámbito de actuación habitual de la auditoria informática en todos los bancos que tienen como tal implantada la función, es de extrema importancia por cuanto comúnmente un error en la interpretación de un criterio, una especificación incompleta, una deficiencia en un algoritmo, suelen tener un impacto elevado, bien por el número de operaciones que resulten

afectas, bien por la repercusión económica del error”, en la actualidad, las cooperativas pertenecientes a la Economía Popular y Solidaria también pretenden utilizar tecnologías de la información para la utilización del dinero electrónico, sistema que debería garantizar el dinero de los socios.

Tipología de las Actividades a auditar

Con el antecedente, de que las cooperativas observan la necesidad de proporcionar más aplicaciones para facilitar el manejo de los recursos de sus socios, proyectan proporcionar servicios a través de aplicaciones, portales electrónicos para el manejo de los recursos de los socios, por lo que es importante mencionar ciertas actividades a auditar, esto según Pianttini & Del Peso (2005, pág. 511) que menciona:

Distinguimos en primer lugar, por su importancia en el conjunto de procesos informáticos de un banco, así como por las implicaciones de cualquier posible error, las auditorías de aplicaciones informáticas que tratan y soportan productos bancarios típicos: planes y fondos de pensiones, fondos de inversión, cuentas corrientes, de ahorro, de plazo y demás productos del pasivo tradicional, inversión crediticia (créditos, préstamos, descuentos de efectos), etc. (..)

Estas aplicaciones tienen básicamente las siguientes características:

- Procesan y generan un gran volumen de datos relativos a contratos y operaciones.
- Los procesos de tratamiento de los datos son relativamente sencillos (aun cuando en algún caso puedan resultar conceptualmente complejos); sin embargo, comparativamente suponen un gran consumo de recursos en el total de los procesos informáticos de un banco.
- Las operaciones y productos tanto por estas aplicaciones tienen normalmente un importante peso específico en el balance de la entidad.
- La disponibilidad de la información suele ser un factor crítico.
- La información generada tiene un elevado alcance, por cuanto se envía masivamente hacia destinos externos a la propia entidad financiera.
- En estas aplicaciones se produce un efecto amplificado de error; cualquier incidencia puede afectar a un número elevado de operaciones y tener más repercusión económica cifrada en millones de pesetas.

En segundo lugar podemos distinguir las auditorías de medios de pago: tarjetas de débito y crédito, transferencias de fondos, cheques personales, cheques de viaje, etc.

Entre las particularidades de estos sistemas destacan:

- Alto volumen de transacción y de clientes
- Existencia de regulaciones específicas para su tratamiento informático y operativo, consecuencia de los convenios suscritos con distintos organismos.
- Son áreas de las que los aspectos de control tienen gran relevancia, principalmente en materia de prevención de fraudes, así como el cumplimiento de diversas normas emitidas por el Banco de España.

2.5. Hipótesis

La Administración de Riesgos es un componente relevante en las Auditorías informáticas en el sector cooperativo, segmento 1 de la ciudad de Ambato.

2.6. Señalamiento de variables de la Hipótesis

- **Variable Independiente:** Administración de Riesgos

- **Variable Dependiente:** Auditoría Informática

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Enfoque

La presente investigación se encuentra enmarcada dentro del enfoque mixto, el mismo que de acuerdo con Hernández, Fernández, & Baptista (2006, pág. 755) consiste en “un proceso que recolecta analiza y vincula datos cuantitativos y cualitativos en un mismo estudio o una serie de investigaciones para responder a un planteamiento del problema”.

En efecto, el estudio se desarrolla mediante la combinación de los enfoques cuantitativo y cualitativo, puesto que de esta forma se logra una perspectiva más precisa del problema; tal como lo señalan Hernández, Fernández, & Baptista (2006, 756) al expresar que: “El enfoque mixto es igual a mayor amplitud, profundidad, diversidad, riqueza interpretativa y sentido de entendimiento”.

Bajo esta premisa, la investigación emplea un enfoque predominantemente cualitativo por cuanto su propósito principal consiste en analizar la problemática tal y como la perciben los actores involucrados en su contexto (enfoque cualitativo) mediante la utilización de instrumentos cuantitativos de medición y técnicas de análisis estadístico como el método denominado t student.

3.2. Modalidades Básicas de la Investigación

Las modalidades para la presente investigación son las siguientes:

Investigación de campo

De acuerdo con Elizondo (2002, 23), la investigación de campo o directa “es la que se efectúa en el lugar y tiempo en que ocurren los fenómenos objetos de estudio”; en otras palabras, es aquella que implica el contacto directo del investigador con los sujetos involucrados a fin de obtener información relevante sobre la problemática.

En este caso, se ha interactuado con el sector cooperativo de la ciudad de Ambato, así como con su ente regulador para la obtención de información.

Investigación Documental

Para Bernal (2006, 110) la investigación documental “consiste en un análisis de la información escrita sobre determinado tema con el propósito de establecer relaciones, diferencias, posturas o estado actual del conocimiento respecto al tema objeto de estudio”, por lo tanto, el objetivo de este trabajo de investigación radica fundamentalmente en la recopilación de las fuentes de información que puedan aportar datos trascendentales para el proyecto.

3.3. Nivel o tipo de Investigación

Teniendo como criterio la forma y el momento en que será analizado el problema, la presente investigación comprende varios niveles:

Investigación Exploratoria

Este tipo de investigación ha sido la primera en aplicarse dado que, como manifiesta Llopis (2004, pág. 40): “La investigación exploratoria es aquella en la que se intenta obtener una familiarización con un tema del que se

tiene conocimiento general, para plantear posteriores investigaciones u obtener hipótesis”

En efecto, dentro de este nivel se ha procedido a examinar el problema mediante el análisis de la bibliografía existente.

3.4. Población y muestra

3.4.1. Población

La población para la presente investigación será todo el sector cooperativo perteneciente al segmento 1 de la ciudad de Ambato, de acuerdo al siguiente detalle:

TABLA 3.1. POBLACIÓN

| RUC | RAZÓN SOCIAL |
|---------------|--|
| 1890001323001 | COOPERATIVA DE AHORRO Y CREDITO OSCUS LTDA |
| 1890003628001 | COOPERATIVA DE AHORRO Y CREDITO SAN FRANCISCO LTDA |
| 1890141877001 | COOPERATIVA DE AHORRO Y CREDITO MUSHUC RUNA LTDA |
| 1890037646001 | COOPERATIVA DE AHORRO Y CREDITO EL SAGRARIO LTDA |
| 1890080967001 | COOPERATIVA DE AHORRO Y CREDITO CAMARA DE COMERCIO DE AMBATO LTDA. |

Elaborado por: Pilamunga, Alfonso (2017)

Fuente: Superintendencia de Economía Popular y Solidaria (2015)

3.4.2. Muestra:

Para el presente trabajo de investigación no existe muestra, pues, se tomará en cuenta y se trabajará con toda la población, es decir, con todas las cooperativas de ahorro y crédito pertenecientes al segmento 1 de la ciudad de Ambato.

3.5. Operacionalización de las variables

3.5.1. Contextualización Variable Independiente

TABLA. 3.2. ADMINISTRACIÓN DE RIESGOS

| CONCEPTUALIZACIÓN | CATEGORÍAS | INDICADORES | ITEMS | TÉCNICAS DE RECOLECCIÓN |
|--|-------------------|---|--|-----------------------------------|
| Proceso mediante el cual las entidades pertenecientes a la Economía Popular y Solidaria identifican, miden, priorizan, controlan, mitigan, monitorean y comunican los riesgos a los cuales se encuentran expuestas debido al desarrollo tecnológico. | PED | Número total de cooperativas que utilizan PED / Número total de cooperativas | ¿En la Cooperativa se utiliza el procesamiento Electrónico de Datos (PED) a través del computador? | CUESTIONARIO ANEXO 1 |
| | AI | Número total de auditores que tienen conocimiento del entorno / Número total de auditores | ¿Usted conoce los productos y servicios que brinda la Cooperativa? | CUESTIONARIO ANEXO 1 |
| | SIC | Número total de cooperativas que utilizan SIC / Número total de cooperativas | ¿Los Sistemas de Información Computarizada (SIC) de la Cooperativa tienen licencias? | CUESTIONARIO ANEXO 1 |
| | Riesgo Operativo | Número total de cooperativas que utilizan aplican procedimientos adecuados / Número total de cooperativas | ¿Los procedimientos para la administración de los riesgos operativos con respecto a la utilización de las tecnologías de la información y comunicación en la Cooperativa son los adecuados? ¿Cuáles son los principales Riesgos Operativos en la cooperativa? | CUESTIONARIO FICHA DE OBSERVACIÓN |
| | Riesgo Legal | Número total de cooperativas que conocen normativa / Número total de cooperativas | ¿Existe normativa que regule los riesgos operativos referentes a las tecnologías de la información y comunicación? | CUESTIONARIO ANEXO 1 |
| | Niveles de riesgo | Número total de cooperativas que conocen riesgos / Número total de cooperativas | ¿Conoce los niveles de riesgos que existen según la SEPS? | CUESTIONARIO ANEXO 1 |

Elaborado por: Pilamunga, Alfonso (2017)

Fuente: Elaboración propia (2017)

3.5.2. Contextualización Variable Dependiente

TABLA 3.3. AUDITORÍA INFORMÁTICA

| CONCEPTUALIZACIÓN | CATEGORÍAS | INDICADORES | ITEMS | TÉCNICAS DE RECOLECCIÓN |
|---|---|--|---|-------------------------|
| Es la revisión y evaluación de los controles, sistemas y procedimientos de la Tecnología de Información, sus recursos, utilización eficiencia y seguridad para lograr los objetivos del negocio | Planificación | Número total de cooperativas que tienen unidad de auditoría informática / Número total de cooperativas | ¿La cooperativa tiene una unidad o departamento responsable de las Auditorías Informáticas? | CUESTIONARIO ANEXO 1 |
| | Ejecución | Número total de auditores que tienen conocimiento de informática / Número total de auditores | ¿El auditor de la Cooperativa tiene conocimiento técnico de informática? | CUESTIONARIO ANEXO 1 |
| | Reporte | Número total de cooperativas que señalan importancia / Número total de cooperativas | ¿Cree usted que es importante la realización de Auditorías informáticas en las Cooperativas? | CUESTIONARIO ANEXO 1 |
| | Monitoreo y control | Número total de cooperativas que mantienen procedimientos / Número total de cooperativas | ¿Existe procedimientos para mitigar los riesgos Operativos con respecto a las Tecnologías de la información y comunicación? | CUESTIONARIO ANEXO 1 |
| | Auditorías de aplicaciones informáticas | Número total de socios que señalan confiabilidad / Número total de socios | ¿Usted cree que las aplicaciones informáticas que tiene su cooperativa son confiables? | CUESTIONARIO ANEXO 2 |
| | Auditorías de medios de pago | Número total de socios que señalan confiabilidad / Número total de socios | ¿Cree usted que es confiable tener medios de pago a través de las tecnologías de la información y comunicación en las Cooperativas? | CUESTIONARIO ANEXO 2 |

Elaborado por: Pilamunga, Alfonso (2017)

Fuente: Elaboración propia (2017)

3.6. RECOLECCIÓN DE INFORMACIÓN

En éste proceso de investigación se encontraron datos que ayudarán a que exista mayor enlace con el trabajo de campo para generar resultados mediante la agrupación, la ordenación y su respectivo análisis. La recolección de información se dará mediante el apoyo de un plan el mismo que contiene preguntas esenciales para el progreso de la investigación, así como también por fichas de observación a las cooperativas.

Plan de Recolección de Información.

TABLA 3.4. RECOLECCIÓN DE LA INFORMACIÓN

| PREGUNTAS BÁSICAS | EXPLICACIÓN |
|------------------------------------|---|
| ¿Para qué? | Para mejorar los controles de los Riesgos Operativos. |
| ¿De qué personas u objetos? | Los elementos que han servido como fuente de recolección de datos e información es la Superintendencia de Economía Popular y Solidaria. |
| ¿Sobre qué aspectos? | La recolección de datos estuvo orientada a descubrir la influencia de Administración de Riesgos y las Auditoría Informáticas. |
| ¿Quién o quiénes? | El responsable de valorar las actividades del plan estará a cargo del investigador, Alfonso Pilamunga |
| ¿A quiénes? | El Sector Cooperativo, Segmento 1. |
| ¿Dónde? | En la ciudad de Ambato |

| | |
|---|--|
| ¿Cuándo? | El desarrollo del trabajo de campo se realizará durante el segundo semestre del año 2017. |
| ¿Cuántas veces? | La técnica de recolección de información será aplicada por una sola vez. |
| ¿Cómo? | La técnica principal utilizada para obtener información será la encuesta. |
| ¿Con qué? | El instrumento que se utilizó en la investigación consiste es un cuestionario previamente estructurado, el cual contiene exclusivamente preguntas cerradas a fin de que los encuestados se sujeten a las posibilidades de respuesta preestablecidas. |
| ¿Cómo evaluar? | La evaluación de la Administración de los Riesgos se realizará durante y después del período de implementación de las actividades encaminadas a la creación de la unidad de Auditoría Informática para los sistemas de información. |
| ¿Qué recursos se aplican para evaluar? | Encuestas |

Elaborado por: Pilamunga, Alfonso (2017)

Fuente: Elaboración propia (2017)

3.7. Procesamiento y Análisis

Plan de procesamiento de la información

Una vez recogida la información a través de las preguntas de las encuestas realizadas se comenzará una previa tabulación utilizando el programa de Excel para la elaboración de los gráficos y así determinar las respectivas estadísticas que servirán de base fundamental para el profundo análisis e interpretación de los datos obtenidos.

Pasos:

- 1) Recopilar datos.
- 2) Definir las variables para obtener los datos.
- 3) Definir las herramientas estadísticas.
- 4) Activar el programa de computadora, elaboración de tablas de ingreso de datos, realizar cálculos.
- 5) Verificar los datos y resultados.
- 6) Representación gráfica y su interpretación correspondiente.
- 7) Imprimir resultados.

3.8. Análisis e interpretación de resultados

El análisis e interpretación de resultados se dará de acuerdo a los porcentajes obtenidos con los valores señalados tanto en los cuadros como en los gráficos, es decir dando a conocer lo que se ha obtenido luego de las respuestas recibidas de cada pregunta formulada en las encuestas y comparándolas, partiendo sobretodo del plan de procesamiento de información recogida.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1. Análisis e interpretación de resultados

La presente etapa de análisis e interpretación de resultados comienza luego de haber concluido la recolección de información. Por una parte se ha identificado los riesgos operativos a través de fichas de observación y por otra parte se presentan los resultados de la aplicación de las encuestas, para este punto, se ha aplicado encuestas a los auditores, gerentes y personal de tecnologías de la información de las cooperativas de ahorro y crédito que conforman el segmento 1 de la ciudad de Ambato.

Para el procesamiento de los datos recolectado de las encuestas se utilizó Microsoft Excel, así como también para la tabulación de los mismos, ya que este programa nos ayuda a contabilizar los resultados y graficarlos en los gráficos circulares (pastel) automáticamente, obteniendo así una información más precisa.

Cada resultado de las preguntas de la encuesta contendrá el enunciado de la pregunta, la tabla con la información obtenida, el gráfico correspondiente y luego el análisis y la interpretación de los resultados.

Los resultados son los siguientes:

CON RESPECTO A LA OBSERVACIÓN

Luego de haber realizado visitas a las diferentes cooperativas de Ahorro y Crédito que conforman el segmento 1 de la ciudad de Ambato, y a través

de fichas de observación se ha podido identificar los principales Riesgos Operativos, los mismos que se detallan a continuación:

- 1. Incidencia en el negocio y fallos en los sistemas**
- 2. Ejecución, entrega y gestión de procesos**
- 3. Fraude externo**

Cada punto detallado con sus respectivos tipos de eventos que podrían ocurrir y presentar riesgo Operativo, de acuerdo al siguiente detalle:

1. Incidencia en el negocio y fallos en los sistemas

- a. Problemas en el cajero automático
- b. Problemas con la impresora
- c. Problemas con el computador
- d. Problemas con la conexión de red
- e. Error o falta de parametrización
- f. Incompatibilidad de funciones
- g. Acceso a funcionalidades no acorde con el perfil sin intención de causar daño
- h. Error en los reportes
- i. Descuadre de cuentas

2. Ejecución, entrega y gestión de procesos

- a. Ejecución, entrega y gestión de procesos
- b. Documentos no legalizados
- c. Incorrecta e inoportuna ejecución de las actividades
- d. Desarrollar actividades fuera del tiempo establecido
- e. Problemas con el enlace de comunicación
- f. Incorrecto e inoportuno registro de las actividades
- g. Faltantes y sobrantes

3. Fraude externo

- a. Falsificación de información o intento de ingresos a los sistemas por terceros

Los Riesgos mencionados, son la recopilación de todas las observaciones realizadas en la Cooperativas de ahorro y crédito segmento 1, de la ciudad de Ambato, por lo que, con dicho procedimiento se ha identificado los Riesgos Operativos a los que están expuestos el sector financiero.

CON RESPECTO A LAS ENCUESTAS APLICADA A LOS AUDITORES, GERENTES Y PERSONAL DE TECNOLOGÍAS DE LA INFORMACIÓN DE LAS COOPERATIVAS DE AHORRO Y CRÉDITO SEGMENTO 1, DE LA CIUDAD DE AMBATO

Se ha aplicado las encuestas aplicada a los auditores, gerentes y personal de tecnologías de la información de las cooperativas de ahorro y crédito segmento 1, de la ciudad de Ambato, la misma que contenía las siguientes preguntas.

1. ¿Usted conoce los productos y servicios que brinda la Cooperativa?

TABLA 4.1. PRODUCTOS Y SERVICIOS

| ALTERNATIVA | FRECUENCIA | RELEVANCIA |
|--------------|------------|------------|
| SI | 15 | 100.00% |
| NO | 0 | 0.00% |
| TOTAL | 15 | 100.00% |

Elaborado por: Pilamunga, Alfonso (2018)

Fuente: Encuesta 1 (2018)

GRÁFICO 4.1. PRODUCTOS Y SERVICIOS



Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

Análisis: Del total de la población encuestada, el 100% manifiesta que conocen los productos y servicios que brinda la cooperativa.

Interpretación: Los resultados encontrados demuestran que todos los auditores encuestados conocen su entorno, referente a los productos y servicios que brinda la cooperativa.

2. ¿En la Cooperativa se utiliza el procesamiento Electrónico de Datos (PED) a través del computador?

TABLA 4.2. PED

| ALTERNATIVA | FRECUENCIA | RELEVANCIA |
|--------------|------------|------------|
| SI | 15 | 100.00% |
| NO | 0 | 0.00% |
| TOTAL | 15 | 100.00% |

Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

GRÁFICO 4.2. PED



Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

Análisis: El total de la población encuestada, es decir, el 100% considera que se utiliza el procesamiento electrónico de datos (PED) a través del computador.

Interpretación: De los resultados encontrados se demuestran que con el avance de la tecnología, todas las cooperativas utilizan éstos medios para brindar productos y servicios financieros.

3. ¿La Cooperativa utiliza los Sistemas de Información Computarizada (SIC)?

TABLA 4.3. SIC

| ALTERNATIVA | FRECUENCIA | RELEVANCIA |
|--------------|------------|------------|
| SI | 15 | 100.00% |
| NO | 0 | 0.00% |
| TOTAL | 15 | 100.00% |

Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

GRÁFICO 4.3. SIC



Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

Análisis: Del total de la población encuestada, el 100% manifiesta que en la cooperativa se utiliza sistemas de información computarizada (SIC).

Interpretación: Los resultados encontrados demuestran que en la actualidad para no realizar trabajos repetitivos y manuales, ya se ocupan los sistemas de información computarizada para ahorro de tiempo y exactitud de cálculo.

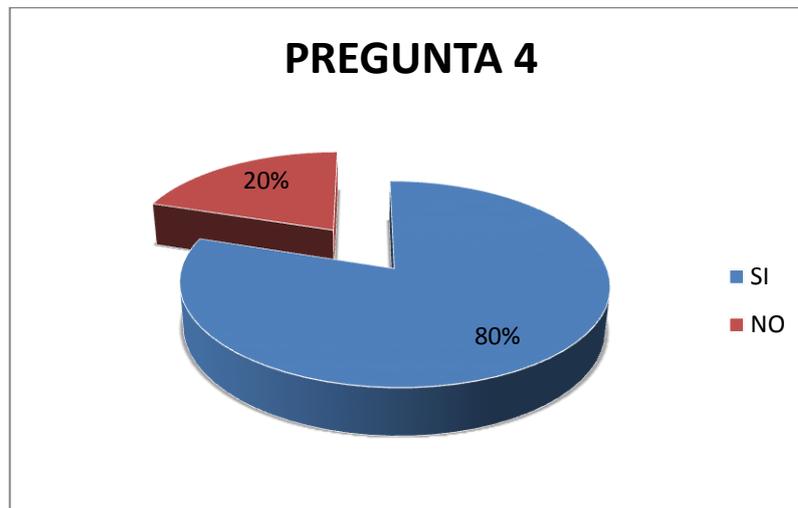
4. ¿Los Sistemas de Información Computarizada (SIC) de la Cooperativa tienen licencias?

TABLA 4.4. LICENCIAS SIC

| ALTERNATIVA | FRECUENCIA | RELEVANCIA |
|--------------|------------|------------|
| SI | 12 | 80.00% |
| NO | 3 | 20.00% |
| TOTAL | 15 | 100.00% |

Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

GRÁFICO 4.5. LICENCIAS SIC



Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

Análisis: Del total de la población encuestada, el 80% considera que los sistemas de información computarizado que mantiene la cooperativa poseen licencias, mientras que el restante, es decir, el 20% considera de no se posee licencias.

Interpretación: Los resultados encontrados demuestran que en algunos casos en la utilización de sistemas de información computarizada se estaría recayendo en la ilegalidad por falta de licencias, lo que podría acarrear demandas, pérdidas de información por falta de funcionamiento, no existe garantía del proveedor en el caso de falla de funcionamiento o recuperación de información.

5. ¿El auditor de la Cooperativa tiene conocimiento técnico de informática?

TABLA 4.5. CONOCIMIENTO INFORMÁTICA

| ALTERNATIVA | FRECUENCIA | RELEVANCIA |
|--------------|------------|------------|
| SI | 15 | 100.00% |
| NO | 0 | 0.00% |
| TOTAL | 15 | 100.00% |

Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

GRÁFICO 4.5. CONOCIMIENTO INFORMÁTICO



Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

Análisis: El total de la población, es decir, el 100% considera tener los conocimientos técnicos de informática.

Interpretación: Los resultados encontrados demuestran que los auditores poseen el conocimiento técnico de informática, lo que conllevaría que al momento de aplicar una auditoría informática el riesgo de detección será menor, por todos estos conocimientos adquiridos por la experiencia en estas funciones.

6. ¿La Cooperativa ha identificado los riesgos operativos con claridad?

TABLA 4.6. RIESGOS CLAROS

| ALTERNATIVA | FRECUENCIA | RELEVANCIA |
|--------------|------------|----------------|
| SI | 12 | 80.00% |
| NO | 3 | 20.00% |
| TOTAL | 15 | 100.00% |

Elaborado por: Pilamunga, Alfonso (2018)

Fuente: Encuesta 1 (2018)

GRÁFICO 4.6. RIESGOS CLAROS



Elaborado por: Pilamunga, Alfonso (2018)

Fuente: Encuesta 1 (2018)

Análisis: Del total de la población, el 80% considera que se han establecido con claridad los riesgos operativos, mientras que el restante, es decir, el 20% considera que no se ha establecido con claridad los riesgos operativos.

Interpretación: Los resultados encontrados demuestran que no todo el personal auditor de las cooperativas establecen con claridad los riesgos operativos, esto, a consecuencia de no haber una normativa legal que obligue a establecer y dar tratamiento a los riesgos operativos.

7. ¿Se aplica Administración de Riesgos Operativos con respecto a las tecnologías de la información y comunicación en la cooperativa?

TABLA 4.7. ADMINISTRACIÓN DE RIESGOS

| ALTERNATIVA | FRECUENCIA | RELEVANCIA |
|--------------|------------|----------------|
| SI | 15 | 100.00% |
| NO | 0 | 0.00% |
| TOTAL | 15 | 100.00% |

Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

GRÁFICO 4.7. ADMINISTRACIÓN DE RIESGOS



Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

Análisis: El total de la población encuestada, el 100% considera que si se aplica Administración de Riesgos Operativos con respecto a las tecnologías de la información y comunicación en la cooperativa.

Interpretación: Los resultados encontrados demuestran que se aplica administración de riesgos operativos con respecto a las tecnologías de la información y comunicación, pero esto, por realizar buenas prácticas empresariales, más no por obligatoriedad de un organismo de control.

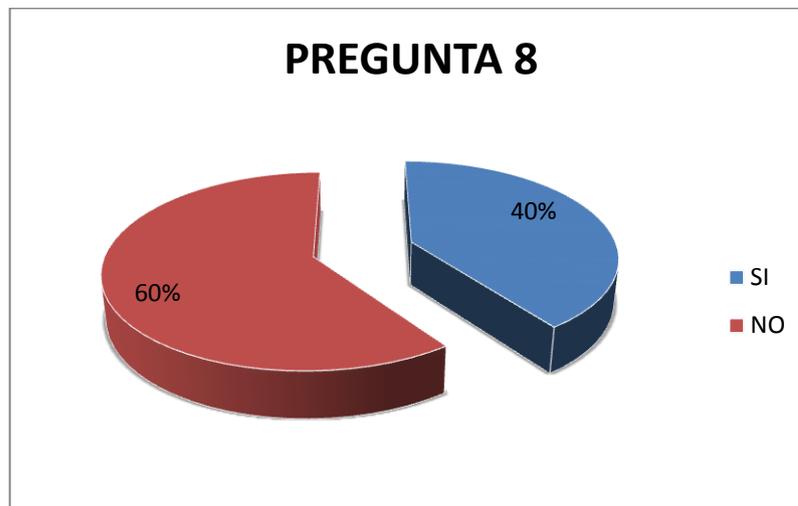
8. ¿Existe procedimientos para mitigar los riesgos Operativos con respecto a las Tecnologías de la información y comunicación?

TABLA 4.8. MITIGACIÓN DE RIESGOS

| ALTERNATIVA | FRECUENCIA | RELEVANCIA |
|--------------|------------|----------------|
| SI | 6 | 40.00% |
| NO | 9 | 60.00% |
| TOTAL | 15 | 100.00% |

Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

GRÁFICO 4.8. MITIGACIÓN DE RIESGOS



Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

Análisis: Del total de la población encuestada, el 60% considera que no existen procedimientos para mitigar los riesgos Operativos con respecto a las Tecnologías de la información y comunicación, mientras que el restante, es decir, el 40% considera de si existen procedimientos.

Interpretación: Los resultados encontrados demuestran que la falta de procedimiento y directrices por parte de organismos de control con respecto a los riesgos operativos es preocupante, ya que, al no ser una

exigencia, las cooperativas lo podrían realizar o no, poniendo en riesgo dinero de los socios pertenecientes a éstas cooperativas.

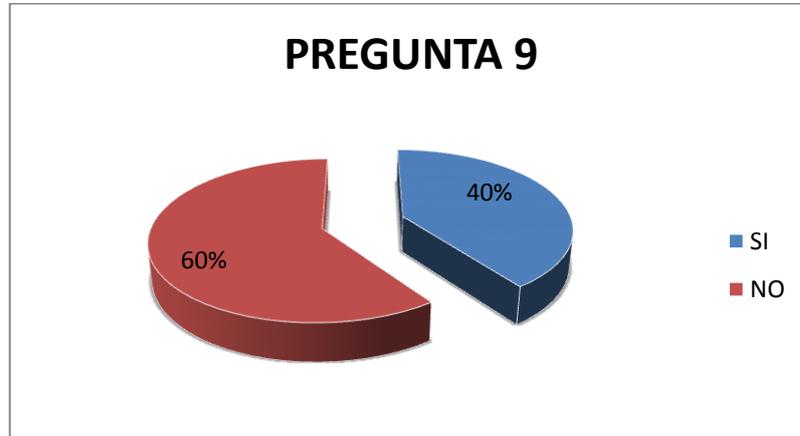
9. ¿Los procedimientos para la administración de los riesgos operativos con respecto a la utilización de las tecnologías de la información y comunicación en la Cooperativa son los adecuados?

TABLA 4.9. PROCEDIMIENTOS - ADMINISTRACIÓN DE RIESGOS

| ALTERNATIVA | FRECUENCIA | RELEVANCIA |
|--------------|------------|------------|
| SI | 6 | 40.00% |
| NO | 9 | 60.00% |
| TOTAL | 15 | 100.00% |

Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

GRÁFICO 4.9. PROCEDIMIENTOS - RIESGOS



Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

Análisis: Del total de la población encuestada, el 60% considera que no son adecuados los procedimientos para la administración de los riesgos operativos con respecto a la utilización de las tecnologías de la información y comunicación en la Cooperativa, mientras que el restante, es decir el 40% considera de si lo son.

Interpretación: Los resultados encontrados demuestran que la mayoría, manifiesta que no son adecuados los procedimientos para la administración de riesgos operativos, esto, por cuanto no existe normativa alguna que regule u obligue a las cooperativas sobre este aspecto.

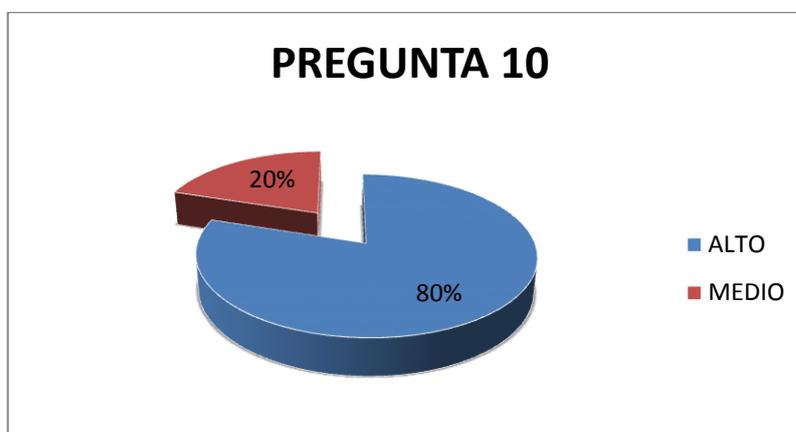
10. ¿Califique la importancia de la Administración de Riesgos Operativos con respecto a las tecnologías de la información y comunicación en las Cooperativas?

TABLA 4.10. IMPORTANCIA ADMINISTRACIÓN DE RIESGOS

| ALTERNATIVA | FRECUENCIA | RELEVANCIA |
|--------------|------------|----------------|
| ALTO | 12 | 80.00% |
| MEDIO | 3 | 20.00% |
| BAJO | 0 | 0.00% |
| TOTAL | 15 | 100.00% |

Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

GRÁFICO 4.10. IMPORTANCIA ADMINSITRACIÓN DE RIESGOS



Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

Análisis: Del total de la población encuestada, el 80% considera que es de alta importancia la Administración de Riesgos Operativos con respecto a las tecnologías de la información y comunicación en las Cooperativas, mientras que el restante, es decir, el 20% considera que tiene importancia

media, y pues ninguna persona contesta que tiene importancia baja, por lo que se le atribuye el 0%.

Interpretación: Los resultados encontrados demuestran que es de gran importancia el tratamiento de la Administración de Riesgos Operativos, por tal razón, esto se lo podría llevar a cabo mediante normativa legal.

11. ¿Existe normativa que regule los riesgos operativos referentes a las tecnologías de la información y comunicación?

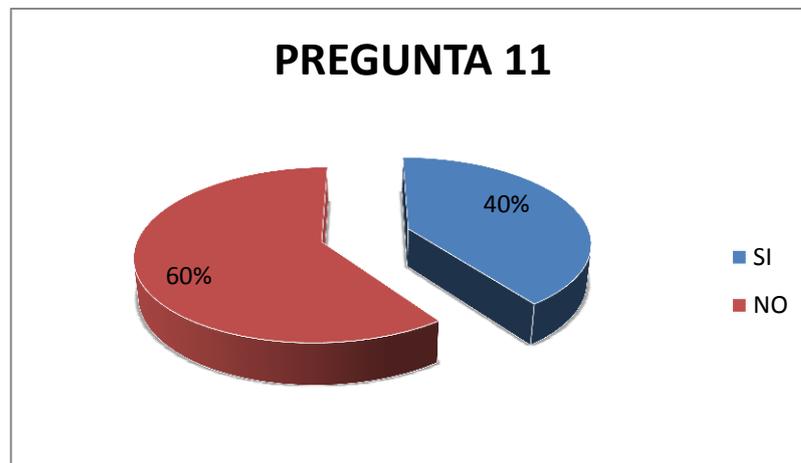
TABLA 4.11. NORMATIVA

| ALTERNATIVA | FRECUENCIA | RELEVANCIA |
|--------------|------------|----------------|
| SI | 6 | 40.00% |
| NO | 9 | 60.00% |
| TOTAL | 15 | 100.00% |

Elaborado por: Pilamunga, Alfonso (2018)

Fuente: Encuesta 1 (2018)

GRÁFICO 4.11. NORMATIVA



Elaborado por: Pilamunga, Alfonso (2018)

Fuente: Encuesta 1 (2018)

Análisis: Del total de la población encuestada, el 60% considera que no existe normativa que regule los riesgos operativos referentes a las

tecnologías de la información y comunicación, mientras que el restante, es decir, el 40% considera de si la existe.

Interpretación: Los resultados encontrados demuestran que la mayoría de los encuestados no conocen sobre normativa específica para riesgos operativos, los que manifiestan conocer sobre normativa, es por una norma en general, más no por mantener normativa específica para el tema, por lo que es importante que el ente de control se pronuncie con respecto a éste tema de interés común.

12. ¿La cooperativa tiene una unidad o departamento responsable de las Auditorías Informáticas?

TABLA 4.12. UNIDAD DE AUDITORÍA INFORMÁTICA

| ALTERNATIVA | FRECUENCIA | RELEVANCIA |
|--------------|------------|----------------|
| SI | 0 | 0.00% |
| NO | 15 | 100.00% |
| TOTAL | 15 | 100.00% |

Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

GRÁFICO 4.12. UNIDAD DE AUDITORÍA INFORMÁTICA



Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

Análisis: El total de la población, es decir el 100% manifiesta que la cooperativa a la que pertenece no tiene una unidad o departamento responsable de las Auditorías Informáticas.

Interpretación: Los resultados encontrados demuestran que las cooperativas del segmento 1 de la ciudad de Ambato no mantienen una unidad o departamento responsable de las Auditorías Informáticas, lo que hace entender, que no existe responsable sobre la valoración, seguimiento y control en temas informáticos.

13. ¿Cree usted que es importante la realización de Auditorías informáticas en las Cooperativas?

TABLA 4.13. AUDITORIAS INFORMÁTICAS

| ALTERNATIVA | FRECUENCIA | RELEVANCIA |
|--------------|------------|------------|
| SI | 15 | 100.00% |
| NO | 0 | 0.00% |
| TOTAL | 15 | 100.00% |

Elaborado por: Pilamunga, Alfonso (2017)

Fuente: Encuesta 1 (2017)

GRÁFICO 4.13. AUDITORÍAS INFORMÁTICA



Elaborado por: Pilamunga, Alfonso (2018)

Fuente: Encuesta 1 (2018)

Análisis: El total de la población encuestada, es decir el 100% considera que sí es importante la realización de Auditorías informáticas en las Cooperativas.

Interpretación: Los resultados encontrados demuestran que es de gran importancia que se desarrollen auditorías informáticas en las cooperativas, de esta manera detectar los riesgos a los que pueden estar expuestos, y por ende, tomar acciones para poderlos mitigar.

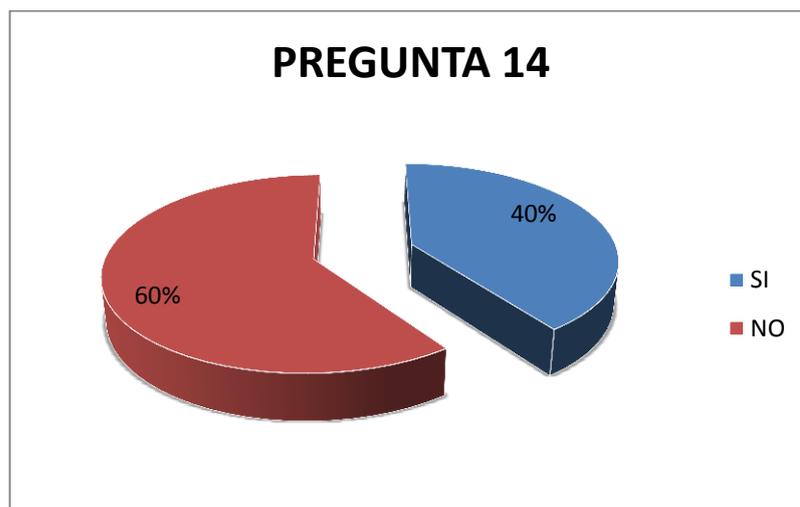
14. ¿En la cooperativa se han realizado auditorías a los sistemas de información y comunicación?

TABLA 4.14. SISTEMAS DE INFORMACIÓN

| ALTERNATIVA | FRECUENCIA | RELEVANCIA |
|--------------|------------|----------------|
| SI | 6 | 40.00% |
| NO | 9 | 60.00% |
| TOTAL | 15 | 100.00% |

Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

GRÁFICO 4.14. SISTEMAS DE INFORMACIÓN



Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

Análisis: Del total de la población, el 60% manifiesta que en la cooperativa no se han realizado auditorías a los sistemas de información y comunicación, mientras que el restante, es decir, el 40% considera de si se han realizados dichas auditorías.

Interpretación: Los resultados encontrados demuestran que es importante normar la frecuencia con la cual se deberá desarrollar las auditorías informáticas en las cooperativas, ya que, al no estar normado, se las puede realizar o no dependiendo de las cooperativas, su personal y su recurso.

15. ¿Se han detectado intentos de accesos no autorizados o de terceras personas a los sistemas de la cooperativa?

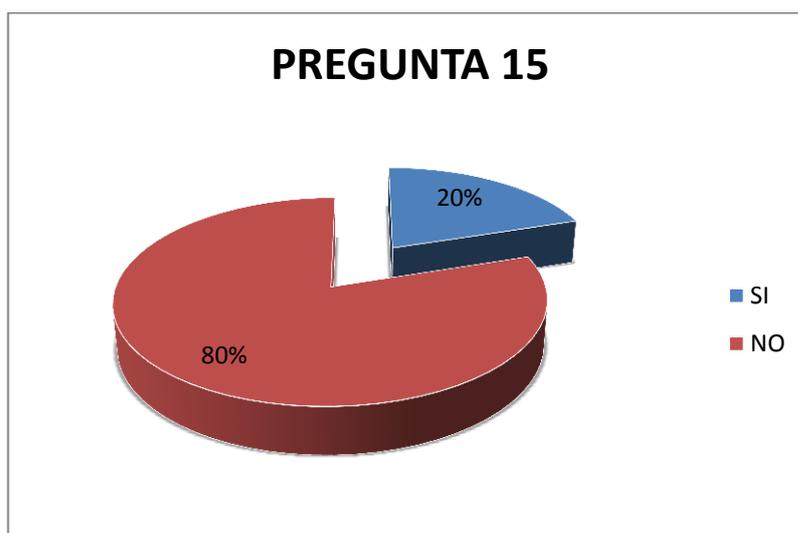
TABLA 4.15. ACCESOS NO AUTORIZADOS

| ALTERNATIVA | FRECUENCIA | RELEVANCIA |
|--------------|------------|----------------|
| SI | 3 | 20.00% |
| NO | 12 | 80.00% |
| TOTAL | 15 | 100.00% |

Elaborado por: Pilamunga, Alfonso (2018)

Fuente: Encuesta 1 (2018)

GRÁFICO 4.15. ACCESOS NO AUTORIZADOS



Elaborado por: Pilamunga, Alfonso (2018)

Fuente: Encuesta 1 (2018)

Análisis: Del total de la población, el 80% considera que no se han detectado intentos de accesos no autorizados o de terceras personas a los sistemas de la cooperativa, mientras que el restante, es decir, el 20% considera de si se han detectado intentos de accesos no autorizados o de terceras personas a los sistemas de la cooperativa.

Interpretación: Los resultados encontrados demuestran que la mayoría no ha detectado intentos de accesos no autorizados o de terceras personas a los sistemas de la cooperativa, es puede ser, por no haber intentos, o por no tener un sistema o procedimiento adecuado para la detección de accesos no autorizados como seguridad informática.

16. ¿Conoce los niveles de riesgos que existe según la SEPS?

TABLA 4.16. RIESGOS SEPS

| ALTERNATIVA | FRECUENCIA | RELEVANCIA |
|--------------|------------|------------|
| SI | 15 | 100.00% |
| NO | 0 | 0.00% |
| TOTAL | 15 | 100.00% |

Elaborado por: Pilamunga, Alfonso (2018)

Fuente: Encuesta 1 (2018)

GRÁFICO 4.16. RIESGOS SEPS



Elaborado por: Pilamunga, Alfonso (2018)

Fuente: Encuesta 1 (2018)

Análisis: El total de la población encuestada, es decir, el 100% manifiesta conocer los niveles de riesgos que existen según la SEPS.

Interpretación: Los resultados encontrados demuestran que al estar dentro de una normativa legal los niveles de riesgos por el ente rector es de conocimiento y de aplicación en todas las cooperativas.

17. ¿Existe procedimientos en la Cooperativa para mitigar los riesgos?

TABLA 4.17. MITIGACIÓN

| ALTERNATIVA | FRECUENCIA | RELEVANCIA |
|--------------|------------|----------------|
| SI | 15 | 100.00% |
| NO | 0 | 0.00% |
| TOTAL | 15 | 100.00% |

Elaborado por: Pilamunga, Alfonso (2018)

Fuente: Encuesta 1 (2018)

GRÁFICO 4.17. MITIGACIÓN



Elaborado por: Pilamunga, Alfonso (2018)

Fuente: Encuesta 1 (2018)

Análisis: El total de la población encuestada, es decir, el 100% considera que si existe procedimientos en la Cooperativa para mitigar el nivel alto del riesgo.

Interpretación: Los resultados encontrados demuestran que las cooperativas mantienen procedimiento para mitigar los niveles altos del riesgo en el caso de existir, por lo que, se podría deducir en que las cooperativas tienen la preparación para mitigar los riesgos, por lo que sería menos complicado en el caso de existir riesgo operativos.

18. ¿Cree usted que la Administración de Riesgos Operativos con relación a las Tecnologías de Información y comunicación mejoraría con una Normativa que obligue la creación de una Unidad de Auditoría informática en el Organigrama estructural de las Cooperativas de Ahorro y Crédito segmento 1 de la ciudad de Ambato?

TABLA 4.18. ORGANIGRAMA

| ALTERNATIVA | FRECUENCIA | RELEVANCIA |
|--------------|------------|------------|
| SI | 15 | 100.00% |
| NO | 0 | 0.00% |
| TOTAL | 15 | 100.00% |

Elaborado por: Pilamunga, Alfonso (2018)

Fuente: Encuesta 1 (2018)

GRÁFICO 4.18. ORGANIGRAMA



Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta 1 (2018)

Análisis: El total de la población encuestada, es decir, el 100% considera que la Administración de Riesgos Operativos con relación a las Tecnologías de Información y comunicación mejoraría con una Normativa que obligue la creación de una Unidad de Auditoría informática en el Organigrama estructural de las Cooperativas de Ahorro y Crédito segmento 1 de la ciudad de Ambato.

Interpretación: Los resultados encontrados demuestran que es de gran importancia la creación de una unidad de auditoría informática en las cooperativas, los mismos que tendrán responsabilidad sobre todos los sistemas que se utilice la cooperativa.

4.2. Comprobación de hipótesis

- a) **Modelo lógico.**- La hipótesis planteada en nuestro problema de investigación tiene opción a tener un resultado, esto puede ser, Hipótesis Nula e Hipótesis Alternativa, así:

Hipótesis nula

H₀: La Administración de Riesgos NO es un componente relevante en las Auditorías informáticas en el sector cooperativo, Segmento 1 de la Ciudad de Ambato.

Hipótesis alternativa

H₁: La Administración de Riesgos es un componente relevante en las Auditorías informáticas en el sector cooperativo, Segmento 1 de la Ciudad de Ambato.

b) Modelo matemático

$$H_0 = p1 = p2$$

$$H_1 = p1 \neq p2$$

c) Modelo estadístico

$$t = \frac{p1 - p2}{\sqrt{(\hat{p} * \hat{q})\left(\frac{1}{n1} + \frac{1}{n2}\right)}}$$

De donde:

$t =$ Estimador "t", t calculada

$p1 =$ Probabilidad de aciertos de la VI

| | |
|-------------|--|
| $p_2 =$ | Probabilidad de aciertos de la VD |
| $\hat{p} =$ | Probabilidad de éxito conjunta |
| $\hat{q} =$ | Probabilidad de fracaso conjunta (1-p) |
| $n_1 =$ | Número de casos de la VI |
| $n_2 =$ | Número de casos de la VD |

Para la verificación de la hipótesis se trabajará con un nivel de confianza del 95%, por lo tanto con un margen de error del 5%, por lo que la significancia es:

$$\alpha = 1 - \text{confianza}$$

$$\alpha = 1 - 0.95$$

$$\alpha = 0.05$$

Luego se procede al cálculo de los grados de libertad, mismos que son necesarios para saber cuál es el valor de t tabular que le corresponde a la presente investigación, de la siguiente manera:

$$gl = n_1 + n_2 - 2$$

$$gl = 15 + 15 - 2$$

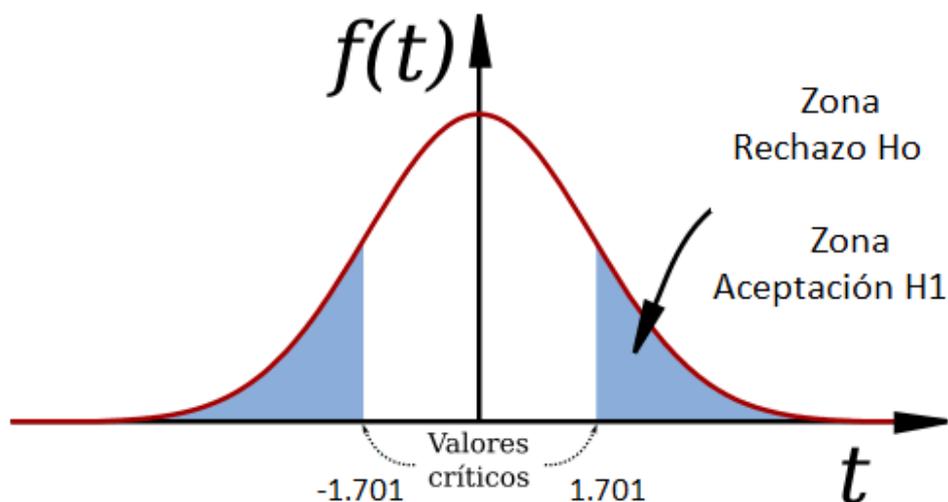
$$gl = 28$$

Por lo que con los grados de libertad y la significancia ya se puede hallar el t tabular, según el ANEXO 3, esto es:

$$t \text{ tabular} = \pm 1.701$$

Por lo que se ACEPTA la Hipótesis Nula (H_0) si t calculada está entre el rango de ± 1.701 con un ensayo bilateral, caso contrario se RECHAZA, y se ACEPTA la Hipótesis Alternativa (H_1)

GRÁFICO 4.25. T STUDENT



Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Tabla T student (2018)

4.3. Cálculo de t student

TABLA 4.19. CÁLCULO T STUDENT

| Variable Independiente | | | |
|---|-------|----|-------------|
| ¿Los procedimientos para la administración de los riesgos operativos con respecto a la utilización de las tecnologías de la información y comunicación en la Cooperativa son los adecuados? | SI | 6 | Acierto |
| | NO | 9 | Desaciertos |
| | TOTAL | 15 | |
| Variable Dependiente | | | |
| ¿Cree usted que es importante la realización de Auditorías informáticas en las Cooperativas? | SI | 15 | Acierto |
| | NO | 0 | Desaciertos |
| | TOTAL | 15 | |

Elaborado por: Pilamunga, Alfonso (2018)
Fuente: Encuesta (2018)

$$p1 = \frac{6}{15}$$

$$p1 = 0,40$$

$$p_2 = \frac{15}{15}$$

$$p_2 = 1$$

$$\hat{p} = \frac{6 + 15}{15 + 15}$$

$$\hat{p} = \frac{21}{30}$$

$$\hat{p} = 0,70$$

$$\hat{q} = 1 - \hat{p}$$

$$\hat{q} = 1 - 0,70$$

$$\hat{q} = 0,30$$

$$t = \frac{p_1 - p_2}{\sqrt{(\hat{p} * \hat{q})\left(\frac{1}{n_1} + \frac{1}{n_2}\right)}}$$

$$t = \frac{0,40 - 1}{\sqrt{(0,70 * 0,30)\left(\frac{1}{15} + \frac{1}{15}\right)}}$$

$$t = \frac{-0,60}{\sqrt{(0,21)(0,133)}}$$

$$t = \frac{-0,60}{0,0280}$$

$$t = \pm 21,43$$

Conclusión

Aplicando el método estadístico t Student el resultado t calculada es de $\pm 21,43$ valor mayor al t tabular de $\pm 1,86$, por lo que, se RECHAZA la Hipótesis Nula (H_0) y se ACEPTA la Hipótesis Alternativa (H_1), es decir, la Administración de Riesgos es un componente relevante en las Auditorías informáticas en el sector cooperativo, Segmento 1 de la Ciudad de Ambato.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Luego de haber completado el proceso investigativo, las conclusiones que se desprenden son las siguientes:

- El sector cooperativo, en nuestra materia de estudio, el segmento 1 de la ciudad de Ambato, en alguno de los casos efectúan procedimiento para la administración de los riesgos operativos con respecto a la utilización de las tecnologías de la información y comunicación, sin embargo éstos son generales, no específicos, lo que dificulta a las entidades detectar a tiempo los puntos críticos en todos los sistemas de información y comunicación, situación que se da, por no mantener una normativa emitida por el ente de control, esto es, la Superintendencia de Economía Popular y Solidaria.
- Se atribuye de gran interés para el sector cooperativo segmento 1 de la ciudad de Ambato, el desarrollo de auditorías informáticas, para prevenir los diferentes tipos de eventos relacionados con el riesgo operativo a los que pueden estar expuestos, esto mediante la verificación de la hipótesis del Capítulo IV, por ende, a través de éstas se puede tomar acciones para poder mitigarlos.
- De acuerdo al desarrollo del presente trabajo de investigación, se deduce que para el sector cooperativo, segmento 1 de la ciudad de Ambato, una alternativa de solución para mejorar la Administración de Riesgos Operativos con relación a las Tecnologías de Información y comunicación es una Normativa que obligue la

creación de una Unidad de Auditoría informática en el Organigrama estructural de las Cooperativas de Ahorro y Crédito.

5.2. RECOMENDACIONES

Como recomendaciones para el presente trabajo investigativo son las siguientes:

- Diseñar y verificar la aplicación de normas de control por parte de la Superintendencia de Economía Popular y Solidaria, para la administración de los riesgos operativos con respecto a la utilización de las tecnologías de la información y comunicación, para que su control sea periódico y obligatorio.
- Desarrollar la metodología para la calificación del Nivel de riesgo que debe ser utilizado en las Auditorías Informáticas para los diferentes tipos de eventos relacionados con el riesgo operativo a los que pueden estar expuestos.
- Elaborar normativa que obligue la creación de una Unidad de Auditoría informática en el Organigrama estructural de las Cooperativas de Ahorro y Crédito segmento 1 de la ciudad de Ambato, para de esta manera el organismo de control dar la responsabilidad de instalación, funcionamiento, procesamiento y seguimiento de todos los sistemas que utilizan tecnologías de la información y comunicación al jefe de la unidad.

CAPÍTULO VI

PROPUESTA

6.1. DATOS INFORMATIVOS

Título:

Normativa de obligatoriedad de contar con una Unidad de Auditoría informática en el Organigrama estructural de las Cooperativas de Ahorro y Crédito segmento 1, de la ciudad de Ambato, para el fortalecimiento de la Administración de Riesgos Operativos de los Sistemas de Información y comunicación.

Institución ejecutora:

Cooperativas de Ahorro y Crédito segmento 1, de la ciudad de Ambato.

Beneficiarios:

Cooperativas de Ahorro y Crédito segmento 1 a nivel nacional, socios de dichas cooperativas.

Ubicación:

Provincia: Tungurahua

Cantón: Ambato

Sector: Cooperativo, segmento 1.

Tiempo estimado: Enero – Mayo 2018

Equipo técnico: Estudiante
Tutor

Costo: 1.212 dólares

6.2. ANTECEDENTES

El sector Cooperativo, segmento 1 de la ciudad de Ambato, a través de la verificación de la hipótesis se ha llegado a la conclusión de que dicho sector necesita mejorar en el área informática, a través de normas de control para la administración de riesgos operativos, esto con respecto a la utilización de las tecnologías de información y comunicación, para lo cual se diseñará y verificará la aplicación de normas de control emitidas por la superintendencia de economía popular y solidaria.

Además, debido al gran interés del sector cooperativo por tener como política de control las auditorías informáticas, se desarrollará normativa legal, en la que conste como política de control las auditorías informáticas, esto con la finalidad de detectar los riesgos a los que pueden estar expuestos, de esta manera conocerlos, verificarlos y tomar medidas para mitigarlos o prevenirlos.

En avance de la tecnología a nivel mundial y en el Ecuador ha sido muy vertiginoso, por tal razón las cooperativas de ahorro y crédito correspondientes al segmento 1 en la ciudad de Ambato, se encuentran proporcionando servicios financieros que agilitan la vida comercial de las empresas y de las personas, causando así el problema de la mala administración de los Riesgos Operativos con respecto a las tecnologías de la información y comunicación.

En este sentido, al ser relativamente nuevo los servicios financieros que proporcionan las Cooperativas de Ahorro y Crédito el problema planteado se da por la inaplicación de las Normas de Control COBI – ISO 27001, sin la adecuada aplicación, esto puede generar la ocurrencia de los Delitos informáticos, así como la divulgación de documentación confidencial para las cooperativas, lo que no garantiza a sus clientes la confiabilidad de sus datos personales y financieros, de la misma manera, se incurriría en la prestación de servicios financieros inseguros, ya que no se tiene la certeza de que las transacciones realizadas utilizando los sistemas de información puedan ser intersectadas por los Cyber – delincuentes, y ser víctimas de transferencias sin el consentimiento del titular.

Otra causa por la cual se genera el problema, es por la mala Administración de los Riesgos Operativos en cuanto a las tecnologías de la información y comunicación, las mismas que ayudan a los sistemas integrados de información a tener un mejor control interno, a través de la detección de riesgos inherentes con su respectivo tratamiento, pero, al no aplicarlos, ocasionaría que exista fuga de información confidencial, por ende, la divulgación de información, como datos de crédito, valores en las cuentas de ahorro, número de tarjetas, etc., en consecuencia, se tendría un servicio financiero inseguro utilizado por los clientes, llegando así a la ocurrencia de los fraudes o delitos informáticos, y más aún al no contar con una unidad de Auditoría Informática para las Cooperativas de Ahorro y Crédito, esto podría no detectar ciertas irregularidades que se estén presentando en las aplicaciones para brindar servicios financieros.

Con relación a los efectos que la mala Administración de los Riesgos Operativos con respecto de los sistemas de información, en primer plano se encuentra la divulgación de la información confidencial, ya que, con dicha información se puede acceder a cuentas, transferencias bancarias, pagos de servicios de otras personas, etc., y caer así, en los denominados delitos informáticos, ya que los hacker aprovechan la

tecnología para ingresar a datos confidenciales de otras personas y hacer de las suyas, como interferir en las transferencias bancarias, apropiación de claves de acceso, direccionamiento de transferencias, etc.

6.3. JUSTIFICACIÓN

Se considera inminente la necesidad de estandarizar procesos a nivel del sector cooperativo, y por ende establecer lineamientos, directrices a seguir emitido por un órgano de control, que en nuestro caso es la Superintendencia de Economía Popular y Solidaria, ya que en la actualidad se maneja de manera por las buenas prácticas empresarias, es decir, cooperativa que desee revisar, verificar, controlar sus tecnologías de la información y comunicación lo realizan por cuenta propia y de manera empírica, sin ninguna periodicidad, y sin reportar ningún informe al ente de control, los criterios con los que realizan éstas actividades no se encuentran establecidos en ninguna norma del ente de control, es por ello que no solicitan evidencias con características determinadas, los reportes no son puntuales, pertinentes, consistentes, completos y formales, es un mero informe para gerencia, esto en cooperativas que lo aplican, de ahí por otra parte, existen cooperativas que no lo aplican, por no ser un requerimiento del ente de control, es decir, no estarían en la obligatoriedad de realizarlo.

Además, dentro del presente trabajo de investigación, en el capítulo cuatro, se realiza a través de un método estadístico t student la comprobación de la hipótesis planteada, dando como resultado que la Administración de Riesgos es un componente relevante en las Auditorías informáticas en el sector cooperativo, Segmento 1 de la Ciudad de Ambato, por lo tanto, es razón suficiente, como para justificar la presente propuesta, para el mejor desarrollo del sector cooperativo.

6.4. OBJETIVOS

6.4.1. Objetivo general

- Formular normativa de obligatoriedad de contar con una Unidad de Auditoría informática en el Organigrama estructural de las Cooperativas de Ahorro y Crédito segmento 1, de la ciudad de Ambato, para el fortalecimiento de la Administración de Riesgos Operativos.

6.4.2. Objetivos específicos

- Identificar los factores del riesgo operativo para una adecuada administración del riesgo.
- Establecer la metodología de calificación del Nivel de riesgo a ser utilizado en las auditorías informáticas para la valoración de los diferentes tipos de eventos relacionados con el riesgo operativo.

6.5. Análisis de factibilidad

Tecnológico

Para el desarrollo de la presente propuesta, para el mejor desarrollo y evaluación de la administración de riesgos en el sector cooperativo segmento 1 de la ciudad de Ambato, se dispone de los recursos tecnológicos adecuados como: software básicos, computador, internet, navegadores, página web institucional del ente de control y otros; además de los conocimientos necesarios para el manejo de dichos elementos, cumpliéndose con la factibilidad tecnológica.

Organizacional

El sector cooperativo al cual pertenece el presente trabajo investigativo, tiene la necesidad de que exista normativa legal, que regule la administración de riesgos operativos, a través de auditorías informáticas, por lo que, dicha necesidad justifica la realización del presente propuesta.

Económico Financiero

Los recursos económicos necesarios para la elaboración de la presente propuesta se obtendrán en base a autofinanciamiento por parte del autor; además dicho financiamiento es mínimo con relación al beneficio que obtendrán tanto las cooperativas como sus usuarios.

Legal

El desarrollo del presente trabajo de investigación y de su propuesta no contraviene ninguna ley, normativa o disposición legal vigente, y se basa específicamente en las atribuciones y competencia que se manifiesta en la Constitución de la República del Ecuador (Asamblea Nacional, Constitución de la República del Ecuador, 2015), en su Art. 213, que textualmente manifiesta: “Las superintendencias son organismos técnicos **de vigilancia**, auditoría, intervención **y control de las actividades económicas, sociales y ambientales, y de los servicios que prestan las entidades públicas y privadas, con el propósito de que estas actividades y servicios se sujeten al ordenamiento jurídico y atiendan al interés general**. Las superintendencias actuarán de oficio o por requerimiento ciudadano. Las facultades específicas de las superintendencias y las áreas que requieran del control, auditoría y vigilancia de cada una de ellas se determinarán de acuerdo con la ley” (lo subrayado me pertenece).

Conjuntamente con la Ley Orgánica de Economía Popular y Solidaria (Asamblea Nacional, 2017), en su Art. 4, hace mención a que las personas y organizaciones amparadas por esta ley, tendrán entre uno de sus principios “la responsabilidad social y ambiental, la solidaridad y **rendición de cuentas...**” (lo subrayado me pertenece), en concordancia, también con el segundo inciso del Art. 146 ibídem, que manifiesta “La Superintendencia tendrá la facultad de **expedir normas de carácter general en las materias propias de su competencia**, sin que puedan alterar o innovar las disposiciones legales” (lo subrayado me pertenece). Además, la Superintendencia de Economía Popular y Solidaria podrá realizar el control a la normativa emitida, según sus atribuciones establecidas en el literal a, del Art. 147 ibídem.

6.6. Fundamentación

Administración de Riesgos

Según la Resolución No. 128-2015-F de la Junta de la Política y Regulación Monetaria y Financiera (2015), en su Art. 3 la Administración de Riesgos es “el proceso mediante el cual las entidades identifican, miden, priorizan, controlan, mitigan, monitorean y comunican los riesgos a los cuales se encuentran expuestas”.

Para el caso de nuestra investigación nos enfocaremos en el Riesgo Operativo, por lo que dentro de la normativa antes citada, en el Art. 15, describe en su parte pertinente:

Riesgo Operativo:

“Es la posibilidad que se produzca pérdidas para la entidad, debido a fallas o insuficiencias originadas en procesos, personas, tecnología de la información y eventos externos.

Así mismo, los factores a considerar para prevenir los riesgos operativos, descritos en la normativa, se propone, la creación de una unidad de auditoría informática dentro del organigrama estructural de cada cooperativa perteneciente al segmento 1 de la ciudad de Ambato, el mismo que tendrá la responsabilidad de realizar auditorías informáticas a las tecnologías de la información y comunicación de manera obligatoria.

Auditoría informática

Para León & Martínez García (1999, pág. 4) la auditoría de sistemas o informática es 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”, por lo tanto, es necesaria que la normativa sea emitida por la autoridad correspondiente, en este caso la Superintendencia de Economía Popular y Solidaria.

Con lo antes indicado, es importante mencionar que la Junta Bancaria del Ecuador a través de sus Resoluciones (Junta Bancaria)JB-2011-1851-1923 y JB-2012-2148 emiten la normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero y su reforma, en las mismas se hace referencia a la importancia de contar con una adecuada administración de Riesgos Operativo en el sector bancario, ya que los sistemas de información y comunicación son el alma de las instituciones financieras, de ahí también la importancia y la justificación para la realización de la presente propuesta.

6.7. Modelo operativo

La propuesta a la investigación realizada tiene como esencia el fortalecimiento de la administración de riesgos operativos en las cooperativas de ahorro y crédito segmento 1 de la ciudad de Ambato, para esto se le ha desarrollado la normativa para la creación de la unidad de Auditoría Informática en dichas cooperativas, según lo descrito a continuación:

RESOLUCIÓN XXX-2018
SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

CONSIDERANDO

Que, la Junta de la Política y Regulación Monetaria y Financiera, mediante Resolución Nro. 038-2015-F de 13 de febrero de 2015, expidió la Norma para la Segmentación de las Entidades del Sector Financiero, Popular y Solidario;

Que, la Superintendencia de Economía Popular y Solidaria mediante Oficio Nro. SEPS-2015-13648 de 22 de julio de 2015, remite para conocimiento y aprobación de la Junta, la propuesta de resolución de la Normas para la Administración Integral del Riesgo en las Cooperativas de Ahorro y Crédito y Cajas Centrales;

Que, la Junta de la Política y Regulación Monetaria y Financiera, mediante Resolución Nro. 128-2015-F de 23 de septiembre de 2015, expidió las Normas para la Administración Integral de Riesgo en las Cooperativas de Ahorro y Crédito y Cajas Centrales; y,

Que, la Ley Orgánica de Economía Popular y Solidaria en el segundo inciso del Art. 146, que manifiesta “La Superintendencia tendrá la facultad de expedir normas de carácter general en las materias propias de su competencia, sin que puedan alterar o innovar las disposiciones legales”,

RESUELVE

EXIGIR A LAS COOPERATIVAS DE AHORRO Y CRÉDITO SEGMENTO 1, CONTAR CON UNA UNIDAD DE AUDITORÍA INFORMÁTICA EN EL ORGANIGRAMA ESTRUCTURAL PARA EL FORTALECIMIENTO DE

LA ADMINISTRACIÓN DE RIESGOS OPERATIVOS, BAJO LOS SIGUIENTES PARÁMETROS.

Art. 1.- Las Cooperativas de Ahorro y Crédito segmento 1 deberán contar con una unidad de auditoría informática en su organigrama estructural.

Art. 2.- **Ámbito:** Las disposiciones de esta resolución se aplicarán de manera obligatoria a las Cooperativas de Ahorro y Crédito segmento 1, las cuales en adelante se les denominará solamente como “entidades”, cuyo control le compete a la Superintendencia de Economía Popular y Solidaria, mismas que implementarán procesos para la Administración Integral de los Riesgos Operativos.

La Administración de los Riesgos Operativos será parte de la estrategia de las entidades y del proceso de toma de decisiones.

Art. 3.- **Objeto:** La presente resolución tiene como objeto establecer los factores del Riesgo Operativo que deberán ser tratados por la unidad de Auditoría Informática, para que las entidades puedan identificar, medir, priorizar, controlar, mitigar, monitorear y comunicar los riesgos a los cuales se encuentran expuestas debido al desarrollo tecnológico.

Art. 4.- Para efectos de la aplicación de la presente resolución se considerarán las siguientes definiciones:

- a. Actividad.-** Es el conjunto de tareas;
- b. Administración de la información.-** Es el proceso mediante el cual se captura, procesa, almacena y transmite información, independientemente del medio que se utilice; ya sea impreso, escrito en papel, almacenado electrónicamente, transmitido por correo o medios electrónicos;

- c. Aplicación.-** Se refiere a los procedimientos programados a través de alguna herramienta tecnológica, que permiten la administración de la información y la oportuna toma de decisiones; así como, la utilización de productos y servicios que ofrece la entidad.
- d. Auditor Informático.-** Profesional con experiencia en informática y auditoría.
- e. Banca electrónica.-** Son los servicios suministrados por las entidades del sector cooperativo, segmento 1 a los clientes a través de internet, desde cualquier sitio a uno o más dominios de la entidad, indistintamente del dispositivo tecnológico a través del cual se acceda;
- f. Banca móvil.-** Son los servicios suministrados por las entidades controladas a los clientes a través de equipos celulares, tablets, u otro dispositivo inteligente, mediante los protocolos propios de este tipo de dispositivos;
- g. Canales electrónicos.-** Se refiere a todas las vías o formas a través de las cuales los clientes o socios pueden efectuar transacciones con las entidades de los sectores cooperativo segmento 1, mediante el uso de elementos o dispositivos electrónicos o tecnológicos, utilizando o no tarjetas. Principalmente son canales electrónicos: los cajeros automáticos (ATM), dispositivos de puntos de venta (POS y PIN Pad), sistemas de audio respuesta (IVR), señal telefónica, celular e internet u otro similares;
- h. Calidad de la información.-** Es el resultado de la aplicación de los mecanismos que garantizan la efectividad, eficiencia y

confiabilidad de la información y los recursos relacionados con ella;

- i. Confiabilidad.-** Es la garantía de que la información es la apropiada (real) para la administración de la entidad, ejecución de transacciones y para el cumplimiento de sus obligaciones;
- j. Confidencialidad.-** Es la garantía de que sólo el personal autorizado acceda a la información preestablecida; personal que deben pertenecer a la entidad, excepto por cuestiones de auditorías o exámenes especiales externos.
- k. Cumplimiento.-** Se refiere a la obediencia de las leyes, resoluciones, regulaciones y acuerdos contractuales a los que los procesos de las entidades están sujetos;
- l. Datos.-** Es cualquier forma de registro electrónico, óptico, magnético, impreso o en otros medios, susceptible de ser capturado, almacenado, procesado y distribuido;
- m. Disponibilidad.-** Es la garantía de que los usuarios autorizados tengan acceso a la información oportuna cada vez que lo requieran a través de los medios electrónicos o manuales adecuados;
- n. Unidad de Auditoría Informática.-** Es el departamento encargado de velar por la integridad, seguridad, confidencialidad y disponibilidad de la información, de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios internos a la información

- o. Efectividad.-** Es la garantía de que la información es relevante, pertinente y que su entrega es oportuna, correcta y consistente;
- p. Eficacia.-** Es la capacidad para contribuir al logro de los objetivos de las entidades de conformidad con los parámetros establecidos;
- q. Eficiencia.-** Es la capacidad para aprovechar racionalmente los recursos disponibles en pro del logro de los objetivos de la entidad, procurando la optimización de recursos y evitando derroches y errores;
- r. Encriptación.-** Es el proceso mediante el cual los archivos con información son alterados en forma lógica, con el objetivo de evitar que alguien no autorizado pueda interpretarlos con verlos o copiarlos, por lo que se utiliza una clave en el origen y en el destino para que puedan ser leídos;
- s. Evento de riesgo operativo.-** Es el hecho que puede derivar en pérdidas financieras para la entidad controlada;
- t. Factor de riesgo operativo.-** Es la causa primaria o el origen que genera un evento de riesgo operativo. Los factores son los procesos, personas, tecnología de la información y eventos externos;
- u. Incidente de tecnología de la información.-** Evento asociado a posibles fallas en la tecnología de la información y comunicación, fallas en los controles, o situaciones con probabilidad significativa de comprometer las operaciones del negocio.
- v. Incidente de seguridad de la información.-** Es el evento asociado a posibles fallas en la seguridad de la información, o una

situación con probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información, esto por, intrusiones no autorizadas o de terceros a los sistemas de información y comunicación.

- w. Insumo.-** Es el conjunto de materiales, datos o información que sirven como entrada para un proceso;
- x. Instalaciones informáticas.-** Es la infraestructura que permite alojar los recursos físicos relacionados con la tecnología de la información;
- y. Información.-** Es cualquier forma de registros electrónicos, ópticos, magnéticos o en otros medios, previamente procesados a partir de datos, que puede ser almacenado, distribuido y sirve para análisis, estudios, toma de decisiones, ejecución de una transacción o entrega de un producto o servicio;
- z. Integridad.-** Es la garantía de mantener en totalidad y exactitud de la información y de los métodos de procesamiento de cada transacción;
- aa. Medios electrónicos.-** Son los elementos de la tecnología de la información y comunicación que tienen características digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares;
- bb. Procedimiento.-** Es el método que especifica los pasos a seguir para cumplir un propósito determinado;

- cc. Proceso.-** Es el conjunto de actividades que transforman materias en productos o servicios con valor para el cliente, sea interno o externo;
- dd. Responsable de la información.-** Es el jefe de la unidad encargada de velar por la integridad, seguridad, confidencialidad y disponibilidad de la información, de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios internos a la información;
- ee. Riesgo legal.-** Es la probabilidad de que una entidad del sector cooperativo segmento 1, sufra pérdidas directas o indirectas; de que sus activos se encuentren expuestos a situaciones de mayor vulnerabilidad; de que sus pasivos y contingentes puedan verse incrementados más allá de los niveles esperados, o de que el desarrollo de sus operaciones enfrente la eventualidad de ser afectado negativamente, debido a error, negligencia, impericia, imprudencia o dolo, que deriven de la inobservancia, incorrecta o inoportuna aplicación de disposiciones legales o normativas, así como de instrucciones de carácter general o particular emanadas de los organismos de control, dentro de sus respectivas competencias; o, en sentencias o resoluciones jurisdiccionales o administrativas adversas; o de la deficiente redacción de los textos, formalización o ejecución de actos, contratos o transacciones, inclusive distintos a los de su giro ordinario de negocio, o porque los derechos de las partes contratantes no han sido claramente estipuladas;
- ff. Tarea.-** Es el conjunto de pasos o procedimientos que conducen a un resultado final visible y ponderable;

gg. Tarjetas.- Se refiere a las tarjetas de débito, de cajero automático y tarjetas de crédito;

hh. Tarjeta inteligente.- Tarjeta que posee circuitos integrados (chip) que permiten la ejecución de cierta lógica programada, contiene memoria y microprocesadores y es capaz de proveer seguridad, principalmente en cuanto a la confidencialidad de la información de la memoria;

ii. Tecnología de la información.- Es el conjunto de herramientas y métodos utilizados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, servicios asociados, entre otros;

jj. Transacción.- Se refiere a las acciones realizadas por los clientes a través de canales electrónicos, tales como: consultas, transferencias, depósitos, retiros, pagos, cambios de clave, créditos, actualización de datos y otras relacionadas;

kk. Transferencia electrónica de información.- Es la forma de enviar, recibir o transferir en forma electrónica datos, información, archivos, mensajes, entre otros;

Art. 5.- La Unidad de Auditoría Informática, será independiente a la de auditoría interna, tendrá la responsabilidad de la administración del riesgo operativo y deberá contar por lo menos con:

a) **Jefe de departamento:** Deberá desarrollar el plan operativo del departamento, las descripciones de los puestos de trabajo del personal a su cargo, las planificaciones de actuación a un año, los métodos de gestión de cambio en sus funciones y los programas

de formación individualizados, así como gestionar los programas de trabajo y los trabajos en sí, los cambios en los métodos de trabajo y evaluar la capacidad del personal a su cargo.

- b) **Supervisor de auditoría informática:** Deberá trabajar estrechamente con el Jefe del departamento en las tareas operativas diarias. Ayuda en la evaluación del riesgo de cada uno de los trabajos, realizar los programas de trabajo, dirigir y supervisar directamente a las personas en cada uno de los trabajos de los que es responsable. Realizar la información sobre el trabajo. Es responsable en junto con su jefe de la obtención del mejor resultado del trabajo auditado, vinculando los conceptos de valor añadido y gestión del cambio en su trabajo.

- c) **Auditor informático:** Es el responsable para la ejecución directa del trabajo. Debe tener una especialización genérica, pero también una específica, su trabajo consistirá en la obtención de información, realización de pruebas, documentación del trabajo, evaluación y diagnóstico de los resultados.

Art. 6.- Perfil del Auditor informático. El profesional que será elegido como auditor informático deberá tener al menos las siguientes características:

- a) **Instrucción Formal:** Título de tercer nivel registrado en la SENESCYT como Ingeniero en contabilidad y auditoría C.P.A. o a fines.

- b) **Experiencia:** Por lo menos 2 años en actividades de auditoría.

c) **Conocimientos:** Los conocimientos del auditor informático deben ser mínimo 180 horas de capacitación en cualquiera de los siguientes temas:

- Desarrollo informático: gestión de proyectos y del ciclo de vida de un proyecto de desarrollo.
- Gestión de departamento de sistemas
- Análisis de riesgos en un entorno informático
- Sistemas operativos
- Telecomunicaciones
- Gestión de base de datos
- Redes locales
- Seguridad física
- Operación y planificación informática; efectividad de las operaciones y del rendimiento de los sistemas
- Gestión de la seguridad de los sistemas y contingencia de la información
- Gestión de problemas y de cambios en entornos informáticos
- Administración de datos
- Ofimática
- Comercio electrónico
- Encriptación de datos
- Economía Popular y Solidaria

d) **Principios:** Los principios que regirán al auditor informático serán:

- Independencia
- Calidad
- Capacidad
- Comportamiento profesional
- Confianza

- Criterio Propio
- Discreción
- Economía
- De formación continua
- Integridad moral
- Legalidad
- No discriminación
- No injerencia
- Secreto profesional
- Veracidad

Art. 7.- Funciones de la Unidad de Auditoría informática. Las funciones de la unidad de auditoría informática serán:

- Elaboración de procedimientos para el riesgo operativo, considerando los factores de riesgo, esto para su evaluación y aprobación;
- Realizar auditorías informáticas, por lo menos dos (2) veces al año;
- Emitir informes de auditoría informática manifestando su opinión responsable sobre la fiabilidad de la información para que se conozca y valore por terceros o por su ente de control;
- Emitir recomendaciones, que al menos tengan, la debilidad encontrada, el criterio o instrumento de medida que se ha utilizado, los efectos que puede tener el sistema de información y la recomendación con la que esta debilidad se podría eliminar;
- Diseñar y proponer las políticas para la administración del riesgo operativo;

- Evaluar y proponer mejoras al proceso de administración de riesgo operativo y asegurarse que sean implementados en toda la entidad y que todos los niveles del personal entiendan sus responsabilidades con relación al riesgo operativo;
- Definir los mecanismos para monitorear y evaluar los cambios significativos y la exposición a riesgos, provenientes de los procesos, las personas, la tecnología de la información y los eventos externos;
- Verificación del control interno, tanto de aplicaciones informáticas como de los sistemas informáticos, centrales y periféricos;
- Análisis de la gestión de los sistemas de información desde un punto de vista de riesgo de seguridad, de gestión y de efectividad de la gestión;
- Análisis de la integridad, fiabilidad y certeza de la información a través del análisis de las aplicaciones;
- Auditorías del riesgo operativo de todos los circuitos informáticos;
- Análisis de la gestión de los riesgos de la información y de la seguridad;
- Verificación del nivel de continuidad de las operaciones informáticas;
- Diagnóstico sobre el grado de confiabilidad de las aplicaciones y sistemas informáticos utilizados por la cooperativa; y,

- Establecer, implementar, ejecutar, monitorear, mantener y documentar un sistema de gestión de seguridad de la información.
- Cumplir y hacer cumplir resoluciones emitidas por la Junta Bancaria, así como por la Junta de la Política y Regulación Monetaria y Financiera.

Art. 8.- Factores del Riesgo Operativo. Con el propósito de que se minimice la probabilidad de incurrir en pérdidas financieras económicas atribuibles al riesgo operativo, se establecen los siguientes aspectos para una adecuadamente elaboración de procedimientos acorde a cada cooperativa:

1. **Ejecución, entrega y gestión de procesos.-** Es la operatividad de los procesos, así como lo atribuible a los responsables de esos procedimientos, para eso se ha clasificado de la siguiente manera:

- **Procesos.-** Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, las entidades deben contar con procesos definidos de conformidad con la estrategia y las políticas adoptadas. Se deberá tomar en consideración una adecuada, oportuna ejecución de actividades, que las actividades se desarrollen dentro del tiempo estimado, que se realice el correcto y oportuno registro de actividades, que se realice todos los trámites con los requisitos previos, así como con una adecuada segregación de funciones, que evite concentraciones de funciones de carácter incompatible, es decir, aquellas tareas cuya combinación y competencia de una sola persona, eventualmente, podría permitir la realización o el ocultamiento de fraudes, errores,

omisiones, faltantes, sobrantes u otros eventos del riesgo operativo.

- **Personas.-** Las entidades controladas deben administrar el capital humano de forma adecuada, e identificar apropiadamente las fallas o insuficiencias asociadas al factor “personas”, tales como: falta de personal adecuado, negligencia, error humano, nepotismo de conformidad con las disposiciones legales vigentes, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros.

Para considerar la existencia de un apropiada gestión del riesgo operativo a través de las personas, las entidades controladas deberán definir formalmente políticas, procesos y procedimientos que aseguren una apropiada planificación y administración del capital humano, los cuales considerarán los procesos de incorporación, permanencia y desvinculación del personal al servicio de la entidad. Para lo cual, los procesos a considerar son:

- **Los procesos de incorporación.-** Que comprenden la planificación de necesidades, el reclutamiento, la selección del personal previa verificación del perfil requerido, la contratación e inducción de nuevo personal;
- **Los procesos de permanencia.-** Que cubren la creación de condiciones laborales idóneas; la promoción de actividades de capacitación y formación que permitan al personal aumentar y perfeccionar sus conocimientos, competencias y destrezas; para de esta manera fidelizar

al trabajador con la empresa, para esto se deberá mantener un sistema de evaluación del desempeño; desarrollo de carrera; rendición de cuentas; e incentivos que motiven la adhesión a los valores y controles institucionales; y,

- **Los procesos de desvinculación.-** Que comprenden la planificación de la salida del personal por causas regulares y por aspectos jurídicos para llegar al finiquito y la finalización de la relación laboral; firmando acuerdos de confidencialidad sobre procesos internos de la empresa.

Los procesos de incorporación, permanencia y desvinculación antes indicados deberán ser soportados técnicamente, ajustados a las disposiciones legales y transparentes para garantizar condiciones laborales idóneas.

2. Incidencia en el negocio y fallos en los sistemas.- Son los atribuibles a los sistemas utilizados por las cooperativas de ahorro y crédito, estos son:

- **Tecnología de la información.-** Las entidades controladas deben contar con tecnología de la información y comunicación que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable, así como que también que esta información sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones.

Para considerar la existencia de un apropiada Administración de riesgo operativo, las entidades deberán definir políticas, procesos,

procedimientos y metodologías que aseguren una adecuada planificación y administración de la tecnología de la información y comunicación.

Dichas políticas, procesos, procedimientos y metodologías se referirán a los siguientes aspectos:

- **Administración de la tecnología de la información y los requerimientos de operación actuales y futuras de la entidad**, las entidades deben contar al menos con lo siguiente:
 - El apoyo y compromiso formal del directorio y la alta gerencia, a través de la asignación de recursos para el cumplimiento de los objetivos tecnológicos;
 - Un plan funcional de tecnología de la información alineado con el plan estratégico institucional; y, un plan operativo que establezca las actividades a ejecutar en el corto plazo (un (1) año), traducido en tareas, cronogramas, personal responsable y presupuesto, de manera que se asegure el logro de los objetivos institucionales propuestos;
 - Tecnología de la información y comunicación acorde a las operaciones del negocio y al volumen de transacciones, monitoreada y proyectada según las necesidades y crecimiento de la entidad, con su correspondiente portafolio de proyectos tecnológicos a ejecutarse en el corto, mediano y largo plazo;



- Políticas, procesos, procedimientos y metodologías de tecnología de la información y comunicación definidos bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, alineados a los objetivos y actividades de la entidad;
 - Los procesos, procedimientos y metodologías de tecnología de la información y comunicación deben ser elaborados por la Unidad de auditoría informática, para que luego sean revisados y aprobados por el directorio;
 - La difusión y comunicación a todo el personal involucrado acerca de las mencionadas políticas, procesos, procedimientos y metodologías aprobadas, de tal forma que se asegure su implementación y cumplimiento; y,
- **Operaciones de tecnología de la información y comunicación**, las entidades deben contar al menos con lo siguiente:
- Procedimientos que establezcan las actividades y responsables de la operación y el uso de las instalaciones de procesamiento de información;
 - Procedimientos de gestión de incidentes de tecnología de la información y comunicación, que considere al menos su registro, priorización, análisis, escalamiento y solución;



- Inventario de la infraestructura tecnológica que considere por lo menos, su registro, responsables de uso y mantenimiento; y,
 - Procedimientos de respaldo de información periódicos, esto es, acorde a las transacciones y movimientos económicos, mínimo será una vez al mes.
- **Adquisición, desarrollo, implementación y mantenimiento de las aplicaciones informáticas**, las entidades controladas deben contar al menos con lo siguiente:
- Una metodología que permita la adecuada administración y control del proceso de compra de software y del ciclo de vida de desarrollo y mantenimiento de aplicaciones, con la aceptación de los usuarios involucrados;
 - Un documento que refleje el alcance de los requerimientos funcionales;
 - Un documento que refleje los requerimientos técnicos y la relación y afectación a la capacidad de la infraestructura tecnológica actual;
 - Ambientes aislados con la debida segregación de accesos, para desarrollo, pruebas y producción, los cuales deben contar con la capacidad requerida para cumplir sus objetivos. Al menos se debe contar con dos ambientes: desarrollo y producción;



- Escaneo de vulnerabilidades en código fuente para identificar el nivel de riesgo del ambiente de la aplicación informática y en aplicaciones puestas en producción;
 - Pruebas técnicas y funcionales que reflejen la aceptación de los usuarios autorizados;
 - Procedimientos de control de cambios que considere su registro, manejo de versiones, segregación de funciones y autorizaciones e incluya los cambios emergentes;
 - Documentación técnica y de usuario permanentemente actualizada de las aplicaciones informáticas de la entidad; y,
 - Procedimientos de migración de la información, que incluyan controles para garantizar las características de integridad, seguridad, disponibilidad y confidencialidad.
- **Infraestructura tecnológica que soporte las operaciones de la entidad**, deben contar al menos con:
- Procedimientos que permitan la administración, monitoreo y registros de configuración de las bases de datos, redes de datos, hardware y software base, que incluya límites y alertas;
 - Un documento de análisis de la capacidad y desempeño de la infraestructura tecnológica que



soporta las operaciones de la entidad, que debe ser conocido y analizado por la Unidad de Auditoría Informática con una frecuencia mínima semestral. El documento debe incluir límites y alertas de al menos: almacenamiento, memoria, procesador, consumo de ancho de banda; y, para bases de datos: áreas temporales de trabajo, log de transacciones y almacenamiento de datos;

- Procedimientos de migración de la plataforma tecnológica, que incluyan controles para garantizar la continuidad del servicio; y por último,
- Instalaciones para el procesamiento de la información debe considerar áreas protegidas con los suficientes controles que eviten el acceso de personal no autorizado, daños a los equipos de computación y a la información en ellos procesada, almacenada o distribuida; y, condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la infraestructura de tecnología de la información y comunicación.

3. **Fraude externo.**- Dentro de éste ítem, se debe considerar lo siguiente:

- **Medidas de seguridad en canales electrónicos,** Con el objeto de garantizar que las transacciones realizadas a través de canales electrónicos cuenten con los controles, medidas y elementos de seguridad para evitar el cometimiento de eventos fraudulentos (delitos informáticos) y garantizar la seguridad y calidad de la información de los clientes o socios, éstas deberán cumplir como mínimo con lo siguiente:

- Las entidades deberán adoptar e implementar los estándares y buenas prácticas internacionales de seguridad vigentes a nivel mundial para el uso y manejo de canales electrónicos y consumos con tarjetas, los cuales deben ser permanentemente monitoreados para asegurar su cumplimiento;
- Establecer procedimientos y mecanismos para monitorear de manera periódica la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones, así como en cualquier otro elemento electrónico o tecnológico utilizado en los canales electrónicos, de tal manera que se garantice permanentemente la seguridad informática y la calidad de la información;
- Canales de comunicación seguros mediante la utilización de técnicas de encriptación acorde con los estándares internacionales vigentes.
- El envío de información de sus clientes o socios relacionada a números de cuentas y tarjetas, debe ser realizado bajo condiciones de seguridad de la información, considerando que cuando dicha información se envíe mediante correo electrónico o utilizando algún otro medio vía Internet, ésta deberá ser encubierta;
- La información confidencial que se transmita entre el canal electrónico y el sitio principal de procesamiento de la entidad, deberá estar en todo momento protegida mediante el uso de técnicas de encriptación acordes con

los estándares internacionales vigentes y deberá evaluarse con regularidad la efectividad del mecanismo utilizado;

- Las entidades deberán contar en todos sus canales electrónicos con software antimalware que esté permanentemente actualizado, el cual permita proteger el software instalado, detectar oportunamente cualquier intento o alteración en su código, configuración y/o funcionalidad, y emitir las alarmas correspondientes para el bloqueo del canal electrónico, su inactivación y revisión oportuna por parte de personal técnico autorizado de la entidad;
- Las entidades deberán utilizar tecnología específica para la generación y validación de claves para procesar y ejecutar transacciones en los diferentes canales electrónicos, dicha información en todo momento debe estar encriptada;
- Establecer procedimientos para monitorear, controlar y emitir alarmas en línea que informen oportunamente sobre el estado de los canales electrónicos, con el fin de identificar eventos inusuales, fraudulentos o corregir las fallas;
- Ofrecer a los clientes los mecanismos necesarios para que personalicen las condiciones bajo las cuales desean realizar sus transacciones que impliquen movimiento de dinero a través de los diferentes canales electrónicos y tarjetas, dentro de las condiciones o límites máximos que deberá establecer cada entidad. Entre las principales condiciones de personalización por cada tipo

de canal electrónico, deberá constar: el registro de las cuentas a las cuales desea realizar transacciones monetarias, números de suministros de servicios básicos, números de telefonía fija y móvil, montos máximos por transacción diaria, semanal y mensual, entre otros. Para el caso de consumos con tarjetas, se deberán personalizar los cupos máximos, principalmente para los siguientes servicios: consumos nacionales, consumos en el exterior, compras por internet, entre otros;

- Requerir a los clientes que el registro y modificación de la información referente a su número de telefonía móvil y correo electrónico, se realicen por canales presenciales, además no se debe mostrar esta información por ningún canal electrónico;
- Las entidades también deben registrar las direcciones IP y números de telefonía móvil desde las que se realizan las transacciones. Para permitir transacciones desde direcciones IP y telefonía móvil de otros países se debe tener la autorización expresa del cliente;
- Renovar por lo menos dos veces (2) al año de las claves de acceso a los canales electrónicos, la clave de banca electrónica debe ser diferente de aquella por la cual se accede a otros canales electrónicos;
- Las entidades deberán establecer procedimientos de control y mecanismos que permitan registrar el perfil de cada cliente sobre sus comportamientos transaccionales que impliquen movimiento de dinero en el uso de canales electrónicos y tarjetas y definir procedimientos

para monitorear en línea y permitir o rechazar de manera oportuna la ejecución de transacciones que impliquen movimiento de dinero que no correspondan a sus hábitos, lo cual deberá ser inmediatamente notificado al cliente mediante mensajería móvil, correo electrónico, u otro mecanismo;

- Incorporar en los procedimientos de administración de la seguridad de la información, el bloqueo de los canales electrónicos o de las tarjetas cuando se presenten eventos inusuales que adviertan situaciones fraudulentas, esto después de un número máximo de tres (3) intentos de acceso fallido. Además, de ser bloqueado el canal electrónico deberán establecer procedimientos que permitan la notificación al cliente a través de llamada telefónica, mensajería móvil, correo electrónico u otro mecanismo, así como su reactivación de manera segura a pedido del cliente;
- Asegurar que exista una adecuada segregación de funciones entre el personal que administra, opera, mantiene y en general accede a los dispositivos y sistemas usados en los diferentes canales electrónicos y tarjetas;
- Las entidades deberán establecer procedimientos y controles para la administración, transporte, instalación y mantenimiento de los elementos y dispositivos que permiten el uso de los canales electrónicos y de tarjetas;
- Las entidades deben mantener sincronizados todos los relojes de sus sistemas de información que estén involucrados con el uso de canales electrónicos, para

saber fecha y hora real en las que las transacciones fueron realizadas;

- Mantener como mínimo durante veinticuatro (24) meses el registro histórico de todas las transacciones que se realicen a través de los canales electrónicos, el cual deberá contener como mínimo: fecha, hora, monto, números de cuenta (origen y destino), código de la entidad de los sectores financieros público y privado de origen y de destino, número de transacción, código del dispositivo: para operaciones por cajero automático: código del ATM, para transacciones por internet: la dirección IP, para transacciones a través de sistemas de audio respuesta - IVR y para transacciones de banca electrónica mediante dispositivos móviles: el número de teléfono con el que se hizo la conexión. En caso de presentarse reclamos por etapas judiciales, la información deberá conservarse hasta que se agoten las instancias legales;
- Incorporar en los procedimientos de administración de la seguridad de la información, controles para impedir que funcionarios de la entidad que no estén debidamente autorizados tengan acceso a consultar información confidencial de los clientes en ambiente de producción. En el caso de información contenida en ambientes de desarrollo y pruebas, ésta deberá ser enmascarada o codificada. Todos estos procedimientos deberán estar debidamente documentados en los manuales respectivos, así como el procedimiento de desvinculación del trabajador, el mismo que tuvo

usuarios y contraseñas para los sistemas de la entidad para que sean desactivados el último día de labores.

- Además, la entidad deberá mantener y monitorear un log de auditoría sobre las consultas realizadas por los funcionarios a la información confidencial de los clientes, la cual debe contener como mínimo: identificación del funcionario, sistema utilizado, identificación del equipo (IP), fecha, hora, e información consultada. Esta información deberá conservarse por lo menos por veinticuatro (24) meses;
- Las tarjetas emitidas por las entidades deben ser tarjetas inteligentes, es decir, deben contar con microprocesador o chip; y, las entidades controladas deberán adoptar los estándares internacionales de seguridad y las mejores prácticas vigentes sobre su uso y manejo;
- Mantener permanentemente informados y capacitar a los clientes sobre los riesgos derivados del uso de canales electrónicos y de tarjetas; y, sobre las medidas de seguridad que se deben tener en cuenta al momento de efectuar transacciones a través de éstos; así como de las medidas o procedimientos que la entidad ha diseñado para evitar los riesgos por uso de canales electrónicos y de tarjetas.
- Informar y capacitar permanentemente a los clientes sobre los procedimientos para el bloqueo, inactivación, reactivación y cancelación de los canales electrónicos ofrecidos por la entidad;

- Las entidades deberán informar sobre las medidas correctivas establecidas en los casos de reclamos de los clientes o socios que involucren debilidades, registros de transacciones no realizadas, violación de los niveles de seguridad; información que deberá remitirse una vez al mes.
- En todo momento en donde se solicite el ingreso de una clave, ésta debe aparecer enmascarada; es decir, oculta para a la vista, utilizando caracteres como “*”, “.”, etc.
- **Cajeros automáticos**, Con el objeto de garantizar la seguridad en las transacciones realizadas a través de los cajeros automáticos, las entidades deberán cumplir con por lo menos con lo siguiente:
 - Los dispositivos utilizados en los cajeros automáticos para la autenticación del cliente o usuario, deben encriptar la información ingresada a través de ellos; y, la información de las claves no debe ser almacenada en ningún momento, y deberá aparecer enmascarada; es decir, oculta para a la vista, utilizando caracteres como “*”, “.”, etc.
 - La entidad controlada debe implementar mecanismos internos de autenticación del cajero automático que permitan asegurar que es un dispositivo autorizado; cajeros automáticos deben ser capaces de procesar la información de tarjetas inteligentes o con chip;
 - Los cajeros automáticos deben estar instalados de acuerdo con las especificaciones del fabricante, así como

con los estándares de seguridad definidos en las políticas de la entidad, incluyendo el cambio de las contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores;

- Establecer y ejecutar procedimientos de auditoría de seguridad informática en todos los cajeros automáticos por lo menos una (1) vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan a través de estos. Los procedimientos de auditoría deberán ser ejecutados por personal capacitado y con experiencia;
- **Banca electrónica,** Con el objeto de garantizar la seguridad en las transacciones realizadas mediante la banca electrónica (web), las entidades que ofrezcan éste servicio por medio de canales electrónicos deberán cumplir como mínimo con lo siguiente:
 - Implementar los algoritmos y protocolos seguros, así como certificados digitales, que ofrezcan las máximas seguridades en vigor dentro de las páginas web de las entidades controladas, a fin de garantizar una comunicación segura, la cual debe incluir el uso de técnicas de encriptación de los datos transmitidos acordes con los estándares internacionales vigentes;
 - Realizar como mínimo una vez (1) al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación utilizados en la ejecución de transacciones por banca electrónica (hacking ético); y, en caso de que se realicen cambios en la plataforma que

podrían afectar a la seguridad de este canal, se deberá efectuar una prueba adicional. Las pruebas de vulnerabilidad y penetración deberán ser efectuadas por personal independiente a la entidad, de comprobada experiencia y aplicando estándares vigentes y reconocidos a nivel internacional. Las entidades deberán definir y ejecutar planes de acción sobre las vulnerabilidades detectadas;

- Los informes de las pruebas de vulnerabilidad deberán estar a disposición de la Superintendencia de Economía Popular y Solidaria, incluyendo un análisis comparativo del informe actual respecto del inmediatamente anterior; además de estar disponible en la página web de la cooperativa, en la sección de transparencia.
- Implementar mecanismos de control, autenticación mutua y monitoreo, que minimicen la posibilidad de que los clientes accedan a páginas web falsas similares a las propias de las entidades para realizar transacciones;
- Implementar mecanismos de seguridad incluyendo dispositivos tales como IPS (sistema de prevención de Intrusos), firewalls, entre otros, que reduzcan la posibilidad de que la información de las transacciones de los clientes sea capturada por terceros no autorizados durante la sesión;
- Establecer un tiempo máximo de inactividad, después del cual deberá ser cancelada la sesión y exigir un nuevo proceso de autenticación al cliente para realizar otras transacciones; no podrá exceder de 10 minutos.

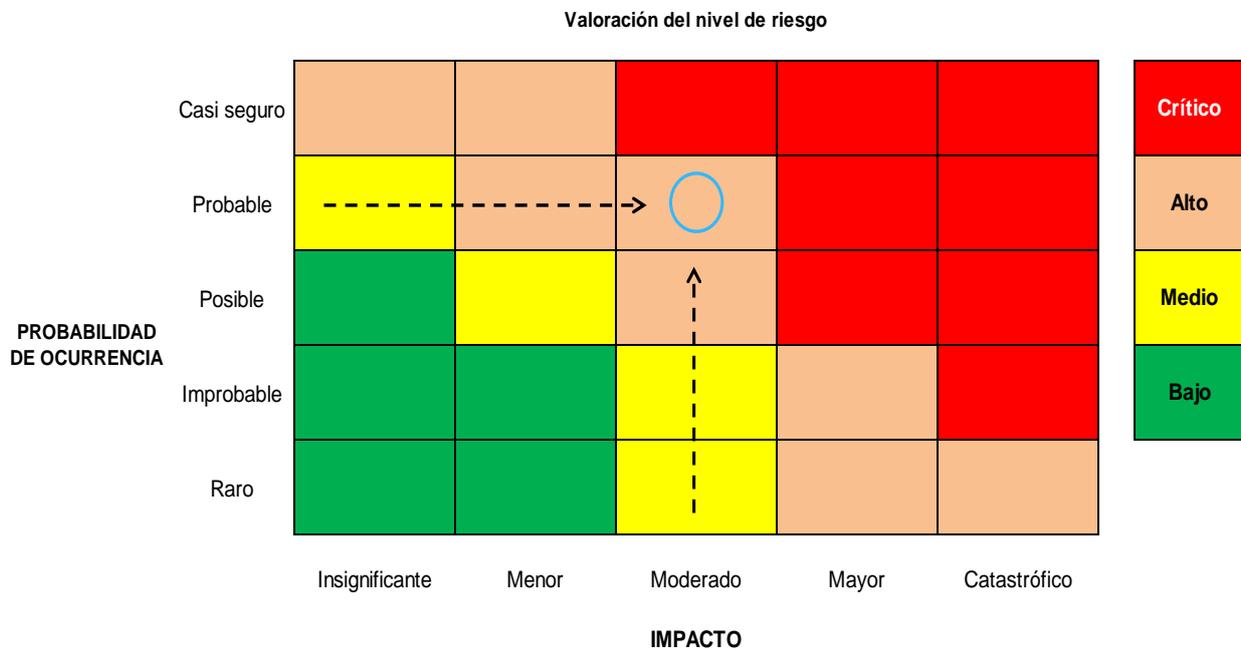
- Se deberá informar al cliente al inicio de cada sesión, la fecha y hora del último ingreso al canal de banca electrónica a través de diferentes medios;
- Para la ejecución de transacciones de clientes, se deberán implementar mecanismos de autenticación que contemplen por lo menos dos de tres preguntas: considerando que se realizará una pregunta de las tres de manera aleatoria al usuario para comprobar autenticidad del cliente, dejando a salvo la utilización de otros controles como biométricos, etc.
- **Banca móvil.-** Las entidades que presten servicios a través de banca móvil deberán sujetarse a lo dispuesto para los factores de riesgo operativo correspondiente al fraude externo.

Art. 9.- Manejo del control interno, la unidad de Auditoría Informática deberá utilizar la siguiente matriz para un adecuado control interno de los Riesgos Operativos:

| No. | Macroproceso / Servicio | Proceso / Producto | Descripción del riesgo | Tipo de Riesgo | Causas | Factor del Riesgo | Consecuencias | Tipo de Impacto | Probabilidad | Impacto | Nivel de Riesgo | Controles Existentes | Tipo de Control | Clase de Control | Frecuencia | Responsable del Control | Documentación del Control | Evaluación Efectividad del Control | |
|-----|-------------------------|--------------------|------------------------|----------------|--------|--|---------------|-----------------|--|--|----------------------------------|----------------------|----------------------------|-----------------------|------------|-------------------------|---------------------------|------------------------------------|--|
| 1 | | | | OPERATIVO | | 1. Incidencia en el negocio y fallos en los sistemas 2. Ejecución, entrega y gestión de procesos 3. Fraude externo | | | Casi seguro Probable Posible Improbable Raro | Insignificante Menor Moderado Mayor Catastrófico | Crítico Alto Medio Bajo | | Preventivo Cumplimiento | Manual Sistemático | | | | | 1. No se aplica 2. Se aplica pero no efectivo 3. Se aplica y es efectivo |

| Plan de Mejoramiento | Responsable | Fecha de inicio (DD/MM/AA) | Fecha de terminación (DD/MM/AA) | Fecha de seguimiento (DD/MM/AA) | Documentación del Control (Evidencia obtenida) | Evaluación Efectividad del Control | Observación / Recomendación |
|----------------------|-------------|----------------------------|---------------------------------|---------------------------------|--|--|-----------------------------|
| | | | | | | 1. No se aplica 2. Se aplica pero no efectivo 3. Se aplica y es efectivo | |

Art. 10.- Nivel de riesgo, para la medición del nivel de riesgo se utilizará la metodología de Ocurrencia – Impacto, de acuerdo al siguiente detalle:



Tomando para dicha metodología, en la opción de probabilidad de Ocurrencia estará los siguientes ítems:

- ✓ Casi seguro
- ✓ Probable
- ✓ Posible
- ✓ Improbable
- ✓ Raro

Del mismo modo, en la opción de Impacto, estarán los siguientes ítems:

- ✓ Insignificante
- ✓ Menor
- ✓ Moderado
- ✓ Mayor
- ✓ Catastrófico

Para lo cual todas las cooperativas utilizarán el aplicativo para éste apartado, que se encuentra anexo al mismo.

Art. 11.- Informes de auditoría.- Luego de haber realizado auditorías, exámenes especiales o análisis a las tecnologías de la información y comunicación por parte de la unidad de auditoría informática, ésta deberá emitir un informe, en el que exprese la opinión del auditor informático, el tipo de opinión, que podrá ser:

- Favorable
- Desfavorable
- Con salvedades
- Negación de opinión

Art. 12.- Presentación de informes de auditoría.- Luego de realizado el informe de auditoría señaladas en el Art. 10, la Unidad de Auditoría informática remitirá el informe al Consejo de Administración, al Comité de Administración Integral de Riesgos y a la Superintendencia de Economía Popular y Solidaria para su análisis, además, dicho informe también deberá ser publicado en la página institucional de la cooperativas, en la sección de transparencia, para que sea de conocimiento y de acceso para todo el público en general.

DISPOSICIONES GENERALES

PRIMERA.- Deróguese toda norma que va contra a la estipulada.

SEGUNDO.- Encárguese a la Dirección de Auditoría del Sector Financiero para que en su planificación para el año 2019, se revise los informes remitidos por las cooperativas segmento 1, acerca de las auditorías informáticas realizadas en el año 2018.

DISPOSICIÓN FINAL

La presente resolución entrará en vigencia a partir de su suscripción, sin perjuicio de la publicación en el Registro Oficial.

COMUNÍQUESE Y PUBLÍQUESE.-

Dado en la ciudad de San Francisco de Quito, Distrito Metropolitano a los .. días del mes de ,,,, de 2018.

SUPERINTENDENTE DE ECONOMÍA POPULAR Y SOLIDARIA

DOCUMENTO ANEXO A LA RESOLUCIÓN

Para la aplicación del Art. 11, la Superintendencia de Economía Popular y Solidaria, ha realizado el siguiente aplicativo para la medición del Nivel de Riesgo Operativo:



Calificación del Riesgo Operativo

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

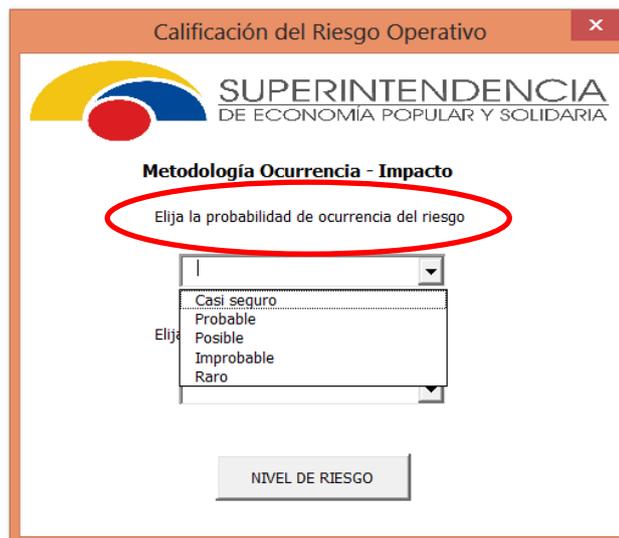
Metodología Ocurrencia - Impacto

Elija la probabilidad de ocurrencia del riesgo

Elija el impacto que podría ocasionar

NIVEL DE RIESGO

Utilizando la metodología de probabilidad de Ocurrencia – Impacto, se deberá elegir lo solicitado en el aplicativo.



Calificación del Riesgo Operativo

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

Metodología Ocurrencia - Impacto

Elija la probabilidad de ocurrencia del riesgo

Elija

- Casi seguro
- Probable
- Posible
- Improbable
- Raro

NIVEL DE RIESGO

Calificación del Riesgo Operativo



SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

Metodología Ocurrencia - Impacto

Elija la probabilidad de ocurrencia del riesgo

Elija el impacto que podría ocasionar

- Insignificante
- Menor
- Moderado
- Mayor
- Catastrófico

Al no seleccionar las opciones indicadas, el aplicativo solicitará que se llene todos los campos,

Calificación del Riesgo Operativo



SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

****Información incompleta**

 Favor de completar los datos

Aceptar

NIVEL DE RIESGO

Llenado que haya sido todos los campos, el aplicativo desplazará la Calificación del nivel de Riesgo Operativo, adicionalmente, de acuerdo a la siguiente imagen,



Luego del mostrar el nivel de Riesgo Operativo, se puede realizar otras consultas o salir del aplicativo.

Bibliografía

- Analuisa, P., & Erazo, T. (Junio de 2007). Auditoría Informática al departamento de Tecnologías de la Información (T.I.) de Hidropaute. *Auditoría Informática al departamento de Tecnologías de la Información (T.I.) de Hidropaute*. Quito, Pichincha, Ecuador: Escuela Politécnica Nacional.
- Arias, M. (2006). Panorama general de la Informática Forense y de los Delitos Informáticos en Costa Rica. *InterSedes: Revista de las Sedes Regionales*, 141-154.
- Arocena, G. (2012). LA REGULACIÓN DE LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL ARGENTINO. *Boletín Mexicano de Derecho Comparado*, XLV(135), 945-988.
- Asamblea Nacional Constituyente. (10 de Febrero de 2014). Código Orgánico integral Penal . Quito, Pichincha, Ecuador: Asamblea Nacional Constituyente.
- Asamblea Nacional, C. (2015). *Constitución de la República del Ecuador*. Quito: Registro Oficial.
- Asamblea Nacional, C. (2017). *Ley Orgánica de Economía Popular y Solidaria*. Quito: Registro Oficial.
- Asociación de Control y Auditoría de sistemas de Información. (2005). *Normas generales para la auditoría de sistemas de información* . Asociación de Control y Auditoría de sistemas de Información.
- Bravo, O. (2010). La Auditoría Informática como un factor de éxito en el cumplimiento de Objetivos Empresariales. Quito, Pichincha, Ecuador: Pontificia Universidad Católica del Ecuador.
- Cerda, H. (1998). *Los elementos de la Investigación*. Bogotá: EL Búho.
- Chiriboga Rosales, L. A. (2010). SISTEMA FINANCIERO. En L. A. Chiriboga Rosales, *SISTEMA FINANCIERO* (pág. 6). Quito: PUBLIGRAFICAS JOKAMA.
- Coello Coello, C. (2003). *Breve historia de la computación y sus pioneros*. México: Fondo de Cultura Económica.

- Constituyente, A. (27 de Febrero de 2012). Reglamento de la Ley Orgánica del Sistema de Economía Popular y Solidaria. Quito, Pichincha, Ecuador: Asamblea Constituyente.
- Cooper, & Lybran . (1997). *Los nuevos conceptos del control interno (Informe COSO)*. (I. C. Framework, Trad.) Madrid: Ediciones Días de Santos, S.A.
- Definición DE. (2008). *Definición DE*. Recuperado el 19 de Enero de 2015, de <http://definicion.de/derecho-constitucional/>
- Delgado Rojas, X. (2015). *Auditoría Informática*. Costa Rica: EUNED.
- DELITOS INFORMÁTICOS. (2015 de Julio de 2015). *DELITOS INFORMÁTICOS*. (J. Alfocea, Editor) Recuperado el 30 de Diciembre de 2015, de <http://www.delitosinformaticos.com/07/2015/delitos/fraudes-y-estafas/investigacion-complicado-caso-transferencias-fantasma-dinero>
- Echenique, J. (2006). *Auditoría en Informática* (Primera ed.). México-México: McGraw-Hill.
- EL PAÍS. (23 de Septiembre de 2015). Los dispositivos de Apple sufren el mayor ciberataque de su historia. *DIARIO EL PAÍS*, págs. s-p.
- El Tiempo. (17 de Junio de 2014). Cae red que robó a bancos más de \$ 10.000 millones por internet. *El Tiempo*, págs. S-P.
- EL UNIVERSO. (17 de Noviembre de 2014). Delitos informáticos en la web podrían aumentar en Ecuador. *EL UNIVERSO - NOTICIAS*, págs. S-N.
- Financiera, J. d. (23 de 09 de 2015). Resolución No. 128-2015-F. *Resolución No. 128-2015-F*. Quito, Pichincha, Ecuador: Registro Oficial.
- Fiscalía General del Estado. (13 de Junio de 2015). *Fiscalía General del Estado*. Recuperado el 29 de Diciembre de 2015, de <http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje.html>
- Fonseca, O. (2011). *Sistema de Control Interno para Organizaciones*. Lima: Instituto de Investigaciones en Accountability y Control - IICO.

- Galán Quiroz, L. (1996). *Informática y auditoría para las ciencias empresariales*. Bucaramanga: UNAB.
- Gilson, E. (1962). *El ser y la esencia*. Buenos Aires: Deschlee de Browner.
- Graterol, C., & Hernández, A. (20 de Junio de 2011). Aplicación de la norma COBIT en el monitoreo de transferencias electrónicas de datos contable-financieros. *Publicaciones en Ciencias y Tecnología*, V(1), 27-42.
- Herrera, L., Medina, A., & Galo, N. (2010). *Tutoría de la Investigación Científica*. Ambato: Diemerino editores.
- Junta Bancaria, d. (2011). *Resolución JB-2011-1851-1923*. Quito: Registro Oficial.
- Junta Bancaria, d. (2012). *JB-2012-2148*. Quito: Registro Oficial.
- Langenbach, R. G. (1976). *Introducción al proceso de datos*. Barcelona: Editores Técnicos Asociados S.A.
- León, Z., & Martínez García, C. (1999). *Auditoría Informática*. La Habana: Cimex.
- Martínez, A., Briseida, B., & Marichal, L. (Agosto de 2012). Auditoría con Informática a Sistemas Contables. *Revista de Arquitectura e Ingeniería*, VI(2), 1-14.
- Mi banco me Enseña, Banco del Pacífico*. (2015). Recuperado el 30 de 09 de 2017, de Mi banco me Enseña, Banco del Pacífico: <https://www.educacionfinanciera.com.ec/sistema-financiero-del-ecuador>
- Morilla, I. (2002). Auditoría informática, Nuevas tendencias. *Partida doble*, 150-155.
- O'Brien, J. (2001). *Sistemas de Información Gerencial*. Bogotá: McGraw.
- Omeba. (1988). *Enciclopedia Jurídica Omeba*. Recuperado el 19 de Enero de 2015, de http://www.omeba.com/voces.php?a=vv&doc_id=&l=D&ini=400
- Ortiz, M., & Pérez, V. (2004). *Léxico jurídico para estudiantes*. Madrid: TECNOS.

- Osorio, M. (2008). *Diccionario de Ciencias Jurídicas Políticas y Sociales*. Guatemala: Datascan S.A.
- Piattini, M. G., & Del Peso, E. (2005). *Auditoria Informática, un enfoque práctico*. Colombia: Alfaomega Grupo Editor.
- Piattini, M. G., & Del Peso, E. (2005). *Auditoria Informatica, Un enfoque práctico*. México, DF: Alfaomega, Grupo Editor S.A.
- Pinilla, J. (2005). *Auditoría Informática (Segunda ed.)*. Bogotá: Ecoe Ediciones.
- Prieto, A., & Martínez, M. (2004). Sistemas de información en las organizaciones: Una alternativa para mejorar la productividad. *Revista de Ciencias Sociales*, X(2), 322-337.
- Públicos, I. A. (1948). Statement on Auditing Standards (SAS). Instituto Americano de Contadores Públicos.
- Rivas, G. A. (1988). *AUDITORIA INFORMATICA*. Madrid: Ediciones DIAS DE SANTOS, S.A.
- Shuttleworth, M. (23 de Enero de 2008). *EXPLORABLE*. Recuperado el 31 de Diciembre de 2015, de <https://explorable.com/es/objetivos-de-la-investigacion>
- Superintendencia De Economía Popular Y Solidaria. (30 de Junio de 2015). *Superintendencia De Economía Popular Y Solidaria*. Recuperado el 29 de 12 de 2015, de Boletín Financiero: <http://www.seps.gob.ec/estadisticas?boletin-financiero>
- SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA. (30 de Noviembre de 2015). *SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA*. Recuperado el 30 de Diciembre de 2015, de <http://www.seps.gob.ec/estadisticas?boletines-mensuales-de-segmento-1>
- Torralba, F. (21 de Abril de 2013). *IESE, Business School*. Recuperado el 31 de Diciembre de 2015, de <http://blog.iese.edu/antonioorgandona/2013/04/21/confianza-en-las-instituciones/>
- Tus Finanzas*. (31 de 08 de 2015). Recuperado el 30 de 09 de 2017, de Tus Finanzas: <https://tusfinanzas.ec/blog/2015/08/31/la-estructura-del-sistema-financiero-ecuatoriano/>

Viloria, N. (2005). Factores que inciden en el sistema de control interno de una organización. *Actualidad Contable Faces*, VIII(11), 87-92.

Yanel Blanco, L. (2015). *Auditoria integral: normas y procedimientos*. Bogotá: Ecoe Ediciones.

AneXOS

ANEXO 1



UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE CONTABILIDAD Y AUDITORIA
DIRECCIÓN DE POSGRADOS
ENCUESTA



DIRIGIDO A: Auditores, Gerentes y Personal de Tecnologías de la información de las cooperativas de ahorro y crédito pertenecientes al segmento 1 de la ciudad de Ambato.

OBJETIVO: Conocer el grado de control de los sistemas de información que utiliza el Sector Cooperativo, segmento 1 de la ciudad de Ambato.

MOTIVACIÓN: Saludos cordiales le invitamos a contestar con la mayor seriedad el siguiente cuestionario a fin de obtener información valiosa y confiable, que será de uso oficial y de máxima confidencialidad.

INSTRUCCIONES:

- Procure ser lo más objetivo y veraz
- Seleccione solo una de las alternativas que se propone
- Marque con una X en el recuadro la alternativa que usted eligió

| Nro. | Pregunta | Respuesta |
|------|--|------------------|
| 1 | ¿Usted conoce los productos y servicios que brinda la Cooperativa? | SI () NO () |
| 2 | ¿En la Cooperativa se utiliza el procesamiento Electrónico de Datos (PED) a través del computador? | SI () NO () |
| 3 | ¿La Cooperativa utiliza los Sistemas de Información Computarizada (SIC)? | SI () NO () |
| 4 | ¿Los Sistemas de Información Computarizada (SIC) de la Cooperativa tienen licencias? | SI () NO () |
| 5 | ¿El auditor de la Cooperativa tiene conocimiento técnico de | SI () |

| | | | |
|----|--|-------|-----|
| | informática? | NO | () |
| 6 | ¿La Cooperativa ha identificado los riesgos operativos con claridad ? | SI | () |
| | | NO | () |
| 7 | ¿Se aplica Administración de Riesgos Operativos con respecto a las tecnologías de la información y comunicación en la cooperativa? | SI | () |
| | | NO | () |
| 8 | ¿Existe procedimientos para mitigar los riesgos Operativos con respecto a las Tecnologías de la información y comunicación? | SI | () |
| | | NO | () |
| 9 | ¿Los procedimientos para la administración de los riesgos operativos con respecto a la utilización de las tecnologías de la información y comunicación en la Cooperativa son los adecuados? | SI | () |
| | | NO | () |
| 10 | ¿Califique la importancia de la Administración de Riesgos Operativos con respecto a las tecnologías de la información y comunicación en las Cooperativas? | ALTO | () |
| | | MEDIO | () |
| | | BAJO | () |
| 11 | ¿Existe normativa que regule los riesgos operativos referentes a las tecnologías de la información y comunicación? | SI | () |
| | | NO | () |
| 12 | ¿La cooperativa tiene una unidad o departamento responsable de las Auditorías Informáticas? | SI | () |
| | | NO | () |
| 13 | ¿Cree usted que es importante la realización de Auditorías informáticas en las Cooperativas? | SI | () |
| | | NO | () |
| 14 | ¿En la cooperativa se han realizado auditorías a los sistemas de información y comunicación? | SI | () |
| | | NO | () |
| 15 | ¿Se han detectado intentos de accesos no autorizados o de terceras personas a los sistemas de la cooperativa? | SI | () |
| | | NO | () |
| 16 | ¿Conoce los niveles de riesgos que existe según la SEPS? | SI | () |
| | | NO | () |
| 17 | ¿Existe procedimientos en la Cooperativa para mitigar los riesgos? | SI | () |
| | | NO | () |
| 18 | ¿Cree usted que la Administración de Riesgos Operativos con relación a las Tecnologías de Información y comunicación mejoraría con una Normativa que obligue la creación de una Unidad de Auditoría informática en el Organigrama estructural de las Cooperativas de Ahorro y Crédito segmento 1 de la ciudad de Ambato? | SI | () |
| | | NO | () |

GRACIAS POR SU COLABORACIÓN..!!

ANEXO 2

TABLA T STUDENT

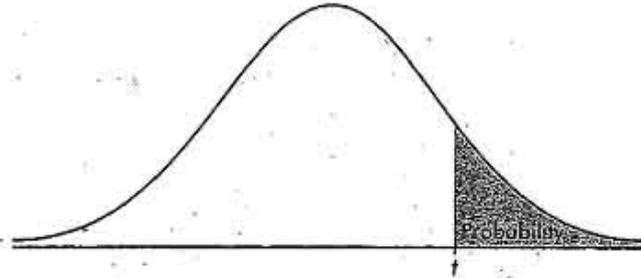


TABLE B: *t*-DISTRIBUTION CRITICAL VALUES

| df | Tail probability <i>p</i> | | | | | | | | | | | |
|------|---------------------------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| | .25 | .20 | .15 | .10 | .05 | .025 | .02 | .01 | .005 | .0025 | .001 | .0005 |
| 1 | 1.000 | 1.376 | 1.963 | 3.078 | 6.314 | 12.71 | 15.89 | 31.82 | 63.66 | 127.3 | 318.3 | 636.6 |
| 2 | .816 | 1.061 | 1.386 | 1.886 | 2.920 | 4.303 | 4.849 | 6.965 | 9.925 | 14.09 | 22.33 | 31.60 |
| 3 | .765 | .978 | 1.250 | 1.638 | 2.353 | 3.182 | 3.482 | 4.541 | 5.841 | 7.453 | 10.21 | 12.92 |
| 4 | .741 | .941 | 1.190 | 1.533 | 2.132 | 2.776 | 2.999 | 3.747 | 4.604 | 5.598 | 7.173 | 8.610 |
| 5 | .727 | .920 | 1.156 | 1.476 | 2.015 | 2.571 | 2.757 | 3.365 | 4.032 | 4.773 | 5.893 | 6.869 |
| 6 | .718 | .906 | 1.134 | 1.440 | 1.943 | 2.447 | 2.612 | 3.143 | 3.707 | 4.317 | 5.208 | 5.959 |
| 7 | .711 | .896 | 1.119 | 1.415 | 1.895 | 2.365 | 2.517 | 2.998 | 3.499 | 4.029 | 4.785 | 5.408 |
| 8 | .706 | .889 | 1.108 | 1.397 | 1.860 | 2.306 | 2.449 | 2.896 | 3.355 | 3.833 | 4.501 | 5.041 |
| 9 | .703 | .883 | 1.100 | 1.383 | 1.833 | 2.262 | 2.398 | 2.821 | 3.250 | 3.690 | 4.297 | 4.781 |
| 10 | .700 | .879 | 1.093 | 1.372 | 1.812 | 2.228 | 2.359 | 2.764 | 3.169 | 3.581 | 4.144 | 4.587 |
| 11 | .697 | .876 | 1.088 | 1.363 | 1.796 | 2.201 | 2.328 | 2.718 | 3.106 | 3.497 | 4.025 | 4.437 |
| 12 | .695 | .873 | 1.083 | 1.356 | 1.782 | 2.179 | 2.303 | 2.681 | 3.055 | 3.428 | 3.930 | 4.318 |
| 13 | .694 | .870 | 1.079 | 1.350 | 1.771 | 2.160 | 2.282 | 2.650 | 3.012 | 3.372 | 3.852 | 4.221 |
| 14 | .692 | .868 | 1.076 | 1.345 | 1.761 | 2.145 | 2.264 | 2.624 | 2.977 | 3.326 | 3.787 | 4.140 |
| 15 | .691 | .866 | 1.074 | 1.341 | 1.753 | 2.131 | 2.249 | 2.602 | 2.947 | 3.286 | 3.733 | 4.073 |
| 16 | .690 | .865 | 1.071 | 1.337 | 1.746 | 2.120 | 2.235 | 2.583 | 2.921 | 3.252 | 3.686 | 4.015 |
| 17 | .689 | .863 | 1.069 | 1.333 | 1.740 | 2.110 | 2.224 | 2.567 | 2.898 | 3.222 | 3.646 | 3.965 |
| 18 | .688 | .862 | 1.067 | 1.330 | 1.734 | 2.101 | 2.214 | 2.552 | 2.878 | 3.197 | 3.611 | 3.922 |
| 19 | .688 | .861 | 1.066 | 1.328 | 1.729 | 2.093 | 2.205 | 2.539 | 2.861 | 3.174 | 3.579 | 3.883 |
| 20 | .687 | .860 | 1.064 | 1.325 | 1.725 | 2.086 | 2.197 | 2.528 | 2.845 | 3.153 | 3.552 | 3.850 |
| 21 | .686 | .859 | 1.063 | 1.323 | 1.721 | 2.080 | 2.189 | 2.518 | 2.831 | 3.135 | 3.527 | 3.819 |
| 22 | .686 | .858 | 1.061 | 1.321 | 1.717 | 2.074 | 2.183 | 2.508 | 2.819 | 3.119 | 3.505 | 3.792 |
| 23 | .685 | .858 | 1.060 | 1.319 | 1.714 | 2.069 | 2.177 | 2.500 | 2.807 | 3.104 | 3.485 | 3.768 |
| 24 | .685 | .857 | 1.059 | 1.318 | 1.711 | 2.064 | 2.172 | 2.492 | 2.797 | 3.091 | 3.467 | 3.745 |
| 25 | .684 | .856 | 1.058 | 1.316 | 1.708 | 2.060 | 2.167 | 2.485 | 2.787 | 3.078 | 3.450 | 3.725 |
| 26 | .684 | .856 | 1.058 | 1.315 | 1.706 | 2.056 | 2.162 | 2.479 | 2.779 | 3.067 | 3.435 | 3.707 |
| 27 | .684 | .855 | 1.057 | 1.314 | 1.703 | 2.052 | 2.158 | 2.473 | 2.771 | 3.057 | 3.421 | 3.690 |
| 28 | .683 | .855 | 1.056 | 1.313 | 1.701 | 2.048 | 2.154 | 2.467 | 2.763 | 3.047 | 3.408 | 3.674 |
| 29 | .683 | .854 | 1.055 | 1.311 | 1.699 | 2.045 | 2.150 | 2.462 | 2.756 | 3.038 | 3.396 | 3.659 |
| 30 | .683 | .854 | 1.055 | 1.310 | 1.697 | 2.042 | 2.147 | 2.457 | 2.750 | 3.030 | 3.385 | 3.646 |
| 40 | .681 | .851 | 1.050 | 1.303 | 1.684 | 2.021 | 2.123 | 2.423 | 2.704 | 2.971 | 3.307 | 3.551 |
| 50 | .679 | .849 | 1.047 | 1.299 | 1.676 | 2.009 | 2.109 | 2.403 | 2.678 | 2.937 | 3.261 | 3.496 |
| 60 | .679 | .848 | 1.045 | 1.296 | 1.671 | 2.000 | 2.099 | 2.390 | 2.660 | 2.915 | 3.232 | 3.460 |
| 80 | .678 | .846 | 1.043 | 1.292 | 1.664 | 1.990 | 2.088 | 2.374 | 2.639 | 2.887 | 3.195 | 3.416 |
| 100 | .677 | .845 | 1.042 | 1.290 | 1.660 | 1.984 | 2.081 | 2.364 | 2.626 | 2.871 | 3.174 | 3.390 |
| 1000 | .675 | .842 | 1.037 | 1.282 | 1.646 | 1.962 | 2.056 | 2.330 | 2.581 | 2.813 | 3.098 | 3.300 |
| ∞ | .674 | .841 | 1.036 | 1.282 | 1.645 | 1.960 | 2.054 | 2.326 | 2.576 | 2.807 | 3.091 | 3.291 |
| | 50% | 60% | 70% | 80% | 90% | 95% | 96% | 98% | 99% | 99.5% | 99.8% | 99.9% |
| | Confidence level <i>C</i> | | | | | | | | | | | |