UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE TECNOLOGÍAS DE LA INFORMACIÓN, TELECOMUNICACIONES E INDUSTRIAL

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

Tema: "Análisis de Riesgos Informáticos en las Cooperativas de Ahorro y Crédito de los Segmentos 2 y 3 en la ciudad de Ambato utilizando COBIT 5"

Trabajo de Investigación, previo a la obtención del Grado Académico de Magister en Gerencia de Sistemas de Información

Autor: Ing. Christian Giovanny Barrera Barragán

Director: Ing. Franklin Oswaldo Mayorga Mayorga, Mg.

Ambato – Ecuador

2019

A la Unidad Académica de Titulación de la Facultad de Tecnologías de la Información, Telecomunicaciones e Industrial.

El Tribunal receptor del Trabajo de Investigación presidido por la Ingeniera Elsa Pilar Urrutia Urrutia, Mg., e integrado por los señores Ingeniero Carlos Israel Núñez Miranda, Mg., Ingeniero Edwin Hernando Buenaño Valencia, Mg., Ingeniero Félix Oscar Fernández Peña, Dr., designados por la Unidad Académica de Titulación de Posgrado de la Facultad de Tecnologías de la Información, Telecomunicaciones e Industrial de la Universidad Técnica de Ambato, para receptar el Trabajo de Investigación con el tema: "ANÁLISIS DE RIESGOS INFORMÁTICOS EN LAS COOPERATIVAS DE AHORRO Y CRÉDITO DE LOS SEGMENTOS 2 Y 3 EN LA CIUDAD DE AMBATO UTILIZANDO COBIT 5", elaborado y presentado por el señor Ingeniero Barrera Barragán Christian Giovanny, para optar por el Grado Académico de Magíster en Gerencia de Sistemas de Información; una vez escuchada la defensa oral del Trabajo de Investigación el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. Elsa Pilar Urrutia Urrutia, Mg.
Presidente del Tribunal

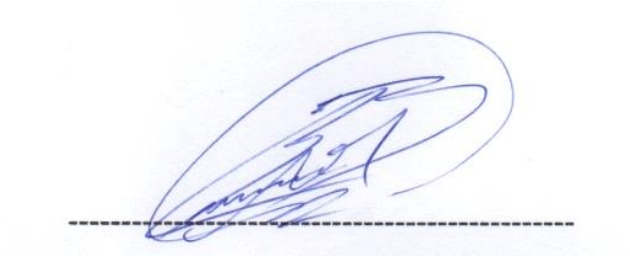
Ing. Carlos Israel Núñez Miranda, Mg.
Miembro del Tribunal

Ing. Edwin Hernando Buenaño Valencia, Mg.
Miembro del Tribunal

Ing. Félix Oscar Fernández Peña, PhD.
Miembro del Tribunal

AUTORÍA DEL TRABAJO DE INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Investigación con el tema: "Análisis de Riesgos Informáticos en las Cooperativas de Ahorro y Crédito de los Segmentos 2 y 3 en la ciudad de Ambato utilizando COBIT 5", le corresponde exclusivamente a: Ing., Christian Giovanny Barrera Barragán, Autor bajo la Dirección de Ing. Franklin Oswaldo Mayorga Mayorga Mg., Director del Trabajo de Investigación ; y el patrimonio intelectual a la Universidad Técnica de Ambato.



Ing. Christian Giovanny Barrera Barragán

c.c.1803038429

AUTOR

Ing. Franklin Oswaldo Mayorga Mayorga Mg.

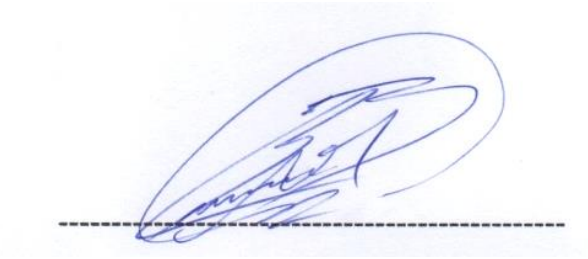
c.c.1802503993

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. Christian Giovanny Barrera Barragán

c.c.1803038429

ÍNDICE GENERAL

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

AGRADECIMIENTO

Agradezco primeramente a Dios y a la Santísima Virgen por sus múltiples bendiciones sobretodo en momentos difíciles dándome la fortaleza para continuar.

A mis padres que en todo momento me brindaron su apoyo.

A mi Director del trabajo de investigación por su acompañamiento y guía para el desarrollo de este trabajo.

DEDICATORIA

A mi padre que me guía desde el cielo, a mi madre que siempre me ha apoyado.

A mi esposa y mis hijos por ser mi inspiración y apoyo para cumplir mis metas.

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA DE TECNOLOGÍAS DE LA INFORMACIÓN, TELECOMUNICACIONES E INDUSTRIAL / DIRECCIÓN DE POSGRADO

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

TEMA:

"Análisis de Riesgos Informáticos en las Cooperativas de Ahorro y Crédito de los Segmentos 2 y 3 en la ciudad de Ambato utilizando COBIT 5."

AUTOR: Ing., Christian Giovanny Barrera Barragán

DIRECTOR: Ing., Franklin Oswaldo Mayorga Mayorga, Mg.

FECHA: junio de 2019

RESUMEN EJECUTIVO

Las instituciones financieras tienen gran responsabilidad con la sociedad, sobre todo porque la comunidad ha depositado su confianza en estas instituciones para guardar sus recursos económicos provenientes de sus trabajos, ahorros, etc. Está confianza obliga a que las entidades financieras tomen todas las medidas para resguardar de forma confiable la información que utilizan. La parte tecnológica no puede quedar aislada, por lo que es necesario que las entidades incorporen dentro de sus análisis de riesgos, los mecanismos necesarios para mitigar y controlar los riesgos pertinentes a la tecnología. Es necesario que las entidades financieras consideren dentro de su análisis de riesgos, al riesgo informático. Considerando la gran responsabilidad que tienen al manejar dinero de sus socios y clientes, deben aplicarse buenas prácticas a pesar de no existir normativas que les obligue. COBIT es una de las metodologías mayormente utilizadas a nivel internacional para la implementación de buenas prácticas y procesos de TI alineándose con varias metodologías como ITIL, Normas ISO de seguridad, entre otras; que permiten a las empresas establecer procesos conjuntamente entre la parte administrativa y de tecnología orientados al logro de metas empresariales. COBIT 5 se basa en cinco principios para el gobierno y la gestión de las TI empresariales, los cuales habilitan a las instituciones a construir un marco de gestión de gobierno y gestión efectivo que optimiza la inversión y el uso de información y tecnología. Con la implementación del marco de referencia COBIT 5 se pretende que las entidades financieras del sector popular y solidario establezcan procesos que permitan identificar y minimizar los riesgos que podrían amenazar la estabilidad institucional, infraestructura tecnológica y sobre todo la información. La presente propuesta, nace de la necesidad de dar solución a la problemática de investigación planteada la cual denota gran interés de aplicar una metodología para las buenas prácticas de TI por parte de las instituciones financieras del segmento 2 y 3 de la ciudad de Ambato.

Descriptores: COBIT, COBIT 5, gestión de TI, ISO de seguridad, instituciones financieras, riesgo informático, análisis de riesgo, TI empresariales, Economía popular y solidaria, metas empresariales.

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA DE TECNOLOGÍAS DE LA INFORMACIÓN, TELECOMUNICACIONES E INDUSTRIAL / DIRECCIÓN DE POSGRADO

MAESTRÍA EN GERENCIA DE SISTEMAS DE INFORMACIÓN

THEME:

"Análisis de Riesgos Informáticos en las Cooperativas de Ahorro y Crédito de los Segmentos 2 y 3 en la ciudad de Ambato utilizando COBIT 5."

AUTHOR: Ing., Christian Giovanny Barrera Barragán

DIRECTED BY: Ing., Franklin Oswaldo Mayorga Mayorga, Mg.

DATE: junio de 2019

EXECUTIVE SUMMARY

Financial institutions have a great responsibility with society, especially because the community has placed their trust in these institutions to save their economic resources from their jobs, savings, etc. This trust forces financial institutions to take all measures to reliably safeguard the information they use. The technological part can not be isolated, so it is necessary for the entities to incorporate, within their risk analysis, the necessary mechanisms to mitigate and control the risks pertinent to the technology. It is necessary for financial institutions to consider computer risk within their risk analysis. Considering the great responsibility they have when handling money from their partners and clients, good practices must be applied despite the lack of regulations that force them. COBIT is one of the most widely used methodologies at international level for the implementation of good IT practices and processes, aligning with several methodologies such as ITIL, ISO Security Standards, among others; that allow companies to establish processes jointly between the administrative part and technology aimed at achieving business goals. COBIT 5 is based on five principles for the governance and management of business IT, which enable institutions to build an effective governance and management management framework that optimizes investment and the use of information and technology. With the implementation of the COBIT 5 reference framework, it is intended that the financial institutions of the popular and solidary sector establish processes that identify and minimize the risks that could threaten institutional stability, technological infrastructure and, above all, information. The present proposal arises from the need to solve the research problem, which shows great interest in applying a methodology for good IT practices by the financial institutions of segment 2 and 3 of the city of Ambato.

Keywords: COBIT, COBIT 5, IT management, security ISO, financial institutions, computer risk, risk analysis, business IT, popular and solidarity economy, business goals.

INTRODUCCIÓN

El manejo de riesgos en las instituciones financieras generalmente se centraban en aspectos netamente financieros, sin embargo aspectos como robo de información, pérdida de datos, destrucción de infraestructura, manipulación de bases de datos, etc., ha dado lugar a que se emitan nuevas normativas por parte de las entidades de control que regulen el ambiente tecnológico, así como a la necesidad y obligatoriedad de las instituciones financieras de estar mejor preparados para afrontar una serie de eventos generadores de tensión como les descritos anteriormente, siendo de esta manera las instituciones financieras las responsables de una adecuada gestión de riesgos entre ellos el riesgo tecnológico. Entre las expectativas que tienen las áreas ejecutivas de las empresas actuales sobre el departamento de TI se encuentran las de incrementar el crecimiento de la institución financiera, reducir los costos, multiplicar las ganancias, y desarrollar un equipo de trabajo talentoso y capaz.

El alcance de las expectativas mencionadas provoca que las empresas estén bajo constante presión para lograr beneficios a través del uso efectivo de las TI. En este sentido, resulta fundamental mantener el riesgo vinculado a TI en un nivel aceptable, reduciendo costos y cumpliendo con las leyes, regulaciones y políticas pertinentes que cada vez son mayores. COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los participantes. Uno de los Principios de COBIT es el de satisfacer las necesidades de las partes interesadas, entre las cuales se encuentran la optimización de recursos y la disminución de riesgos tecnológicos.

Se entiende como partes interesadas a las partes:

- Externas: sociedad en general, clientes, proveedores.
- Internas: administración gobierno de la empresa, responsables de los procesos de negocios, responsables de la TI, responsables de cumplimiento, etc.

En las Cooperativas de Ahorro y Crédito de la ciudad de Ambato, específicamente las ubicadas dentro de los segmentos 2 y 3 según la calificación de la Superintendencia de

Economía Popular y Solidaria, se han enfocado en su mayoría en analizar los riesgos financieros dejando en segundo plano los riesgos tecnológicos (ver tabla 1)

RAZÓN SOCIAL	SEGMENTO	TIENE PROCESOS DE TI DEFINIDOS
COOPERATIVA DE AHORRO Y CREDITO INDIGENA SAC LTDA	SEGMENTO 2	NO
COOPERATIVA DE AHORRO Y CREDITO AMBATO LTDA	SEGMENTO 2	SI
COOPERATIVA DE AHORRO Y CREDITO KULLKI WASI LTDA	SEGMENTO 2	SI
COOPERATIVA DE AHORRO Y CREDITO CHIBULEO LTDA	SEGMENTO 2	SI
COOPERATIVA DE AHORRO Y CREDITO EDUCADORES DE TUNGURAHUA LTDA	SEGMENTO 3	NO
COOPERATIVA DE AHORRO Y CREDITO MAQUITA CUSHUN LTDA	SEGMENTO 3	NO
COOPERATIVA DE AHORRO Y CREDITO CREDIAMBATO LTDA	SEGMENTO 3	NO
COOPERATIVA DE AHORRO Y CREDITO CAMPESINA COOPAC	SEGMENTO 3	NO
COOPERATIVA DE AHORRO Y CREDITO SEMBRANDO UN NUEVO PAIS	SEGMENTO 3	NO
COOPERATIVA DE AHORRO Y CREDITO CRECER WIÑARI LTDA	SEGMENTO 3	NO

Tabla 1: Catastro de Cooperativas Segmentos 2 y 3 de la ciudad de Ambato
Fuente: SEPS – Investigador
Elaborado por: El autor

Por lo antes indicado surge la necesidad del presente trabajo de investigación, a través del cual se propone la implementación del Marco de Referencia COBIT 5 para identificar, mitigar, minimizar y monitorear los riesgos tecnológicos presentes en las Cooperativas de Ahorro y Crédito de los Segmentos 2 y 3 de la ciudad de Ambato, a fin de evitar problemas de pérdidas o fugas de información, pérdidas de servicio, etc.

El CAPÍTULO I, EL PROBLEMA contiene: el tema de investigación, el planteamiento del problema, su contexto, análisis crítico, prognosis, formulación del problema, interrogantes, delimitación, justificación y objetivos.

El CAPÍTULO II MARCO TEÓRICO establece: antecedentes de la investigación, fundamentación filosófica, fundamentación legal, categorías fundamentales, hipótesis y señalamiento de variables.

El CAPÍTULO III METODOLOGÍA menciona: el enfoque de investigación, modalidad básica de la investigación, nivel o tipo de investigación, población y muestra, operacionalización de variables, plan de recolección de información y plan de procesamiento de la información.

El CAPÍTULO IV, ANÁLISIS E INTERPRETACIÓN DE RESULTADOS abarca la tabulación y sus respectivos gráficos estadísticos de la encuesta aplicada al personal de las instituciones financieras, así como la comprobación de hipótesis.

El CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES constituye, la comprobación de cada objetivo específico y sus respectivas soluciones.

El CAPÍTULO VI PROPUESTA comprende la solución a la problemática de estudio planteada.

CAPÍTULO I
EL PROBLEMA DE INVESTIGACIÓN

1.1 Tema de Investigación

Análisis de Riesgos Informáticos en las Cooperativas de Ahorro y Crédito de los Segmentos 2 y 3 en la ciudad de Ambato utilizando COBIT 5.

1.2 Planteamiento del Problema

1.2.1 Contextualización

El uso de las tecnologías de la información se ha intensificado en las organizaciones independientemente de la naturaleza o actividad de las mismas, éstas se encuentran en constante evolución adaptándose a las nuevas necesidades de las organizaciones y así mismo dando lugar a otras relacionadas con su operación diaria. Castro & Bayona (2011, pág. 57)

El desarrollo y uso de metodologías integradas y ágiles para gestionar riesgos y en especial el tecnológico es importante con el fin de minimizar el impacto que pueda causar algún posible daño de la seguridad de la información. Castro & Bayona (2011, pág. 57)

El riesgo de origen tecnológico puede incidir sobre las metas y objetivos organizacionales y ser causa de otro tipo de riesgos al ser intrínseco al uso de tecnología. Por ello el daño, interrupción, alteración o falla derivada del uso de TI puede implicar pérdidas significativas en las organizaciones, pérdidas financieras, multas o acciones legales, afectación de la imagen de una organización y causar inconvenientes a nivel operativo y estratégico. Castro & Bayona (2011, pág. 57)

Hasta el momento el marco existente para gestión de riesgos lo conforman los estándares ISO 31000 (Risk management) y la ISO/IEC 27005 (Information security risk management), los cuales proveen lineamientos generales con los cuales se podría

desarrollar una guía más precisa orientada a la realidad actual de alguna organización. Castro & Bayona (2011, pág. 57)

De acuerdo al catastro de la Superintendencia de Economía Popular y Solidaria hasta junio del 2017, en el Ecuador existen 693 Cooperativas de Ahorro y Crédito activas, las cuales están clasificadas en cinco segmentos de acuerdo al monto de activos que poseen. Superintendencia de Economía Popular y Solidaria (2018)

En la Provincia de Tungurahua se encuentra un número importante de Cooperativas de Ahorro y Crédito, siendo la mayoría de tipo indígena, por lo que éste mercado se ha vuelto más competitivo. Villacres & Chacha (2015)

Estas cooperativas debido a sus actividades, enfrentan algunos riesgos, que pueden afectar su normal desenvolvimiento como son: Riesgo de Crédito, de Liquidez, de Mercado, Reputacional y Riesgo Operativo. Criollo (2016)

El Riesgo Operativo, es uno de los más importantes, sin embargo no se lo considera como tal dentro de las Cooperativas de Ahorro y Crédito. Esta falta de control puede producir cuantiosas pérdidas en las instituciones financieras. Por tal razón es de vital importancia detectar oportunamente las vulnerabilidades potenciales y crear controles para minimizar la posibilidad de que se materialicen. Salazar & Esparza (2016)

En la ciudad de Ambato existen 10 cooperativas de ahorro y crédito ubicadas dentro de los segmentos 2 y 3, según el catastro de organizaciones publicado por la Superintendencia de Economía Popular y Solidaria. Como resultado de análisis realizados mediante encuestas al personal de tecnología de cada Cooperativa, se observa que el 70% de estas organizaciones no han implementado procesos para una adecuada administración de la información y de la tecnología que se requiere para el manejo de la misma. Superintendencia de Economía Popular y Solidaria (2018)

1.2.2 Análisis Crítico

Las partes administrativas de las Cooperativas de Ahorro y Crédito, tienen poco interés por potenciar su área de tecnología, principalmente debido a los costos que conlleva una implementación de recursos tecnológicos confiables y seguros. Esto puede dar

como resultado que la información que guarda la empresa y que debe ser considerada como información sensible, se encuentre en una situación que pueda alterar su integridad y confiabilidad. Perjudicando no solamente a las empresas sino a las personas dueñas de esta información.

Una institución, como una entidad financiera, que no tiene entre sus objetivos garantizar la información de sus clientes, corre el riesgo de que éstos no tengan la confianza suficiente como para depositar sus ahorros y sus datos personales.

1.2.3 Prognosis

Una institución financiera que no establezca dentro de sus políticas los procesos que ayuden a minimizar sus riesgos tecnológicos, será demasiado vulnerable con la información que está obligada a manejar. El no aplicar adecuadamente algún modelo de referencia como por ejemplo COBIT 5 para identificar los riesgos tecnológicos que pudieren afectar a la empresa, prácticamente provocaría que la institución se maneje tecnológicamente de forma desordenada con el alto riesgo de que su información no sea cuidadosamente resguardada pudiendo provocar un gravísimo impacto de desconfianza y pánico en la sociedad si sus datos se vieran comprometidos.

Cuando las entidades financieras incorporen dentro de sus políticas la aplicación de los procesos que identifiquen y minimicen los riesgos tecnológicos, podrán brindar mayor seguridad hacia sus socios y a su propio personal, con la confianza de que su información será manejada de una forma confiable y segura considerándola como uno de los bienes más valiosos para la institución.

1.2.4 Formulación del Problema

¿Cuál sería el impacto de los riesgos informáticos en las Cooperativas de Ahorro y Crédito de los Segmentos 2 y 3 de la ciudad de Ambato implementando la metodología COBIT 5.?

1.2.5 Interrogantes (Sub problemas)

- ¿Cuáles son los niveles de riesgo informático en las Cooperativas de Ahorro y Crédito de la ciudad de Ambato?

- ¿Cuál es la situación actual de los procesos y beneficios de las TI actualmente empleadas en las Cooperativas de Ahorro y Crédito de la ciudad de Ambato?

- ¿Cuáles son los procesos más adecuados para disminuir los niveles de riesgos informáticos utilizando la metodología Cobit 5?

- ¿La aplicación de la metodología COBIT 5 reducirá el impacto de los riesgos informáticos en las Cooperativas de Ahorro y Crédito de los segmentos 2 y 3 de la ciudad de Ambato?.

1.2.6 Delimitación del objeto de investigación

Campo: Financiero Cooperativo
Área: Tecnología de la Información
Aspecto: Análisis de procesos de análisis de riesgos tecnológicos.

1.2.6.1 Delimitación Espacial:

Cooperativa de Ahorro y Crédito Indígena SAC Ltda.

1.2.6.2 Delimitación Temporal:

Seis meses a partir de la aprobación del proyecto.

1.2.6.3 Unidades de Observación:

Cooperativa de Ahorro y Crédito Indígena SAC Ltda.

1.3 Justificación

Las instituciones financieras tienen gran responsabilidad con la sociedad, sobre todo porque la comunidad ha depositado su confianza en estas instituciones para guardar sus recursos económicos provenientes de sus trabajos, ahorros, etc.

Está confianza obliga a que las entidades financieras tomen todas las medidas para resguardar de forma confiable la información que utilizan. La parte tecnológica no puede quedar aislada, por lo que es necesario que las entidades incorporen dentro de

sus análisis de riesgos, los mecanismos necesarios para mitigar y controlar los riesgos pertinentes a la tecnología.

El organismo encargado de establecer políticas para las todas entidades financieras del Ecuador es la "Junta de Política y Regulación Monetaria y Financiera", y el organismo de control y regulación de las Cooperativas de Ahorro y Crédito es la Superintendencia de Economía Popular y Solidaria. Sin embargo hasta el momento ninguno de los dos organismos ha establecido políticas o normativas referentes al control del ambiente y riesgo informático.

Al no contar con una normativa para solventar el riesgo tecnológico, varias Cooperativas de Ahorro y Crédito no se han preocupado de definir procesos, presupuestos, planes, manuales de seguridad que considere a la tecnología como parte esencial de la institución, dejando a la deriva y talvez sin un plan de reacción en caso de sufrir un fallo de sus servidores, cuarto de equipos o robo de información.

Es necesario que las entidades financieras consideren dentro de su análisis de riesgos, al riesgo informático. Considerando la gran responsabilidad que tienen al manejar dinero de sus socios y clientes, deben aplicarse buenas prácticas a pesar de no existir normativas que les obligue.

COBIT es una de las metodologías mayormente utilizadas a nivel internacional para la implementación de buenas prácticas y procesos de TI alineándose con varias metodologías como ITIL, Normas ISO de seguridad, entre otras; que permiten a las empresas establecer procesos conjuntamente entre la parte administrativa y de tecnología orientados al logro de metas empresariales.

COBIT 5 se basa en cinco principios para el gobierno y la gestión de las TI empresariales, los cuales habilitan a las instituciones a construir un marco de gestión de gobierno y gestión efectivo que optimiza la inversión y el uso de información y tecnología.

"Un proceso se define como una colección de prácticas influenciadas por las políticas y procedimientos de la empresa que toma entradas de un número dado de fuentes incluyéndose otros procesos, manipulando las entradas y produciendo salidas (p. ej., productos, servicios)." (COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa)

Con la implementación del marco de referencia COBIT 5 se pretende que las entidades financieras del sector popular y solidario establezcan procesos que permitan identificar y minimizar los riesgos que podrían amenazar la estabilidad institucional, infraestructura tecnológica y sobre todo la información.

1.4 Objetivos

1.4.1 Objetivo General

Realizar un análisis del impacto de los riesgos informáticos en las Cooperativas de Ahorro y Crédito de los Segmentos 2 y 3 de la ciudad de Ambato implementando la metodología COBIT 5.

1.4.2 Objetivos Específicos:

- Identificar los niveles de riesgo informático en las Cooperativas de Ahorro y Crédito de la ciudad de Ambato.

- Analizar la situación actual de los procesos y beneficios de las TI actualmente empleadas en las Cooperativas de Ahorro y Crédito de la ciudad de Ambato.

- Definir los procesos más adecuados para disminuir los niveles de riesgos informáticos utilizando la metodología Cobit 5.

- Aplicar la metodología COBIT 5 para reducir el impacto de los riesgos informáticos en las Cooperativas de Ahorro y Crédito de los segmentos 2 y 3 de la ciudad de Ambato.

CAPÍTULO II
MARCO TEÓRICO

2.1 Antecedentes Investigativos

Luego de efectuar una revisión y análisis bibliográfico, de investigaciones relacionadas a la administración de riesgos y al uso de la Metodología COBIT se encuentran diversos conceptos, entre los cuales se rescatan:

Según Larrea (2013) en su trabajo de investigación ubicado en el Repositorio de la Universidad Técnica de Ambato, "El Riesgo Operativo y su impacto en el Control Interno del Banco Nacional de Fomento Sucursal Ambato", en el año 2013 en la que se trata la importancia de la administración del riego operativo en las instituciones financieras sobre todo en el entendimiento de que una adecuada gestión de riesgos busca la protección de los recursos de una entidad y el logro de sus objetivos, en dicha investigación, y luego de su trabajo de investigación concluye y recomienda:

- Implantar una metodología de gestión de riesgo operativo que permita controlar adecuadamente y reaccionar a las condiciones y circunstancias que puedan afectar el sistema de control interno.

- La identificación de riesgo operacional es fundamental para el posterior desarrollo de un sistema viable de control y seguimiento del mismo.

Según Domínguez (2009) de la Escuela Superior Politécnica del Litoral, en su trabajo de investigación "Creación de un Marco de Control para la Administración del Riesgo Operativo relacionado con la Tecnología de Información como modelo para las Cooperativas de Ahorro y Crédito del Ecuador", donde uno de sus objetivos es el de establecer los lineamientos de control para la Gestión Integral de Riesgos tecnológicos en las Cooperativas de Ahorro y Crédito del Ecuador bajo las normas internacionales vigentes y aquellas establecidas por la Superintendencia de Bancos y Seguros del Ecuador, concluye:

- Es posible dentro de las Cooperativas de Ahorro y Crédito crear un marco de control integral para la administración del riesgo tecnológico, basado en las directrices de COSO-ERM, ISO 27001, COBIT y la Resolución 834 que garantice la seguridad de la información, la salvaguarda de los recursos tecnológicos y la continuidad del negocio.

Para Guerra (2015) de la Escuela Politécnica del Ejército, en su Tesis "La Mejores prácticas aplicadas a un Análisis de Riesgos de seguridad de la información para las Entidades Financieras Controladas por La Superintendencia de Economía Popular y Solidaria (Cooperativas de Ahorro y Crédito) que conforman el grupo de Asistencia Tecnológica Cooperativa (Asistecooper)", menciona que para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo las instituciones deben generar políticas y procedimientos referentes a :

- Administración de las Tecnologías de la información.
- Control de las tecnologías de la información
- Control de proveedores tecnológicos

Considera que la mejor metodología para llevar a cabo estas tareas es COBIT.

2.2 Fundamentación Filosófica

Como menciona Aguilar (2011, pág. 344) La indagación del tema de investigación se sitúa en el paradigma crítico propositivo, porque conlleva el enfoque social crítico, donde cuestiona los esquemas sociales para proponer alternativas de solución, mismas que son planteadas en un clima de sinergia y pro actividad, utilizando herramientas o técnicas como la observación, interpretación y la comprensión de los fenómenos sociales en toda su complejidad.

2.3 Fundamentación Legal

Como menciona Asamblea Constituyente (2008) El presente trabajo de investigación se sustenta en las siguientes leyes y normativas:

CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR
SECCIÓN OCTAVA
SISTEMA FINANCIERO

Art. 309.- El sistema financiero nacional se compone de los sectores público, privado, y del popular y solidario, que intermedian recursos del público. Cada uno de estos sectores contará con normas y entidades de control específicas y diferenciadas, que se encargarán de preservar su seguridad, estabilidad, transparencia y solidez. Estas entidades serán autónomas. Los directivos de las entidades de control serán responsables administrativa, civil y penalmente por sus decisiones.
Concordancias: CONSTITUCION DE LA REPUBLICA DEL ECUADOR, Arts. 310, 311, 312 CODIGO ORGANICO MONETARIO Y FINANCIERO, LIBRO I, Arts. 6, 160, 161, 162, 163, 274

Art.311.- El sector financiero popular y solidario se compondrá de cooperativas de ahorro y crédito, entidades asociativas o solidarias, cajas y bancos comunales, cajas de ahorro. Las iniciativas de servicios del sector financiero popular y solidario, y de las micro, pequeñas y medianas unidades productivas, recibirá un tratamiento diferenciado y preferencial del Estado, en la medida en que se impulsen el desarrollo de la economía popular y solidaria.
Concordancias: LEY ORGANICA DEL SISTEMA NACIONAL DE CONTRATACION PUBLICA, Arts. 67 LEY ORGANICA DE ECONOMIA POPULAR Y SOLIDARIA, Arts. 1, 2, 8, 9, 78, 132 CODIGO ORGANICO MONETARIO Y FINANCIERO, LIBRO I, Arts. 160, 163

Mediante resolución No. JB-2005-834 de 20 de octubre de 2005, la Superintendencia de Bancos y Seguros (SBS) emitió la norma "De la Gestión del Riesgo Operativo". En el Libro I "Normas Generales para las Instituciones del Sistema Financiero", dice:

CAPÍTULO I.- De la Gestión integral y Control de riesgos
Sección I.- Alcance y Definiciones
Articulo 1.- "Las instituciones del sistema financiero controladas por la Superintendencia de Bancos y Seguros, deberán establecer esquemas eficientes y efectivos de administración y control de todos los riesgos a los que se encuentran expuestas en el desarrollo del negocio, conforme su objeto social, sin perjuicio del cumplimiento de las obligaciones que sobre la materia establezcan otras normas especiales y/o particulares. La administración integral de riesgos es parte de la estrategia institucional y del proceso de toma de decisiones."

Sección II - Administración de Riesgos
Artículo 3.- "Las instituciones del sistema financiero tienen la responsabilidad de administrar sus riesgos, a cuyo efecto deben contar con procesos formales de

administración integral de riesgos que permitan identificar, medir, controlar / mitigar y monitorear las exposiciones de riesgo que están asumiendo…".
Artículo 5.- "Una vez identificados los riesgos deben ser cuantificados o medidos con el objeto de determinar el cumplimiento de las políticas, los límites fijados y el impacto económico en la organización, permitiendo a la administración disponer los controles o correctivos necesarios…".
Articulo 8.- "El proceso que se implante en la institución para la administración integral de riesgos deberá ser permanentemente revisado y actualizado. Una adecuada administración integral de riesgos debe incluir, al menos lo siguiente, de acuerdo con la complejidad y tamaño de cada institución:
8.1 "Estrategia de negocio de la entidad, que incluirá los criterios de aceptación de riesgos en función del mercado objetivo determinado y de las características de los productos diseñados para atenderlos. Dicha estrategia deberá contar con fundamentos teóricos y empíricos adecuados y estará debidamente documentada;…"
8.5 "Sistemas de información que establezcan los mecanismos para elaborar e intercambiar información oportuna, confiable, fidedigna, tanto interna como externa".

CAPÍTULO V.- De La Gestión Del Riesgo Operativo

Según República del Ecuador Superintendencia de Bancos (2005) **ARTÍCULO 2.-** Para efectos de la aplicación de las disposiciones del presente capítulo, se considerarán las siguientes definiciones:

2.1 Alta gerencia.- La integran los presidentes y vicepresidentes ejecutivos, gerentes generales, vicepresidentes o gerentes departamentales, entre otros, responsables de ejecutar las disposiciones del directorio u organismo que haga sus veces, quienes toman decisiones de alto nivel, de acuerdo con las funciones asignadas y la estructura organizacional definida en cada institución controlada;

2.2 Evento de riesgo operativo.- Es el hecho que puede derivar en pérdidas financieras para la institución controlada;

2.3 Factor de riesgo operativo.- Es la causa primaria o el origen de un evento de riesgo operativo. Los factores son los procesos, personas, tecnología de la información y eventos externos; (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

2.6 Proceso crítico.- Es el indispensable para la continuidad del negocio y las operaciones de la institución controlada, y cuya falta de identificación o aplicación deficiente puede generarle un impacto financiero negativo;

2.13 Información crítica.- Es la información considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones;

2.14 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 por medios electrónicos o presentado en imágenes;

2.15 Tecnología de la información.- Es el conjunto de herramientas y métodos empleados 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; (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

2.18 Responsable de la información.- Es la persona encargada de cuidar la integridad, confidencialidad y disponibilidad de la información; debe tener autoridad para especificar y exigir las medidas de seguridad necesarias para cumplir con sus responsabilidade**s**; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

2.19 Seguridad de la información.- Son los mecanismos implantados que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella;

2.20 Seguridades lógicas.- Se refieren a la seguridad en el uso del software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información;

2.21 Confidencialidad.- Es la garantía de que sólo el personal autorizado accede a la información preestablecida;

2.22 Integridad.- Es la garantía de mantener la totalidad y exactitud de la información y de los métodos de procesamiento;

2.23 Disponibilidad.- Es la garantía de que los usuarios autorizados tienen acceso a la información cada vez que lo requieran a través de los medios adecuados que satisfagan sus necesidades;

2.24 Cumplimiento.- Se refiere a la observancia de las leyes, regulaciones y acuerdos contractuales a los que los procesos de las instituciones controladas están sujetos;

2.25 Pista de auditoría.- Es el registro de datos lógicos de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el propósito de mantener información histórica para fines de control, supervisión y auditoría;

2.29 Plan de continuidad.- Está orientado a asegurar la continuidad del negocio, la satisfacción del cliente y la productividad a pesar de eventos inesperados. Se ejecuta permanentemente como parte de la administración de riesgos. Un plan de continuidad debe contener procedimientos que se ajusten a la realidad del negocio de cada institución; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

2.30 Administración de la continuidad.- Es un proceso permanente que garantiza la continuidad de las operaciones del negocio de las instituciones del sistema financiero, a través de la efectividad del mantenimiento del plan de continuidad; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

2.31 Eficacia.- Es la capacidad para contribuir al logro de los objetivos institucionales de conformidad con los parámetros establecidos;

2.32 Eficiencia.- Es la capacidad para aprovechar racionalmente los recursos disponibles en pro del logro de los objetivos institucionales, procurando la optimización de aquellos y evitando dispendios y errores;

2.33 Calidad de la información.- Es el resultado de la aplicación de los mecanismos implantados que garantizan la efectividad, eficiencia y confiabilidad de la información y los recursos relacionados con ella; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.34 Efectividad.- Es la garantía de que la información es relevante y pertinente y que su entrega es oportuna, correcta y consistente; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.35 Confiabilidad.- Es la garantía de que la información es la apropiada para la administración de la entidad, ejecución de transacciones y para el cumplimiento de sus obligaciones; (incluido con resolución No. JB-2012-2148 de 26 de abril del 2012)

2.43 Incidente de tecnología de la información.- Evento asociado a posibles fallas en la tecnología de la información, fallas en los controles, o situaciones con probabilidad significativa de comprometer las operaciones del negocio; y, (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

2.44 Incidente de seguridad de la información.- 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. (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

De acuerdo con lo dispuesto en el numeral 2 del artículo 18 del Código Civil, los términos utilizados en la definición de riesgo legal se entenderán en su sentido natural y obvio, según el uso general de las mismas palabras, a menos de que tengan definiciones diferentes expresadas en la ley, reglamentos y demás normativa. (incluido con resolución No. JB-2008-1202 de 23 de octubre del 2008)

ARTÍCULO 3.- Para efectos del presente capítulo, el riesgo operativo se entenderá como la posibilidad de que se ocasionen pérdidas financieras por eventos derivados de fallas o insuficiencias en los procesos, personas, tecnología de la información y por eventos externos. (Reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014).

SECCIÓN II.- FACTORES DEL RIESGO OPERATIVO

Para la República del Ecuador Superintendencia de Bancos (2005) **En el Artículo 4.-** Con el propósito de que se minimice la probabilidad de incurrir en pérdidas financieras atribuibles al riesgo operativo, deben ser adecuadamente administrados los siguientes aspectos, los cuales se interrelacionan entre sí:

4.1 Procesos.- Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, las instituciones controladas deben contar con procesos definidos de conformidad con la estrategia y las políticas adoptadas, que deberán ser agrupados de la siguiente manera:

4.1.1 Procesos gobernantes o estratégicos.- Se considerarán a aquellos que proporcionan directrices a los demás procesos y son realizados por el directorio u organismo que haga sus veces y por la alta gerencia para poder cumplir con los objetivos y políticas institucionales. Se refieren a la planificación estratégica, los lineamientos de acción básicos, la estructura organizacional, la administración integral de riesgos, entre otros;

4.1.2 Procesos productivos, fundamentales u operativos.- Son los procesos esenciales de la entidad destinados a llevar a cabo las actividades que permitan ejecutar efectivamente las políticas y estrategias relacionadas con la calidad de los productos o servicios que ofrecen a sus clientes; y,

4.1.3 Procesos habilitantes, de soporte o apoyo.- Son aquellos que apoyan a los procesos gobernantes y productivos, se encargan de proporcionar personal competente, reducir los riesgos del trabajo, preservar la calidad de los materiales, equipos y herramientas, mantener las condiciones de operatividad y funcionamiento, coordinar y controlar la eficacia del desempeño administrativo y la optimización de los recursos.

Identificados los procesos críticos, se implantarán mecanismos o alternativas que ayuden a la entidad a evitar incurrir en pérdidas o poner en riesgo la continuidad del negocio y sus operaciones.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas para un adecuado diseño, control, actualización y seguimiento de los procesos.

Las políticas deben referirse por lo menos a: (i) diseño claro de los procesos, los cuales deben ser adaptables y dinámicos; (ii) descripción en secuencia lógica y ordenada de las actividades, tareas, y controles; (iii) determinación de los responsables de los procesos, que serán aquellas personas encargadas de su correcto funcionamiento, a través de establecer medidas y fijar objetivos para gestionarlos y mejorarlos, garantizar que las metas globales se cumplan, definir los límites y alcance, mantener contacto con los clientes internos y externos del proceso para garantizar que se satisfagan y se conozcan sus expectativas, entre otros; (iv) difusión y comunicación de los procesos buscando garantizar su total aplicación; y, (v) actualización y mejora continua a través del seguimiento permanente en su aplicación.

Deberá existir una adecuada separación de funciones que evite concentraciones de carácter incompatible, entendidas éstas como aquellas tareas cuya combinación en las competencias de una sola persona, eventualmente, podría permitir la realización o el ocultamiento de fraudes, errores, omisiones u otros eventos de riesgo operativo.

Las instituciones controladas deberán mantener inventarios actualizados de los procesos existentes, que cuenten, como mínimo con la siguiente información: tipo de proceso (gobernante, productivo y de apoyo), nombre del proceso, responsable, productos y servicios que genera el proceso, clientes internos y externos, fecha de aprobación, fecha de actualización, además de señalar si se trata de un proceso crítico.

4.2 Personas.- Las instituciones 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 apropiado ambiente de gestión de riesgo operativo, las instituciones 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 institución.

Dichos procesos corresponden a:

4.2.1 Los procesos de incorporación.- Que comprenden la planificación de necesidades, el reclutamiento, la selección, la contratación e inducción de nuevo personal;

4.2.2 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; la existencia de un sistema de evaluación del desempeño; desarrollo de carrera; rendición de cuentas; e incentivos que motiven la adhesión a los valores y controles institucionales.

4.2.3 Los procesos de desvinculación.- Que comprenden la planificación de la salida del personal por causas regulares, preparación de aspectos jurídicos para llegar al finiquito y la finalización de la relación laboral.

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.

Las instituciones controladas deberán analizar su organización con el objeto de evaluar si han definido el personal necesario y las competencias idóneas para el desempeño de cada puesto, considerando no sólo experiencia profesional, formación académica, sino también los valores, actitudes y habilidades personales que puedan servir como criterio para garantizar la excelencia institucional.

Las instituciones controladas mantendrán información actualizada del capital humano, que permita una adecuada toma de decisiones por parte de los niveles directivos y la realización de análisis cualitativos y cuantitativos de acuerdo con sus necesidades.

Dicha información deberá referirse al personal existente en la institución; a la formación académica y experiencia; a la forma y fechas de selección, reclutamiento y contratación; información histórica sobre los eventos de capacitación en los que han participado; cargos que han desempeñado en la institución; resultados de evaluaciones realizadas; fechas y causas de separación del personal que se ha desvinculado de la institución; y, otra información que la institución controlada considere pertinente.

4.3 Tecnología de la información.- Las instituciones controladas deben contar con la tecnología de la información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones. (reformado con resolución No. JB- 2014-3066 de 2 de septiembre del 2014)

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir políticas, procesos, procedimientos y metodologías que aseguren una adecuada planificación y administración de la tecnología de la información. (inciso reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Dichas políticas, procesos, procedimientos y metodologías se referirán a: (inciso reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.1 Con el objeto de garantizar que la administración de la tecnología de la información soporte adecuadamente los requerimientos de operación actuales y futuros de la entidad, las instituciones controladas deben contar al menos con lo siguiente: (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.1.1 El apoyo y compromiso formal del directorio u organismo que haga sus veces y la alta gerencia, a través de la asignación de recursos para el cumplimiento de los objetivos tecnológicos; (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.1.2 En función del tamaño y complejidad de las operaciones, las entidades deben conformar el comité de tecnología, que es el responsable de planificar, coordinar y supervisar las actividades de tecnología. El directorio asumirá las responsabilidades del comité de tecnología en las entidades que decidieran no conformarlo. La Superintendencia de Bancos y Seguros podrá disponer la conformación de este comité, si las condiciones de tamaño y complejidad de la entidad lo amerita. (numeral incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Dicho comité debe estará integrado como mínimo por: un delegado del directorio, quien lo presidirá, el representante legal de la institución y el funcionario responsable del área de tecnología;

4.3.1.3 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; (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.1.4 Tecnología de la información acorde a las operaciones del negocio y al volumen de transacciones, monitoreada y proyectada según las necesidades y crecimiento de la institución, con su correspondiente portafolio de proyectos tecnológicos a ejecutarse en el corto, mediano y largo plazo; (reformado con resolución No. JB- 2014-3066 de 2 de septiembre del 2014)

4.3.1.5 Políticas, procesos, procedimientos y metodologías de tecnología de la información 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 institución, así como las consecuencias de la violación de éstas. (numeral sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Los procesos, procedimientos y metodologías de tecnología de la información deben ser revisados por el comité de tecnología y propuestos para la posterior aprobación del directorio o el organismo que haga sus veces;

4.3.1.6 Difusión y comunicación a todo el personal involucrado de las mencionadas políticas, procesos, procedimientos y metodologías, de tal forma que se asegure su implementación; y, (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.1.7 Una metodología de administración de proyectos que considere al menos su planificación, ejecución, control y cierre, enfocada en la optimización de recursos y la gestión de riesgos. (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.2 Con el objeto de garantizar que las operaciones de tecnología de la información satisfagan los requerimientos de la entidad, las instituciones controladas deben contar al menos con lo siguiente: (reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.2.1 Procedimientos que establezcan las actividades y responsables de la operación y el uso de las instalaciones de procesamiento de información; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.2.2 Procedimientos de gestión de incidentes de tecnología de la información, que considere al menos su registro, priorización, análisis, escalamiento y solución; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.2.3 Inventario de la infraestructura tecnológica que considere por lo menos, su registro, responsables de uso y mantenimiento; y, (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.2.4 Procedimientos de respaldo de información periódicos, acorde a los requerimientos de continuidad del negocio que incluyan la frecuencia de verificación, las condiciones de preservación y eliminación y el transporte seguro hacia una ubicación remota, que no debe estar expuesto a los mismos riesgos del sitio principal. (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3 Con el objeto de garantizar que el proceso de adquisición, desarrollo, implementación y mantenimiento de las aplicaciones satisfagan los objetivos del negocio, las instituciones controladas deben contar al menos con lo siguiente:

4.3.3.1 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; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.2 Un documento que refleje el alcance de los requerimientos funcionales; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.3 Un documento que refleje los requerimientos técnicos y la relación y afectación a la capacidad de la infraestructura tecnológica actual; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.4 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; (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.5 Escaneo de vulnerabilidades en código fuente para identificar el nivel de riesgo del ambiente de la aplicación y en aplicaciones puestas en producción; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.6 Pruebas técnicas y funcionales que reflejen la aceptación de los usuarios autorizados; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.7 Procedimientos de control de cambios que considere su registro, manejo de versiones, segregación de funciones y autorizaciones e incluya los cambios emergentes; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.8 Documentación técnica y de usuario permanentemente actualizada de las aplicaciones de la institución; y, (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.3.9 Procedimientos de migración de la información, que incluyan controles para garantizar las características de integridad, disponibilidad y confidencialidad. (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.4 Con el objeto de garantizar que la infraestructura tecnológica que soporta las operaciones sea administrada, monitoreada y documentada, las instituciones

controladas deben contar al menos con: (sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.4.1 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; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.4.2 Un documento de análisis de la capacidad y desempeño de la infraestructura tecnológica que soporta las operaciones del negocio, que debe ser conocido y analizado por el comité de tecnología 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; (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.4.3 Procedimientos de migración de la plataforma tecnológica, que incluyan controles para garantizar la continuidad del servicio; e, (incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.3.4.4 Instalaciones de procesamiento de información crítica en 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. (Incluido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

La Resolución No. 128-2015-F de la Junta de Política y Regulación Monetaria y Financiera dice:

Sección VI. Elementos para la administración integral de riesgos
Como menciona la República del Ecuador Superintendencia de Bancos (2005) **En su Artículo 20.- Sistema de Información**: "Las entidades de los segmentos 1, 2, y cajas centrales deberán disponer de un sistema de información capaz de proveer a la administración y a las áreas involucradas, la información necesaria para identificar, medir, priorizar, controlar, mitigar y monitorear las exposiciones de riesgo, considerando parámetros de metodologías propias de esta gestión. Esta información deberá apoyar la toma de decisiones oportunas y adecuadas. El alcance y nivel de especialización del sistema estará en relación con el volumen de las transacciones de la entidad…"

Categorías Fundamentales

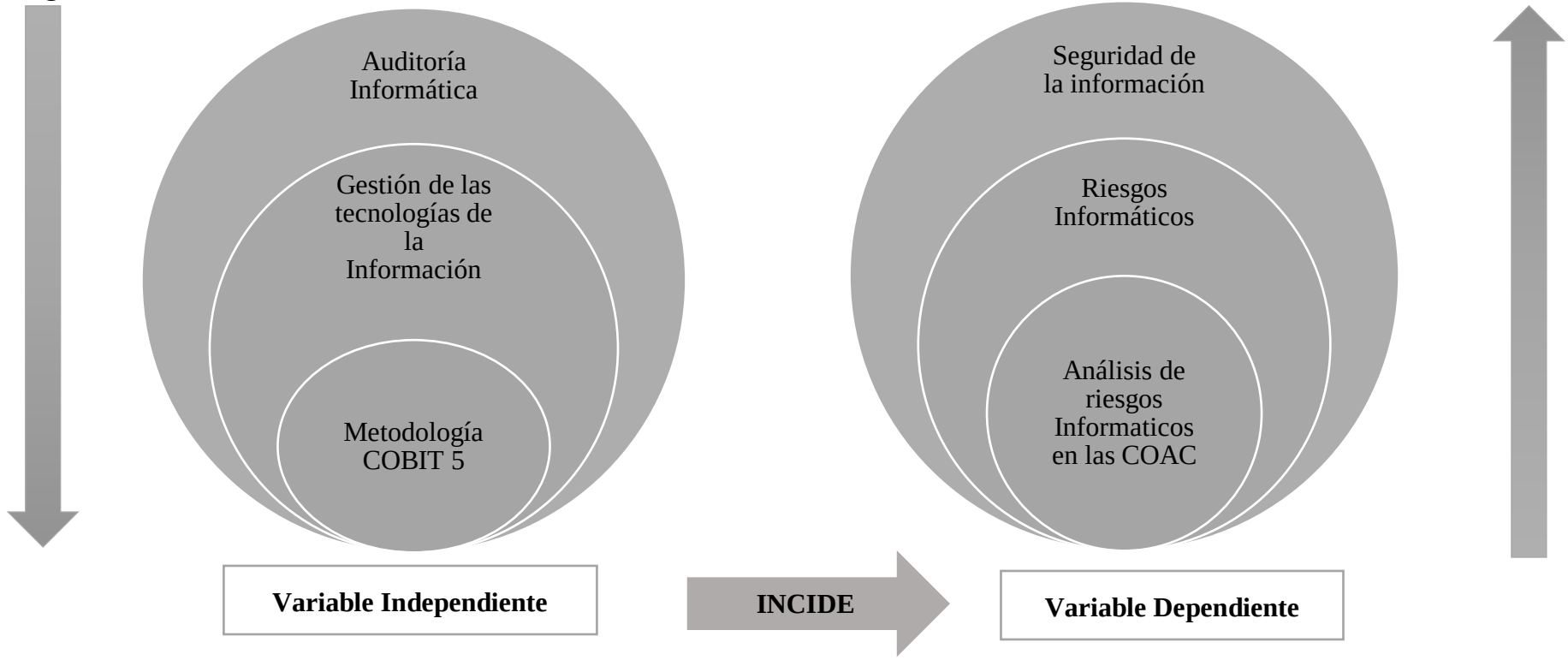


Gráfico 1: Categorías Fundamentales
Elaborador por: El autor

2.4 Categorías Fundamentales

Auditoría Informática

Para Rivas (1889, pág. 40) La auditoría informática es un examen metódico del servicio informático o de un sistema informático en particular, realizado de una forma puntual y de modo discontinuo a instancias de la dirección, con la intención de ayudar a mejorar conceptos como la seguridad, la eficacia y la rentabilidad del servicio o del sistema que resultan auditados. En esta definición hay cuatro palabras que destacan sobremanera: examen, metódico, puntual, discontinuo. Esta relevancia podrían justificar diciendo que la auditoria informática es un examen, pues debe partir de una situación dada: que este metódico, puesto que seguirá un plan de trabajo perfectamente sistematizado que permite llegar a conclusiones suficientemente fundamentadas (conclusión esta exigible a cualquier auditoria), que es puntual ya que se da un corte en el calendario para llevarla a cabo y que es discontinua, extraña al servicio de informática, en aras de buscar la objetividad requerida, por lo que será ejecutada por personas ajenas al departamento independientes de las funciones a auditar.

Principios de la auditoría informática.

Como menciona Piattini & Peso (2001, pág. 108) La futura de la auditoría informática radicará en los siguientes principios:

1. Todos los auditores tendrán que tener conocimientos informáticos que les permitan trabajar en el cada vez más fluctuante entorno de las tecnologías de la información dentro de las organizaciones empresariales, culturales y sociales.
2. Este aspecto no eliminará la necesidad de especialistas en auditoría informática; antes al contrario, los especialistas necesitarán cada vez más, unos conocimientos muy específicos, que al igual que sucede en el entorno de los sistemas de información, les permitan ser expertos en las diferentes ramas de la tecnología informática: comunicaciones, redes, ofimática. comercio electrónico, seguridad, gestión de bases de datos, etc.

3. El auditor informático dejará de ser un profesional procedente de otra área, con su consiguiente reciclado, para pasar a ser un profesional formado y titulado en auditoria informática que tendrá a su alcance diferentes medios de formación externa fundamentalmente, y que tendrá que formar una red de conocimientos compartidos con otros profesionales, tanto en su organización como con profesionales de otras organizaciones.

Fases de la auditoría informática

Como menciona Rivas (1889, págs. 47-50) La auditoría informática comprende las siguientes fases:

1. Toma de contacto.- Esta etapa tendrá lógicamente mucho más sentido si el equipo auditor es externo a la organización ya que en ella se recaba toda la información, relativa a la empresa a auditar, en puntos tales como:

- Organización
- organigrama
- Volumen, líneas de producto, planes.
- Situación en el mercado. etc.

2. Planificación de la operación.- Una vez que el auditor ha completado la etapa anterior y conoce suficientemente las condiciones de comentar y exponer si ha habido problemas en la atapa anterior (falta de comprensión o colaboración en algún nivel de la organización) así como definir los resultados esperados en la operación, para lo que tendrá que fijar, entre otros:

- Concentración de objetivos.
- Las áreas que cubrirá
- Personas de la organización que habrán de colaborar y en qué momento de la auditoria.
- Plan de trabajo:
    - Tareas
    - Calendario
    - Resultados parciales
    - Presupuesto

- Equipo auditor necesario

3. Desarrollo de la auditoria. - Es el momento de ejecutar las tareas que se enunciaron en la fase anterior; es esta una fase de observación, de recogida de datos, situaciones, diferencias. Se resumen en un período en el que:

- Se efectuarán las entrevistas previstas en la fase de planificación.
- Se completarán los cuestionarios que conlleva el auditar.
- Se observarán las situaciones deficientes, no solo las aparentes sino las que hasta ahora no hayan sido detectadas, para lo que se podrá llegar a asimilar situaciones límite.
- Se observa los procedimientos, tanto en los informáticos como en los usuarios.
- Se ejecutarán, por tanto. todas las previsiones efectuadas en la fase anterior al objeto de llegar a la siguiente etapa en condiciones de diagnosticar sobre la situación encontrada.

4. Fase de diagnóstico.- Cuando ya se han efectuado todas las revisiones, el equipo auditor debe encerrarse ya sin la intervención de la empresa auditada, para poder analizar e interpretar todos los datos obtenidos en el punto anterior y ser capaces de concluir con un diagnóstico de la situación real encontrada.
5. Presentación de conclusiones.- Es el momento de que los responsables comprometidos conozcan las conclusiones obtenidas por los auditores en la realización de la fase anterior. Esta fase claramente una fase delicada por cuanto es el momento en el que se presenta deficiencias, situaciones anímalas o cuanto menos mejorables. Es por ello recomendable que los auditores tengan el suficiente tacto como para presentar estas conclusiones como un plan de mejoras en beneficio de todos, más que como una reprobación de los afectados.
6. Formación del plan de mejoras.- Este último punto, la dirección ya conoce las deficiencias que el quipo auditor ha observado en su departamento informático; estas han sido discutidas. Mas no basta con quedarse ahí ahora es cuando los auditores han de demostrar su experiencia en situaciones anteriores lo suficientemente contrastadas y exitosas y ser capaces de adjuntar, junto con el informe de auditoría, el plan de mejoras que permitirá solventar las deficiencias encontradas.

Según Piattini & Peso (2001, pág. 107) La auditaría informática ha estado siempre ligado al de auditoría en la auditoría interna en particular, y este ha estado unido desde tiempos históricos al de contabilidad, control, veracidad de operaciones, etc. En tiempo de los egipcios ya se hablaba de contabilidad y de control de los registros y de las operaciones. Aun algunos historiadores fijan el nacimiento de la escritura como consecuencia de la necesidad de registrar y controlar operaciones. Es evidente que para que dichos sistemas cumplan sus objetivos debe existir una intuición de gestión de dichos sistemas, de los recursos que los manejan y de las inversiones que se ponen a disposición de dichos recursos para que el funcionamiento y los resultados sean los esperados. En ese momento, los equipos de auditoria, tanto extremos como internos, empezaron a ser mixtos, con involucración de auditores informáticos junto con auditores financieros. En ese momento se comenzaron a utilizar dos tipos de enfoque diferentes que en algunos casos convergían:

- Trabajos en los que el equipo de auditoría informática trabajaba bajo un programa de trabajo propio, aunque entroncando sus objetivos con los de la auditoría financiera; éste era el caso de trabajos en los que se revisaba controles generales de la instalación y controles específicos de las aplicaciones bajo conceptos de riesgos pero siempre unido al hecho de que el equipo de auditoría financiera utilizaría este trabajo para sus conclusiones generales sobre el componente financiero determinado.
- Revisiones en las que la auditoría informática consistía en la extracción de información para el equipo de auditoría financiera. En este caso el equipo o función de auditoría interna era un exponente de la necesidad de las organizaciones y departamentos de auditoría de utilizar expertos en informática para proveer al personal de dicho departamento de información extraída del sistema informático cuando la información a auditar estaba empezando a ser voluminosa y se estaba perdiendo la pista de cómo se habla creado.

Para Piattini & Peso (2001, pág. 108) Las diferentes acepciones de auditoría informática son las siguientes:

- Auditoría informática como soporte a la auditoría tradicional, financiera, etc.
- Auditoría informática con el concepto anterior, pero añadiendo la función de auditoría de la función de gestión del entorno informático.

- Auditoría informática como (función independiente, enfocada hacia la obtención de la situación actual de un entorno de información e informático a aspectos de seguridad y riesgo, eficiencia y veracidad e integridad.
- Las acepciones anteriores desde un punto de vista interno y externo.
- Auditoría como función de control dentro de un de partimento de sistemas.

Gestión de las tecnologías de la información

Como menciona Olave & Gómez (2006, pág. 379) Es una oportunidad profesional para ampliar el espectro de aprovechamiento de la Computación en el país. Utilizar estratégicamente la Tecnología de Información (TI) para mejorar las organizaciones donde es común encontrar empresas que padecen el fenómeno del despilfarro computacional. Esta oportunidad profesional es también una desatención curricular. Esto se debe, entre otras razones, a la ausencia en el contexto académico nacional de alternativas sólidamente constituidas para la profesionalización en Computación. Como se expone con la formación comúnmente establecida en esta área de conocimiento presenta varias falencias:

a) se encuentra ligada erróneamente a la denominación "Ingeniería de Sistemas";
b) está aún distante de lineamientos curriculares internacionales
c) su carácter de Ingeniería es discutible
d) los conocimientos correspondientes a la denominada área de formación profesional que no favorecen un perfil definido dada su naturaleza superficial.

Como menciona Utel (2013) Tiene como encomienda apoyar los procesos de planeación, organización, dirección y control de un negocio en las diferentes áreas de la organización, con el propósito de crear oportunidades y mejorar la cadena de valor, la productividad y la competitividad. Cuenta con las siguientes habilidades que son:

- Formulación y evaluación de proyectos de inversión en tecnología de información.
- Administración y optimización de la operación de una organización.
- Establecer estrategias de tecnologías de la información y la comunicación en el marco y procesos de negocio de la organización.

- Determinar las necesidades de información y tecnología aplicada a las empresas.
- Administración de proyectos de integración y desarrollo de tecnología de la información y de la comunicación.

Aspectos principales de la gestión de la tecnología de la información.

Para Iglesias (1998, pág. 11) Las mayores necesidades de gestión son las siguientes:

1) Las profundidades del análisis en ocasiones se descienden a detalles muy altos en la información exigida (detalles de ventas por cliente/ geografía/producto/canal/periodo)
2) La amplitud del mismo, ya que se necesitan cifras agregadas o consolidadas de varias empresas, relación con cifras ajenas al grupo.
3) Los menores tiempos de reacción ante los resultados.
4) Las nuevas posibilidades ofrecidas por las tecnologías de la información.

Según Naciones Unidas (2003, pág. 100) Cuatro aspectos principales han ampliado en grado sumo la capacidad de los organizamos de estadística:

a) La aparición en el mercado de computadoras de bajo costo y gran capacidad de procesamiento ha permitido a muchos organismos de estadísticas dotar a todo el personal con este tipo de equipo.
b) El desarrollo de aplicaciones de software fáciles de usar permite a los funcionarios acceder a importantes funciones estadísticas desde el diseño de los cuestionarios hasta la recopilación, la depuración, la tabulación, la representación y la publicación. Las herramientas comerciales disponibles han simplificado la programación de aplicaciones propias y la reutilización de componentes en la organización se ha hecho más frecuente.
c) Las redes de computadoras han facilitado el acceso interno a los datos y los metadatos mediante el establecimiento de entornos escalonados clientes-servidor.
d) La tecnología de internet ha permitido que el personal acceda oportunamente a fuentes de información externa, lo cual ha posibilitado las investigaciones, la

búsqueda de información general y el desarrollo de otras labores relevantes desde todos los niveles dela organización y no solo desde la cúpula directiva.

Necesidades de la gestión informática.

Como menciona Iglesias (1998, pág. 12) En un intento de estructurar las necesidades del control de gestión se pueden destacar las siguientes:

- Necesidad de disponer de información. Aunque (información) no son solo datos hay que recoger datos de dos tipos:
  1.- internos como los resultados de la contabilidad financiera y analítica, datos de transacciones de pedidos, almacén, facturación, seguimiento de calidades.
  2.- externos, como datos macroeconómicos, precios internacionales, datos de la competencia.
- Agregar y analizar la información obtenida.
- Posibilidad de elaborar y emitir informes con el resultado del análisis, elaborando y sintetizando toda la información procesada en diagnósticos de la situación de la empresa. El resultado serán los cuadros de mando de los responsables de las diversas unidades.
- Posibilidad de realizar proyecciones de las variables fundamentales.

Para Pérez & Dressler (2007, págs. 37-38) Especial importancia en la evolución de las TIC tiene el desarrollo del software, que ha permitido la aparición de avanzadas herramientas informáticas de gestión con nuevas funcionalidades y aplicaciones empresariales, entre las que se pueden destacar las siguientes:

- Intranets: Red privada de una organización diseñada y desarrollada siguiendo los protocolos propios y el funcionamiento de Internet, protocolo TCP/IP, navegador web, etc. Su utilización es interna pero puede estar conectada a Internet y a otras redes externas. Para los usuarios se resume en una serie de páginas Web que dan acceso a la distinta documentación de la empresa, informaciones corporativas, aplicaciones informáticas, incluso permiten la publicación de información y conocimientos personales de cada empleado. Además, dentro de las Intranet se pueden organizar y tener acceso a comunidades de prácticas virtuales, foros y listas de distribución.

- Software de Simulación y realidad virtual: aplicaciones que permiten minimizar los costes de la realización de prototipos, experimentar nuevas ideas y simular la aplicación de conocimientos.
- Workflow: aplicaciones que permiten mediante herramientas informáticas automatizar las fases que componen la elaboración de un proceso de negocio. Facilita la distribución, seguimiento y ejecución de las tareas o flujos que componen un trabajo, indicando en qué fase se encuentra el trabajo, quién es el encargado de la ejecución de cada fase, qué procedimientos se tienen que seguir y qué incidencias suceden durante las mismas.
- Video conferencias: Sistema que permite a varias personas, con independencia de su ubicación geográfica, entablar mediante aplicaciones específicas una conversación con soporte audio y video prácticamente en tiempo real.
- Datamining: tecnología que permite la explotación y análisis de los datos almacenados por la organización, generalmente una gran cantidad de datos almacenados en bases de datos y datawarehouse, buscando entre ellos relaciones y patrones de comportamiento no observables directamente.
- Datawarehouse: Repositorio o almacén de datos de gran capacidad que sirve de base común a toda la organización. Almacena los datos procedentes tanto del interior de la organización como del exterior organizándolos por temas, lo que facilita su posterior explotación.
- Inteligencia artificial: Aplicaciones informáticas a las que se dota de propiedades asociadas a la inteligencia humana. Ejemplos son los sistemas expertos, redes neuronales, etc. que a partir del conocimiento y reglas introducidas por un experto humano permiten alcanzar inferencia y resolver problemas.
- Motores de búsqueda: software diseñado para rastrear fuentes de datos tales como bases de datos, Internet, etc. lo que permite indexar su contenido y facilitar su búsqueda y recuperación.
- Gestión documental: Aplicaciones que permiten la digitalización de documentos, su almacenamiento, el control de versiones y su disponibilidad para los usuarios con autorización para su consulta y/o modificación.
- Mapas de conocimiento y páginas amarillas: Directorios que facilitan la localización del conocimiento dentro de la organización mediante el desarrollo

de guías y listados de personas, o documentos, por áreas de actividad o materias de dominio.

- Mensajería instantánea y correo electrónico: aplicaciones que facilitan la comunicación en tiempo real o diferido, así como el intercambio de documentos.
- Groupware: Tecnologías diseñadas para la gestión de trabajos en equipo. Facilita coordinar el trabajo y compartir informaciones y aplicaciones informáticas.

Metodología de COBIT 5

COBIT 5 acopla 5 principios que guían a la Empresa el desarrollo de forma segura el marco de Gobierno y Administración enfocado en una sucesión de 7 habilitadores que tienen relación, que perfeccionan en financiamiento, en información así como también en tecnología mediante lo cual la utilización va en beneficio de los interesados Isaca (2013)

Para Isaca (2013) COBIT 5 es adaptable a todas las dimensiones de organizaciones incluidas a las pequeñas empresas, entornos de tecnología. Se lo puede utilizar en:

- Seguridad de la información
- Gestión de riesgo
- Gobierno y administración de TI en la empresa
- Cumplimiento legislativo y regulador
- Procesamiento financiero
- Toma de decisiones sobre el manejo de tendencias actuales.

Conceptos Normativos.

Mediante Resolución 128-2015-F la Junta de Política y regulación Monetaria y Financiera expide las “Normas para la Administración Integral de Riesgos en las Cooperativas de Ahorro y Crédito y cajas Centrales”, establece las principales definiciones de Riesgos:

Riesgos informáticos en las COAC

Como menciona Tarazona (2007, pág. 137) Los riesgos de la información están presentes cuando confluyen dos elementos: amenazas y vulnerabilidades. Las amenazas y vulnerabilidades están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas. Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa, relacionada con el entorno de las organizaciones. Las vulnerabilidades son una debilidad en la tecnología o en los procesos relacionados con la información, y como tal, se consideran características propias de los sistemas de información o de la infraestructura que la contiene. Una amenaza, en términos simples es cualquier situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades afectando directamente la información o los sistemas que la procesan.

Para Tarazona (2007, pág. 137) Podemos agrupar las amenazas a la información en cuatro grandes categorías: Factores Humanos (accidentales, errores); Fallas en los sistemas de procesamiento de información; Desastres naturales y; Actos maliciosos o malintencionados; algunas de estas amenazas son:

- Virus informáticos o código malicioso
- Uso no autorizado de Sistemas Informáticos
- Robo de Información
- Fraudes basados en el uso de computadores
- Suplantación de identidad
- Denegación de Servicios (DoS)
- Ataques de Fuerza Bruta
- Alteración de la Información
- Divulgación de Información
- Desastres Naturales
- Sabotaje, vandalismo
- Espionaje

Para Gaitán & Niebel (2015) Todas las organizaciones enfrentan riesgo informático. Los riesgos afectan la posibilidad de la organización de competir para mantener su

poder financiero y la calidad de sus productos o servicios. Los riesgos determinados por la alta dirección incluyen aspectos tales como:

- Clima de ética y presión a la dirección para el logro de objetivos.
- Competencia, aptitud e integridad del personal
- Tamaño del activo, liquidez o volumen de transacciones.
- Condiciones económicas del país.
- Impacto en reglamentos gubernamentales.
- Procesos y sistemas de información automatizados.
- Dispersión geográfica de las operaciones.
- Cambios organizacionales, operacionales, tecnológicos y económicos.

Como menciona Gaitán & Niebel (2015) Los aspectos a considerar en el establecimiento de prioridades, en la planeación de auditoria, en adición a la identificación de riesgos son los siguientes:

- Fecha y resultados de la última auditoria.
- Exposición financiera en términos de riesgo.
- Riesgos y pérdidas potenciales.
- Requerimientos de la gerencia.
- Cambios importantes en operaciones, programas, sistemas y controles.
- Oportunidades para lograr beneficios operativos.
- Cambios en el equipo y capacidad del departamento de auditoria.

Niveles básicos de los riesgos informáticos de las COAC

Para Valdés (1988, pág. 34) La prevención contra los riesgos diversos tiene como finalidad la protección de las personas, equipos y trabajos vinculados con la actividad informática. Dentro de la protección se distinguen tres niveles básicos como lo son:

- La protección amplia, la cual debe ser eficaz y concierne a los locales de procesamiento y sus anexos. En algunos casos también los locales de disposición de las informaciones de entrada y los de almacenamiento y archivo disfrutan de esta protección.

- La protección media, cuyos efectos deben ser compensadores y complementarios. Se instala en los locales de control y de disposición de resultados.
- La protección restringida, en función del grado seleccionado de vulnerabilidad. Es conveniente para los locales de gestión y también para los de análisis y programación.

Como menciona Valdés (1988, pág. 34) Dichas protecciones, independientemente del nivel de que se traten, reclaman decisiones directivas en lo que concierne a:

- Implantación de locales y equipos
- Selección de medios de protección, alarmas, evacuación y servicio.
- Circulación de las personas y los medios de control.
- Circulación de informaciones y control de esta circulación.
- Previsión de medios de reinicio de operaciones después de un siniestro.

Según Carpentier (2016, págs. 40-41) Los riesgos informáticos cuentan con la siguiente clasificación:

1. El activo.- Es partes de un bien que compone el patrimonio y el valor para la empresa.
2. Las amenazas.- Es alguien o algo que puede explotar una vulnerabilidad para obtener, modificar o impedir el acceso a un activo o comprometerlo. Existe una correlación con una o varias vulnerabilidades. También puede existir varias amenazas para cada vulnerabilidad. El conocimiento de los diferentes tipos de amenazas para cada vulnerabilidad. El conocimiento de los diferentes tipos de amenazas puede ayudar en la determinación de su peligrosidad y los controles apropiados para reducir su impacto potencial. La amenaza es una fuente efectiva de incidentes que puedan provocar reacciones adversas graves sobre un activo o un conjunto de activos o sobre la empresa misma. Las amenazas se clasifican en general por:

- Origen o fuente
- Tipo
- Motivación, acción

3. El riesgo.- Es la posibilidad de que un evento critico aparezca. Su evaluación permite establecer las acciones para reducir y mantener la amenaza a un nivel razonable y aceptable. Los riesgos pueden ser clasificados según sus orígenes (internos o externos).

- Riesgos externos:
- Los ataques no dirigidos. Toda empresa puede verse afectada por la infección de virus o ataques globales sobre la red (denegación de servicio)
- Los ataques dirigidos. Los riesgos físicos (robo o destrucción de material) o lógicos (acceso de intrusos)
- Riesgos internos:
- Son más difíciles de comprender porque se refieren a los recursos internos de la empresa.

4. El impacto de un riesgo.- Puede ser expresado por las consecuencias o daños que afectan a un activo: atentado contra la integridad o la imagen de marca, perdida de disponibilidad o de volumen de negocio. Podemos evaluar el impacto según los criterios siguientes:

- Financiero (gastos de rehabilitación o restauración, pérdidas de explotación.)
- Jurídico y legal
- Reputación e imagen de la empresa (en relación con el exterior y con el personal)
- Experiencia

5. Las vulnerabilidades.- En el ámbito de la seguridad informática, existen tres familias de vulnerabilidades:

- Vulnerabilidades relacionadas con los ámbitos físicos
    - Falta de redundancia y recursos a nivel de equipo
    - Acceso a salas de informática no seguras
    - Ausencia o mala estrategia de protección de datos
- Vulnerabilidades relacionadas con los ámbitos organizativos
    - Falta de:
    - Recursos humanos y personal cualificado
    - Comunicaciones

- Falta de:
- Controles periódicos
- Documentos de procedimientos adaptados a la empresa
- Medios relativos a los riesgos
- Complejidad funcional

- Vulnerabilidades relacionadas con los ámbitos tecnológicos
  - Múltiples fallos en los servicios y aplicaciones web y las bases de datos
  - Falta de actualizaciones y parches de los sistemas operativos
  - Falta de control suficiente sobre los programas malintencionados
  - Recurrencia de fallos y falta de supervisión de incidentes
  - Redes complejas, no protegidas, mal organizadas, sin redundancia
  - Mala utilización del correo

Riesgo

Es la posibilidad de que se produzca un evento que genere pérdidas con un determinado nivel de impacto para la entidad. Junta de Regulación Monetaria Financiera (2017)

Para la Junta de Regulación Monetaria Financiera (2017) en el ARTÍCULO 14.- indica que el procedimiento de la administración integral de riesgos.- La Corporación para la definición de los procedimientos en cada una de las etapas del proceso de administración de riesgos, como mínimo deberán considerar los siguientes lineamientos:

a) Identificación: reconocer los riesgos existentes en cada operación, producto, proceso y línea de negocio que desarrolla la entidad, para lo cual se identifican y clasifican los eventos adversos según el tipo de riesgo al que corresponden;

b) Medición: los riesgos deberán ser cuantificados con el objeto de medir el posible impacto económico en los resultados financieros de la entidad.

c) Priorización: una vez identificados los eventos de riesgos y su impacto, la entidad deberá priorizar aquellos en los cuales enfocará sus acciones de control.

d) Control: es el conjunto de actividades que se realizan con la finalidad de disminuir la probabilidad de ocurrencia de un evento adverso, que pueda originar pérdidas a la entidad.

e) Mitigación: corresponde a la definición de las acciones para reducir el impacto de un evento de riesgo y minimizar las pérdidas.

f) Monitoreo: consiste en el seguimiento que permite detectar y corregir oportunamente deficiencias y/o incumplimientos en las políticas, procesos y procedimientos para cada uno de los riesgos a los cuales se encuentra expuesta la entidad.

g) Comunicación: acción orientada a establecer y desarrollar un plan de comunicación que asegure de forma periódica la distribución de información apropiada, veraz y oportuna, relacionada con la entidad y su proceso de administración integral de riesgos, destinada al Consejo de Administración, así como a las distintas áreas que participan en la forma de decisiones y en la gestión de riesgos. Esta etapa debe coadyuvar a promover un proceso de empoderamiento y mejora continua en la administración integral de riesgos.

Como menciona la Junta de Regulación Monetaria Financiera (2017) En el Artículo 15.- Tipos de Riesgo: En la implementación de la administración integral de riesgos las entidades deberán considerar al menos los siguientes tipos de riesgo:

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 vea 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 los 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 de que se produzcan pérdidas para la entidad, debido a fallas o insuficiencias originadas en procesos, personas, tecnología de 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 estipulados.

Niveles de riesgo

Para Junta de Regulación Monetaria Financiera (2017) En su Artículo 16. - Niveles de riesgo.- Para la definición de los niveles de riesgo la Corporación podrá desarrollar sus propias metodologías, que deberán considerar criterio que estimen el impacto en los resultados y la probabilidad de ocurrencia. Los niveles de riesgo son los siguientes:

a) Riesgo Crítico: cuando el riesgo representa una probabilidad de pérdida alta que puede afectar gravemente a la continuidad del negocio, por lo tanto, requiere “acciones" inmediatas por parte del Directorio y el Director General.
b) Riesgo Alto: cuando el riesgo representa una probabilidad de pérdida alta, que puede afectar el funcionamiento normal de ciertos procesos de la Corporación, y que requiere la atención del comité Técnico, el Director General y mandos medios.
c) Riesgo Medio: cuando el riesgo representa una probabilidad de pérdida moderada, que afecta a ciertos procesos de la Corporación, y que requiere la atención del Director General y de mandos medios.

d) Riesgo Bajo: cuando el riesgo representa una probabilidad de pérdida baja, que no afecta significativamente a los procesos de la corporación, y que se administran con controles y procedimientos rutinarios.

Clasificación de riesgos

Para Fábrega, Montiel, Planas & Vílchez (2009, pág. 21) Los riesgos pueden clasificarse en otras tres categorías:

- Riesgos convencionales: relacionados con la actividad y el equipo existentes en cualquier sector.
- Riesgos específicos: asociados a la utilización o manipulación de productos que por su naturaleza puedan ocasionar daños.
- Riesgos mayores: relacionados con accidentes y situaciones excepcionales. Sus consecuencias pueden presentar una especial gravedad ya que la rápida expulsión de productos peligrosos o de energía podría afectar a áreas considerables.

Cooperativas de Ahorro y Crédito

Como menciona la Ley Orgánica de Economía Popular y Solidaria del Sistema Financiero (2011) En el Art. 81.- Cooperativas de ahorro y crédito.- Son organizaciones formadas por personas naturales o jurídicas que se unen voluntariamente con el objeto de realizar actividades de intermediación financiera y de responsabilidad social con sus socios y, previa autorización de la Superintendencia, con clientes o terceros con sujeción a las regulaciones y a los principios reconocidos en la presente Ley.

Art. 82.- Requisitos para su constitución.- Para constituir una cooperativa de ahorro y crédito, se requerirá contar con un estudio de factibilidad y los demás requisitos establecidos en el Reglamento de la presente Ley. Ley Orgánica de Economía Popular y Solidaria del Sistema Financiero (2011)

Para la Ley Orgánica de Economía Popular y Solidaria del Sistema Financiero (2011) En el Art. 83.- Actividades financieras.- Las cooperativas de ahorro y crédito, previa autorización de la Superintendencia, podrán realizar las siguientes actividades:

a) Recibir depósitos a la vista y a plazo, bajo cualquier mecanismo o modalidad autorizada.
b) Otorgar préstamos a sus socios.
c) Conceder sobregiros ocasionales.
d) Efectuar servicios de caja y tesorería.
e) Efectuar cobranzas, pagos y transferencias de fondos, así como emitir giros contra sus propias oficinas o las de instituciones financieras nacionales o extranjeras.
f) Recibir y conservar objetos muebles, valores y documentos en depósito para su custodia y arrendar casilleros o cajas de seguridad para depósitos de valores.
g) Actuar como emisor de tarjetas de crédito y de débito.
h) Asumir obligaciones por cuenta de terceros a través de aceptaciones, endosos o avales de títulos de crédito, así como por el otorgamiento de garantías, fianzas y cartas de crédito internas y externas, o cualquier otro documento, de acuerdo con las normas y prácticas y usos nacionales e internacionales.
i) Recibir préstamos de instituciones financieras y no financieras del país y del exterior.
j) Emitir obligaciones con respaldo en sus activos, patrimonio, cartera de crédito hipotecaria o prendaria propia o adquirida, siempre que en este último caso, se originen en operaciones activas de crédito de otras instituciones financieras.
k) Negociar títulos cambiarios o facturas que representen obligación de pago creados por ventas a crédito y anticipos de fondos con respaldo de los documentos referidos.
l) Invertir preferentemente, en este orden, en el Sector Financiero Popular y Solidario, sistema financiero nacional y en el mercado secundario de valores y de manera complementaria en el sistema financiero internacional.
m) Efectuar inversiones en el capital social de cajas centrales.
n) Cualquier otra actividad financiera autorizada expresamente por la Superintendencia.

Las cooperativas de ahorro y crédito podrán realizar las operaciones detalladas en este artículo, de acuerdo al segmento al que pertenezcan, de conformidad a lo que establezca el Reglamento de esta Ley.

Como menciona García, Prado, Salazar & Mendoza (2018, pág. 5) Las Cooperativas al buscar el logro o beneficio de los agentes que la conforman, participan en el desarrollo local y territorial. Portales (2014), el desarrollo local enfatiza la creación de procesos que buscan minimizar la pobreza, formando actividades productivas que pueden realizar en una localidad, con el fin de participar en el mercado y así demostrar el avance de una comunidad en un territorio determinado, es decir, se identificó como aportadores de recursos productivos que permiten avanzar a pesar de la competencia mercado, todo esto desde una localidad en específico, que busca aprovechar las oportunidades económicas. En relación al capital social, permiten a los socios el desenvolvimiento y participación dentro de la entidad, conformando así una estructura social, basada en la confianza; se direcciona en el cumplimiento de los objetivos propuestos, es decir, generar una corriente de beneficios para las personas que interactúan en el grupo (Coleman, 1988).

Para García, Prado, Salazar & Mendoza (2018, pág. 6) Las Cooperativas al ejercer dos tipos de influencia en el capital social; evidencian la fortaleza de la estructura social, además que al considerarse una red pueden compartir información, innovaciones creadas para los procesos sociales, empleo, acceso a capitales; y la coordinación, compromiso y administración de los capitales de los socios. Es importante señalar que en relación al capital social en algunos estudios propuestos, estos describen una influencia positiva en la búsqueda de empleo, para mejorar la rentabilidad en términos colaborativos, para la utilización de los créditos, para mejorar la parte administrativa de la institución, así como el manejo de los flujos financieros (Lin, 2001). Y las aportaciones de los socios permiten que las actividades financieras en las cooperativas de ahorro y crédito puedan efectuarse, según los criterios internos administrativos, estas contribuyen minimizar costes mediante los niveles de confianza.

2.4.1 Segmentación de Cooperativas de Ahorro y Crédito

Para la Superintendencia de Economía Popular y Solidaria (2015) La Junta de Política y Regulación Monetaria y Financiera mediante la resolución No. 038-2015-F el 13 de febrero de 2015 establece la "NORMA PARA LA SEGMENTACIÓN DE LAS ENTIDADES DEL SECTOR FINANCIERO POPULAR Y SOLIDARIO", y en su artículo 1 menciona:

Como menciona la Superintendencia de Economía Popular y Solidaria (2015) En el "Artículo 1.- Las entidades del sector financiero popular y solidario de acuerdo al tipo y al saldo de sus activos se ubicarán en los siguientes segmentos:" (Ver Tabla 2)

Segmento	***Activos (USD)***
1	*Mayor a 80'000.000,00*
2	*Mayor a 20'000.000,00 hasta 80'000.000,00*
3	*Mayor a 5'000.000,00 hasta 20'000.000,00*
4	*Mayor a 1'000.000,00 hasta 5'000.000,00*
5	*Hasta 1'000.000,00*
	Cajas de Ahorro, bancos comunales y cajas comunales

Tabla 2: Segmentación de Cooperativas de Ahorro y Crédito
Fuente: SEPS

Artículo 2.- Las entidades de los segmentos 3, 4 y 5 definidas en el artículo anterior se segmentarán adicionalmente al vínculo con sus territorios. Se entenderá que las entidades referidas tienen vínculo territorial cuando coloquen al menos el 50% de los

recursos en los territorios donde estos fueron captados." Superintendencia de Economía Popular y Solidaria (2015)

En el artículo 447 del Código Orgánico Monetario y Financiero se indica que las cooperativas se ubicarán en los segmentos que la Junta determine. Superintendencia de Economía Popular y Solidaria (2015)

La Superintendencia de Economía Popular y Solidaria se acoge a lo dispuesto por el Código Monetario Financiero y precautelando los intereses del Sector de la Economía Popular y Solidaria. Superintendencia de Economía Popular y Solidaria (2015)

2.5 Hipótesis

La metodología COBIT 5 incidirá en la minimización de los Riesgos Informáticos en las Cooperativas de Ahorro y Crédito de los Segmentos 2 y 3 de la ciudad de Ambato.

VARIABLES	TIPO	CONCEPTO
Metodología COBIT 5	Independiente	Conjunto de conceptos y procesos que la metodología COBIT 5 establece para la gestión TI de las Empresas
Análisis de riesgos informáticos.	Dependiente	Determinación de eventos o sucesos que pudieren afectar a los bienes o servicios informáticos en las Cooperativas de Ahorro y Crédito.

Tabla 3: Hipótesis
Elaborado por: El autor

2.6 Señalamiento de Variables

En razón de la hipótesis planteada tenemos dos variables.

Variable Independiente: Metodología COBIT 5

Variable Dependiente: Análisis de riesgos informáticos.

CAPÍTULO III

METODOLOGÍA

3.1 Enfoque

El presente trabajo de investigación tiene un enfoque cuali- cuantitativo, es cuantitativa porque se va a utilizar parámetros de medición; también es cualitativa porque se va he emitir juicios de valor respecto al riesgo operativo en la institución.

Para Hernández & Baptista (2010, pág. 16) Investigación cualitativa es un método de investigación usado principalmente en las ciencias sociales que se basa en cortes metodológicos basados en principios teóricos tales como la fenomenología, la hermenéutica, la interacción social. Investiga el por qué y el cómo se tomó una decisión, así como también busca responder preguntas tales como cuál, dónde, cuándo, cuánto. La investigación cualitativa se basa en la toma de muestras pequeñas.

3.2 Modalidad básica de la investigación

3.2.1 Investigación Bibliográfica

La investigación será bibliográfica porque nos apoyaremos en libros, documentos técnicos, tesis del área financiera e informática, revistas, artículos y leyes existentes para la elaboración del marco teórico sobre procesos y riesgos de TI.

3.2.2 Investigación de Campo

La investigación será también de campo porque se buscará obtener información dentro de la institución respecto a los procesos de TI y métodos para minimizar los riesgos en el área tecnológica.

3.3 Nivel o tipo de investigación

Investigación Descriptiva

La investigación será descriptiva por que se realizará un análisis para llegar a determinar la incidencia que tienen la falta de procesos y su incidencia en la detección de riesgos de TI.

Como menciona Tamayo (2004, pág. 46), comprende la descripción, registro, análisis e interpretación de la naturaleza y la composición o procesos de los fenómenos. El enfoque se hace sobre conclusiones dominantes o sobre como una persona, grupo o cosa se conduce o funciona en el presente sobre las realidades de hecho, y sus características fundamentales es la de presentarnos una interpretación correcta.

Explicativa

La investigación es explicativa porque se va a poder sustentar la importancia que tienen la elaboración de procesos para la disminución de los riesgos de TI utilizando la metodología COBIT 5.

3.4 Población y Muestra

El presente proyecto trabajará con la población total que es el grupo de profesionales encargados de la administración y manejo de riesgos y del departamento de Sistemas de las instituciones financieras.

Al momento de realizar la investigación en la ciudad de Ambato se encuentran 10 Cooperativas de ahorro y crédito las cuales están en el segmento dos y tres, realizando la investigación al personal administrativo de éstas instituciones financieras, dicho personal tiene acceso o conocimiento acerca de las TI obteniendo un total de 130 personas.

Muestra

Según Vallejo P. (2012):

$$\frac{N*(\alpha_c*0{,}5)^2}{1+(e^2*(N-1))} =$$

Donde:

e = Margen de error; para el caso de estudio se trabajará con un margen de error del 3%.

a_c = Valor del nivel de confianza (varianza)

N = Población

Muestra = 116

3.5 Operacionalización de variables

3.5.1 **Variable Independiente:** Metodología COBIT 5

Conceptualización o Descripción	**Dimensiones**	**Indicadores**	**Ítems Básicos**	**Técnicas e Instrumentos**
COBIT 5 acopla 5 principios que guían a la Empresa el desarrollo de forma segura el marco de Gobierno y Administración enfocado en una sucesión de 7 habilitadores que tienen relación, que perfeccionan en financiamiento, en información así como también en tecnología mediante lo cual la utilización va en beneficio de los interesados, estos principios son: - Seguridad de la información - Gestión de riesgo - Gobierno y administración de TI en la empresa - Cumplimiento legislativo y regulador - Procesamiento financiero - Toma de decisiones sobre el manejo de tendencias actuales.	Cinco principios que guían a la Empresa el desarrollo de forma segura el marco de Gobierno y Administración	- Seguridad de la información - Gestión de riesgo - Gobierno y administración de TI en la empresa - Cumplimiento legislativo y regulador - Procesamiento financiero - Toma de decisiones sobre el manejo de tendencias actuales.	- Cuenta con un manual de funciones para el personal de la misma. - La información de los procedimientos para el desarrollo de sus funciones es entendible y de su conocimiento. - Las herramientas informáticas son de apoyo para la toma de decisiones. - Cuenta con un diseño de procesos para las partes interesadas tanto internas como externas. - Cree usted que la aplicación de una metodología de buenas prácticas para el control de la información, reducirá el nivel de riesgo informático en las instituciones financieras.	- Encuesta con Cuestionario

Tabla 4: Variable Independiente: Procesos de análisis COBIT 5
Elaborado por: El autor

3.5.2 **Variable Dependiente**: Análisis de riesgos informáticos

Conceptualización o Descripción	Dimensiones	Indicadores	Ítems Básicos	Técnicas e Instrumentos
Los riesgos de la información están presentes cuando confluyen dos elementos: amenazas y vulnerabilidades. Las vulnerabilidades son una debilidad en la tecnología o en los procesos relacionados con la información, y como tal, se consideran características propias de los sistemas de información o de la infraestructura que la contiene. Una amenaza, en términos simples es cualquier situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades afectando directamente la información o los sistemas que la procesan.	- Amenazas - Vulnerabilidades	- Riego operativo actual - Estructuras que se generan actualmente - Estructuras que se deberían generar - Medidas de control del riesgo operativo - Disponibilidad de la información.	- El nivel actual del riesgo operativo es aceptable. - Cuentan con estructuras y reportes de riesgo de TI actualmente. - Se aplican medidas de control del riesgo. - Se dispone de la contingencia tecnológica necesaria.	Encuesta Cuestionario

Tabla 5: Variable Dependiente: Impacto de riesgos informáticos
Elaborado por: El autor

3.6 Recolección de Información

La técnica a emplearse será la encuesta dirigida para lo que es necesario utilizar como instrumento el cuestionario a través de preguntas cerradas, lo que ayudará a la obtención más concreta de la información que queremos obtener.

PREGUNTAS BÁSICAS	EXPLICACIÓN
¿Para qué?	Para alcanzar los objetivos de la investigación
¿De qué personas u objetos?	Jefe Financiero Responsables del área de riesgos Jefe de Sistemas
¿Sobre qué aspectos?	Control de riesgos de TI
¿Quién, Quiénes?	Investigador: Ing. Christian Giovanny Barrera Barragán
¿Cuándo?	Segundo semestre del 2017
¿Dónde?	Cooperativa de Ahorro y Crédito Indígena SAC
¿Cuántas veces?	Una para la obtención de la información y para la Investigación.
¿Qué técnicas de recolección?	Encuesta Entrevista
¿Con qué?	Cuestionario Inspecciones
¿En qué situación?	Dentro del horario de trabajo con profesionalismo investigativo y absoluta confidencialidad y reserva.

Tabla 6: Recolección de la Información
Elaborado por: El autor

3.7 Procesamiento y Análisis

Como menciona Villavicencio (2007) el siguiente orden:

- Revisión crítica de la información recogida; es decir limpieza de información defectuosa, contradictoria, incompleta, no pertinente y otras fallas.
- Repetición de la recolección, en ciertos casos individuales para corregir errores de contestación.
- Tabulación o cuadros variables de la hipótesis y objetivos.

- Manejo de información (reajuste de cuadros con casillas vacías o con datos tan reducidos cuantitativamente que no influyen significativamente en los análisis).

3.8 Análisis de Resultados

Encuesta Personal

Como menciona Nogales (2004, pág. 103) Permite obtener la información mediante un coloquio directo y personal entre entrevistador y entrevistado. Normalmente, la encuesta personal se realiza con un cuestionario en formato papel y es el entrevistador quien plantea directamente las preguntas al entrevistado y cumplimenta el cuestionario con las respuestas proporcionadas. En algunas ocasiones el entrevistador entrega el cuestionario al entrevistador y este lo contesta directamente bajo el control del primero. El lugar de realización de la encuesta personal es un factor clave en su diseño y planteamiento metodológico. El tema de la investigación y el colectivo son aspectos a considerar cuando se decide el lugar más apropiado para realizar el trabajo de campo y una vez elegido este, es necesario diseñar el cuestionario y plantear el procedimiento de captación muestral adaptándose a las características de dicho lugar. Cuenta con las siguientes modalidades:

- Encuesta en el hogar.
  - Temas: productos para el hogar, artículos personales.
  - Colectivo: amas de casa, niños, jóvenes, jubilados.
  - Cuestionario: puede ser más extenso y utilizar material auxiliar.
  - Dificultad: vencer la desconfianza de los entrevistados.

- Encuesta en el centro de trabajo.
  - Temas: relacionados con la actividad de la empresa.
  - Colectivo: empresas, colectivos de profesionales.
  - Cuestionario: también puede ser extenso y con material auxiliar.
  - Dificultad: es necesario concertar citas previas.

- Encuesta en el exterior.
  - Temas: de todo tipo mientras no sean muy personales.

- Colectivo: consumidores en general
- Cuestionario: tiene que ver reducido y muy sencillo
- Dificultad: captar y convencer a los entrevistados.

Para Villavicencio (2007) indica lo siguiente:

- Análisis de los resultados estadísticos, destacando tendencias o relaciones fundamentales de acuerdo con los objetivos e hipótesis.
- Interpretación de los resultados con apoyo del marco teórico en el aspecto pertinente.
- Comprobación de hipótesis para la verificación estadística.
- Establecimiento de conclusiones y recomendaciones.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Al realizar la investigación de campo se utilizó la técnica de la encuesta, la cual se aplicó al personal administrativo de las Cooperativas de Ahorro y Crédito del segmento dos y tres de la ciudad de Ambato. El personal analizado se encuentra desglosado de la siguiente manera:

MUESTRA	
DEPENDENCIA	**TOTAL DE PERSONAL**
GERENCIA	10
JEFE DE SISTEMAS	10
ANALISTAS DE SISTEMAS	20
JEFE DE RIESGO	10
ANALISTA DE RIESGO	20
AUDITORÍA INTERNA	10
AUDITORÍA EXTERNA	10
PERSONAL DE ATENCIÓN AL CLIENTE	26

ENCUESTA

1. ¿La Cooperativa cuenta con un manual de funciones para el personal de la misma?

Tabla 7: Funciones

CATEGORIA	CANTIDAD	FRECUENCIA %
Si	76	66%
No	40	34%
Total	116	100%

Fuente: Encuestas
Elaborado por: El autor

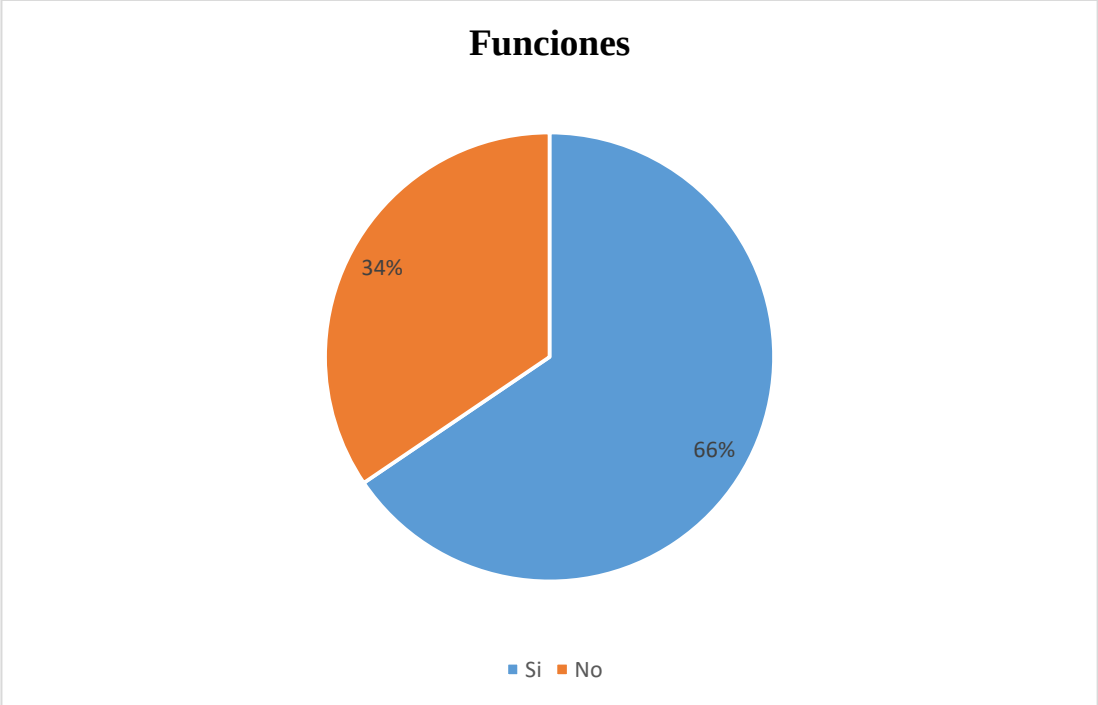


Gráfico 2: Funciones

Elaborado por: El autor

ANÁLISIS. - En las encuestas realizadas a 116 personas, 40 personas que representa el 34% indicaron que no cuentan con un manual o desconocen acerca de su existencia y 76 personas que corresponde al 66% mencionaron que si lo cuentan

INTERPRETACIÓN. - Según las respuestas obtenidas se observa que en las instituciones financieras cuentan con un manual de funciones pero existe un porcentaje considerable que desconoce de su existencia y no se estaría aplicando.

2. ¿La información de los procedimientos para el desarrollo de sus funciones es entendible y de su conocimiento?

Tabla 8: Procedimientos Personal

CATEGORIA	CANTIDAD	FRECUENCIA %
Si	66	57%
No	50	43%
Total	116	100%

Fuente: Encuestas
Elaborado por: El autor

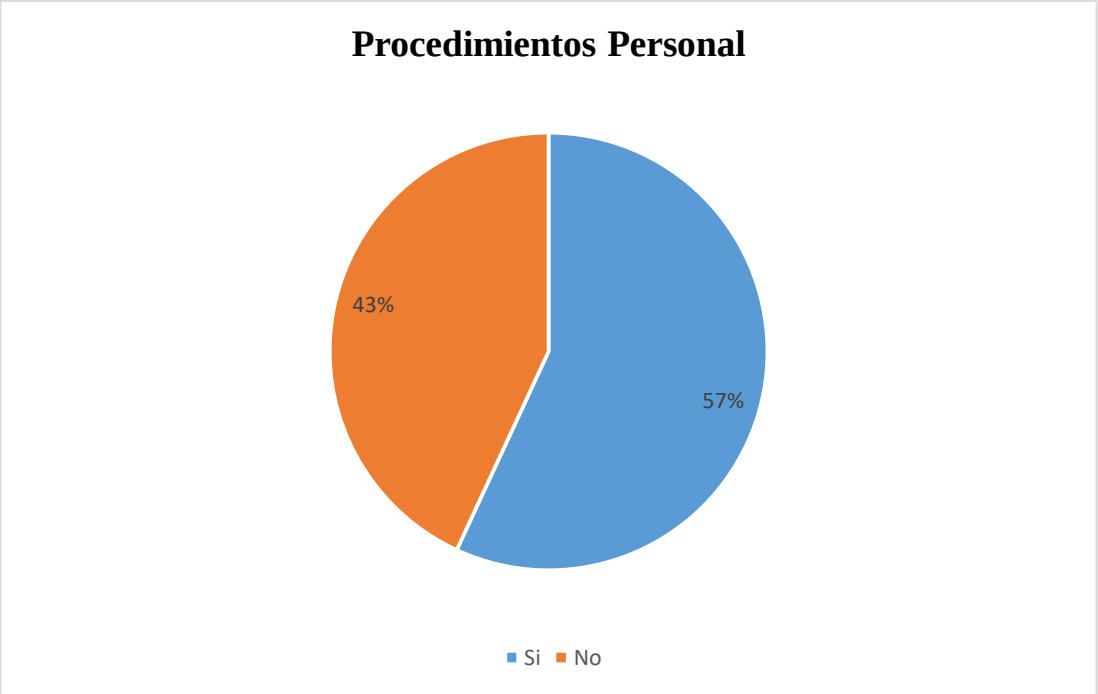


Gráfico 3: Información confiable
Elaborado por: El autor

ANÁLISIS. - De las 116 personas encuestadas, 66 que representa el 57% indicaron que la información de los procedimientos para el desarrollo de sus funciones es entendible y de su conocimiento, y 50 personas que corresponde al 43% manifiestan que No.

INTERPRETACIÓN. - En esta pregunta se pudo determinar que la información con la que cuenta la institución financiera para los procedimientos de su personal en su mayoría es entendible pero existe un personal considerable que menciona lo contrario lo cual puede mermar su desempeño laboral.

3. ¿Las herramientas informáticas que utiliza en la institución, ya sean estas para el manejo de la información financiera y contable, información administrativa, u otra información sirven de apoyo para la toma de decisiones?

Tabla 9: Herramientas de apoyo.

CATEGORIA	CANTIDAD	FRECUENCIA %
Siempre	8	7%
Casi siempre	8	7%
A veces	100	86%
Nunca	0	0%
Total	116	100%

Fuente: Encuestas
Elaborado por: El autor

Gráfico 4: Cumple con sus expectativas
Elaborado por: El autor

ANÁLISIS. - En las 116 personas encuestadas, 100 que representa el 86% indicaron que a veces las herramientas utilizadas en la institución cumplen con sus expectativas y 8 que corresponde al 7% aludieron que siempre y que casi siempre lo realizan.

INTERPRETACIÓN. - Al analizar lo referente a las herramientas informáticas que utilizan en las instituciones, se puede observar que las mismas ayudan a la toma de decisiones del personal de forma esporádica u ocasional.

4. ¿La institución cuenta con un diseño de procesos que recoja las necesidades de las partes interesadas tanto internas como externas?

Tabla 10: Diseño de procesos

CATEGORIA	CANTIDAD	FRECUENCIA %
Siempre	7	6%
Casi siempre	7	6%
A veces	80	69%
Nunca	22	19%
Total	116	100%

Fuente: Encuestas
Elaborado por: El autor

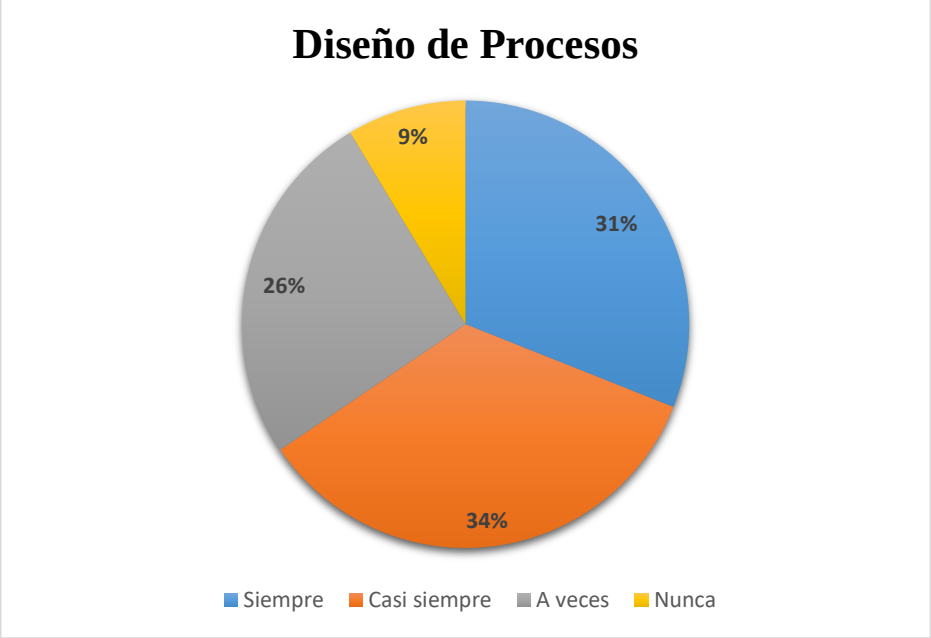


Gráfico 5: Diseño de procesos
Elaborado por: El autor

ANÁLISIS. - Como indican las 116 personas encuestadas, 7 que representan el 6% mencionaron que siempre y casi siempre la institución establece un diseño de procesos, mientras que 80 personas que representan un 69% indican que a veces realizan un diseño de procesos; y 22 personas que representan un 19% manifiestan que nunca lo hacen.

INTERPRETACIÓN. - De las respuestas obtenidas en esta pregunta se puede denotar que a veces consideran establecer o definir un diseño de procesos para las tareas que realiza la institución. Esto podría ocasionar gran impacto en el correcto orden, confiabilidad y oportuna entrega de servicios e información a las partes interesadas.

5. ¿La información que se obtiene de los clientes o socios de la institución financiera es la necesaria para un real conocimiento de los socios?

Tabla 11: Información necesaria de socios y clientes

CATEGORIA	CANTIDAD	FRECUENCIA %
Siempre	18	16%
Casi siempre	18	16%
A veces	80	68%
Nunca	0	0%
Total	116	100%

Fuente: Encuestas
Elaborado por: El autor

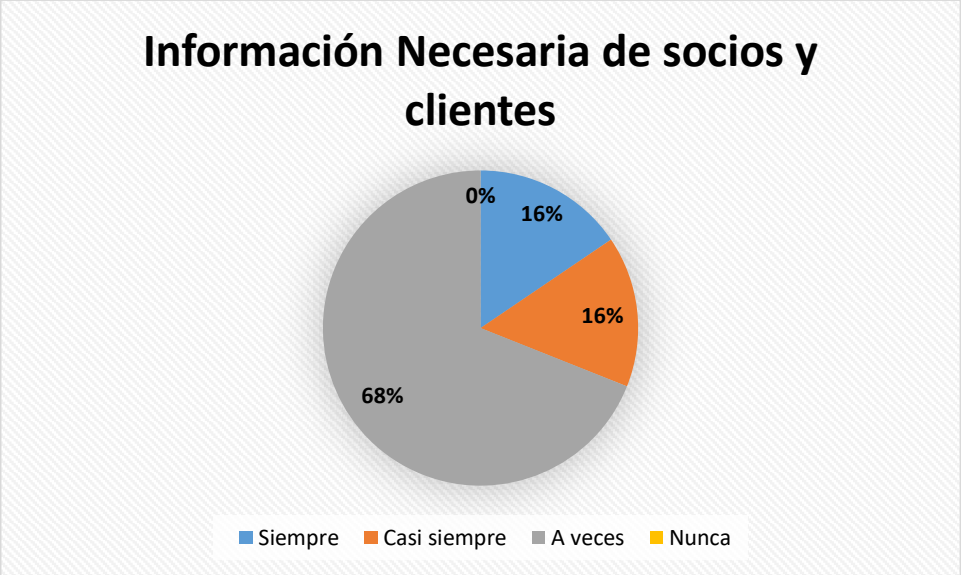


Gráfico 6: Información necesaria
Elaborado por: El autor

ANÁLISIS. - De las 116 personas encuestadas, 80 que representa el 68% mencionaron que a veces la información que se obtiene es la necesaria y 18 que corresponde al 16% indicaron que siempre y casi siempre lo es.

INTERPRETACIÓN. - Mediante las repuestas obtenidas la mayoría de las personas indicaron que a veces obtienen la información necesaria de los clientes o socios de las instituciones financieras ya que en varios casos se omite información importante para el giro del negocio de la institución, de ahí la importancia de la validación de la información obtenida.

6. ¿El personal de la institución conoce y aplica las políticas elaboradas por TI?

Tabla 12: Políticas de TI

CATEGORIA	CANTIDAD	FRECUENCIA %
Siempre	0	0%
Casi siempre	46	40%
A veces	48	41%
Nunca	22	19%
Total	116	100%

Fuente: Encuestas
Elaborado por: El autor

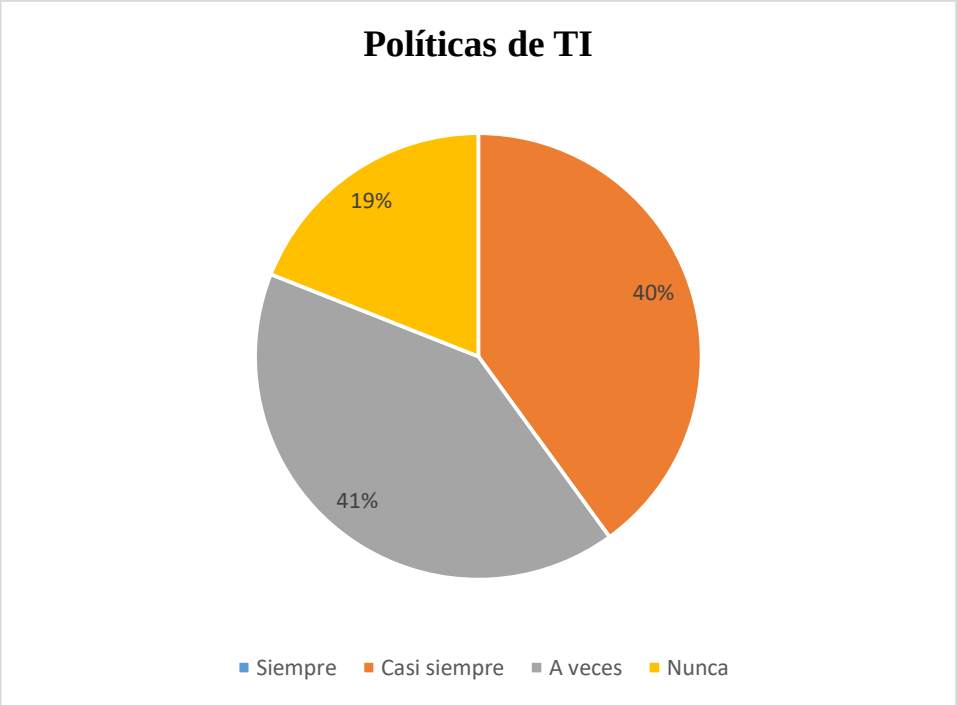


Gráfico 7: Políticas de TI
Elaborado por: El autor

ANÁLISIS. - De las 116 personas encuestadas, 48 que representan el 41% mencionaron que a veces conocen y aplican las políticas establecidas por TI, 46 que representa un 40% aludieron que casi siempre lo hacen, y 22 que representa el 19% indicaron que nunca conocieron ni aplicaron las políticas de TI.

INTERPRETACIÓN. – Según las respuestas obtenidas, se puede observar que las políticas de TI son poco conocidas y aplicadas dentro de las instituciones financieras, provocando un alto riesgo de mal uso de los recursos de TI.

7. ¿La administración realiza un tratamiento adecuado para mitigar los riesgos informáticos en la institución?

Tabla 13: Tratamiento de Riesgo informático

CATEGORIA	CANTIDAD	FRECUENCIA %
Siempre	0	0%
Casi siempre	0	0%
A veces	100	86%
Nunca	16	14%
Total	116	100%

Fuente: Encuestas
Elaborado por: El autor

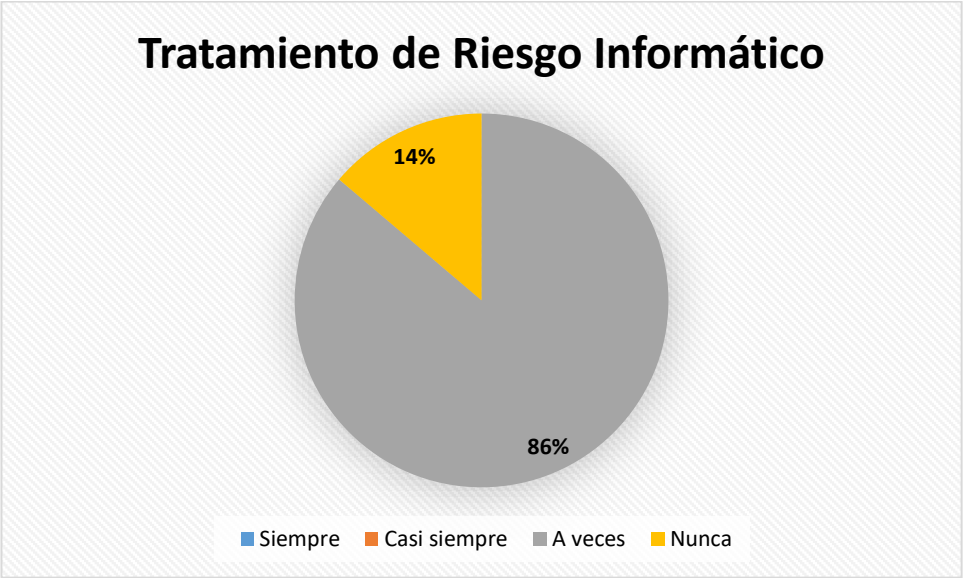


Gráfico 8: Riesgo operativo
Elaborado por: El autor

ANÁLISIS. - Mediante las 116 personas encuestadas, 100 que representa el 86% indicaron que a veces la administración trata adecuadamente los riesgos informáticos y 16 que corresponde al 14% aludieron que nunca lo hacen.

INTERPRETACIÓN. - Del gráfico se determina que existe un alto riesgo informático latente ya que no siempre se considera un tratamiento adecuado para la mitigación y prevención de dichos riesgos como es el caso de la elaboración de un manual con el cual se podría alertar y evitar el riesgo en la institución financiera.

8. ¿La institución cuenta actualmente con reportes de riesgo de TI?

Tabla 14: Reportes de Riesgo de TI

CATEGORIA	CANTIDAD	FRECUENCIA %
Siempre	22	19%
Casi siempre	50	43%
A veces	22	19%
Nunca	22	19%
Total	116	100%

Fuente: Encuestas
Elaborado por: El autor

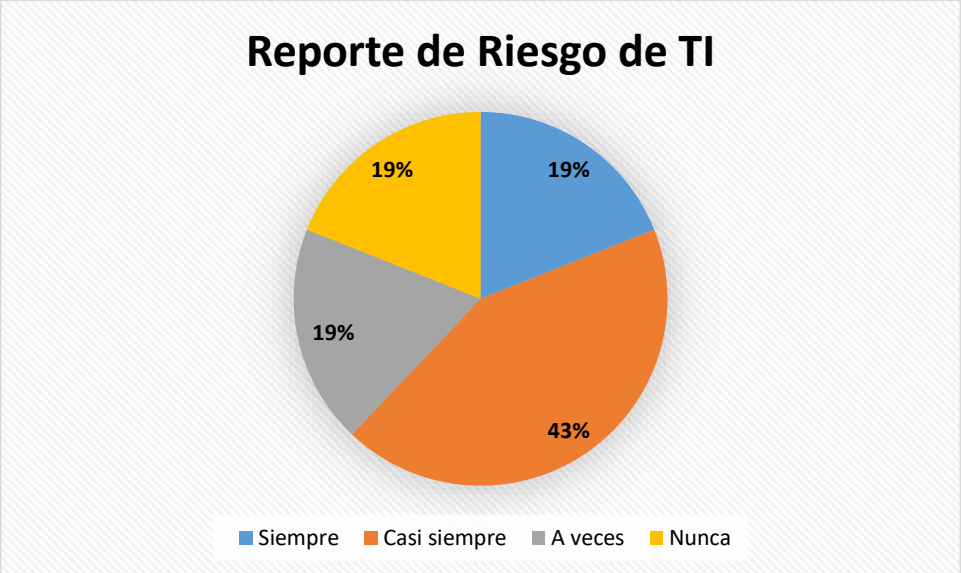


Gráfico 9: Reportes de riesgo de TI
Elaborado por: El autor

ANÁLISIS. - Con las 116 personas encuestadas, 50 que representa el 43% mencionaron que casi siempre cuentan con herramientas que emitan reportes de riesgo de TI y 22 personas que representan el 19% indicaron que siempre, a veces y nunca describen la información requerida.

INTERPRETACIÓN. - De las respuestas obtenidas se observa que la mayoría de las instituciones financieras si cuentan con estructura y reportes de riesgo de TI, sin embargo existe un considerable porcentaje de instituciones que no tienen éstos reportes, o que no los aplican regularmente.

9. ¿Se aplican medidas de control de riesgo dentro de la institución?

Tabla 15: Control de riesgo

CATEGORIA	CANTIDAD	FRECUENCIA %
Siempre	15	13%
Casi siempre	15	13%
A veces	71	61%
Nunca	15	13%
Total	116	100%

Fuente: Encuesta
Elaborado por: El autor

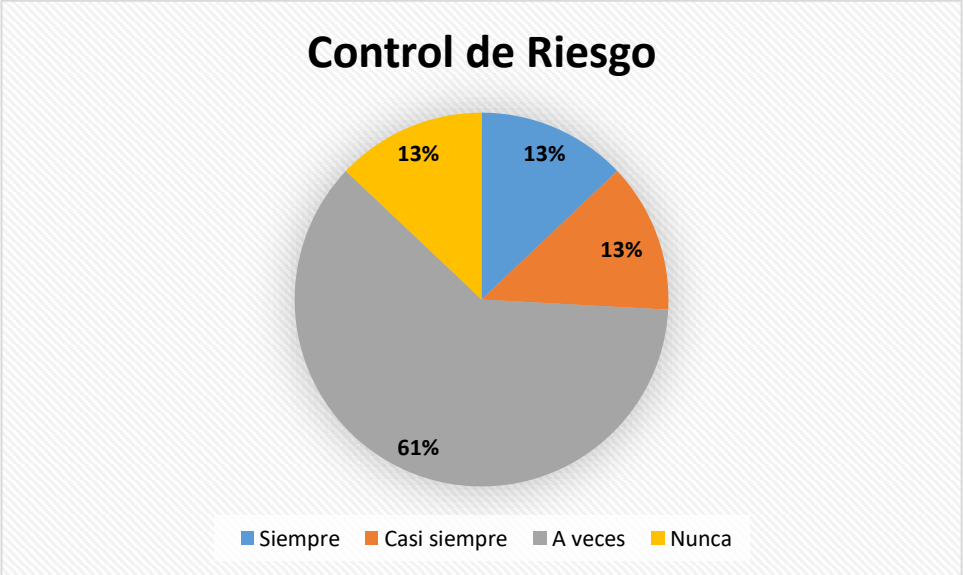


Gráfico 10: Control de riesgo
Elaborado por: El autor

ANÁLISIS. - Con las 116 personas encuestadas, 71 que representan el 61% aludieron que a veces se aplica medidas del control de riesgo y 15 que corresponde a 13% indicaron siempre, a veces y nunca lo realizan.

INTERPRETACIÓN. - De la entrevista realizada se pudo obtener que la mayoría del personal encuestado manifiesta que en la institución a veces aplican medidas de control de riesgo, siendo esto un factor negativo para la institución.

10. ¿Las instituciones financieras disponen del contingente tecnológico necesario, para su normal desenvolvimiento de sus funciones en cada departamento de la misma?

Tabla 16: Contingente Tecnológico

CATEGORIA	CANTIDAD	FRECUENCIA %
Siempre	36	31%
Casi siempre	40	34%
A veces	30	26%
Nunca	10	9%
Total	116	100%

Fuente: Encuesta
Elaborado por: El autor

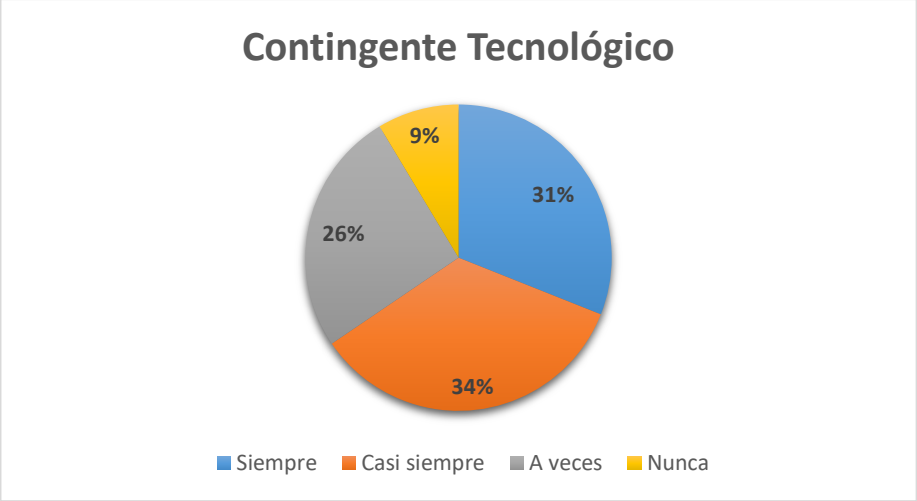


Gráfico 11: Contingente Tecnológico
Elaborado por: El autor

ANÁLISIS. - Mediante las encuestas realizadas a 116 personas, 36 que representan el 31% mencionaron que siempre dispone de la contingencia tecnológica necesaria, 40 que corresponde el 34% indicaron que siempre cuentan con este contingente, 30 personas que representan el 26% manifestaron a veces pueden contar con un contingente y 10 personas que corresponden al 9% indican que nunca han contado con un contingente tecnológico

INTERPRETACIÓN. - Con las respuestas obtenidas la mayoría de las personas indicaron que la institución cuenta con el contingente tecnológico necesario permitiéndoles desarrollar sus actividades de una forma ágil, sin embargo, un alto porcentaje mencionan que no cuentan con este tipo de contingente, provocando un alto riesgo de posible pérdida de información o daños en equipos.

11. ¿Cree usted que la aplicación de una metodología de buenas prácticas para el control de la información, reducirá el nivel de riesgo informático en las instituciones financieras?

Tabla 17: APLICACIÓN DE BUENAS PRÁCTICAS

CATEGORIA	CANTIDAD	FRECUENCIA %
Siempre	20	17%
Casi siempre	96	83%
A veces	0	0%
Nunca	0	0%
Total	116	100%

Fuente: Encuestas
Elaborado por: El autor

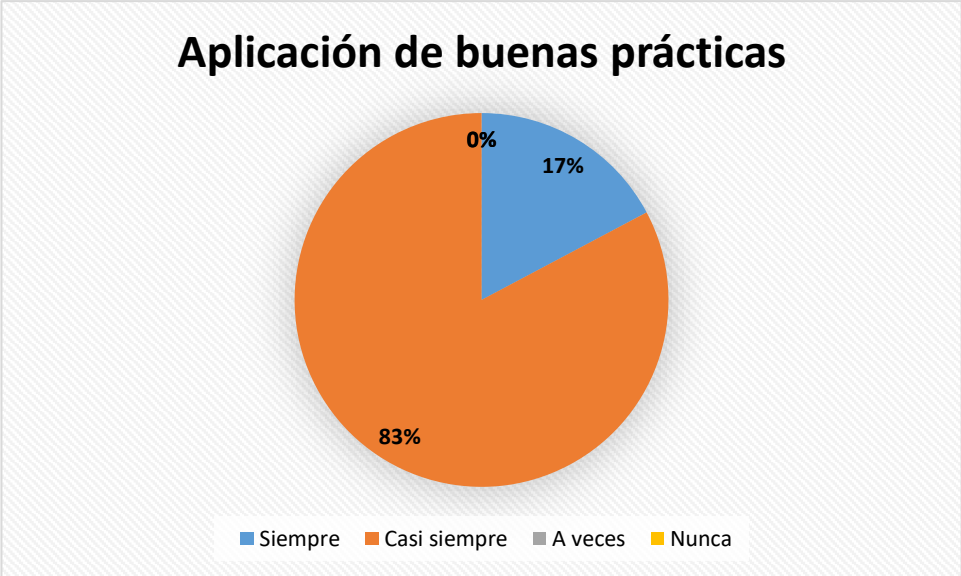


Gráfico 12: Aplicación de buenas prácticas
Elaborado por: El autor

ANÁLISIS. - De las 116 personas encuestadas, 96 que representan el 83% mencionaron que casi siempre la aplicación de una metodología de buenas prácticas para el control de la información reduciría el nivel de riesgo informático para mejorar la gestión de riesgo informático y 20 que representa un 17% indicaron que siempre lo harían.

INTERPRETACIÓN. – Las personas encuestadas piensan que es necesario aplicar una metodología de buenas prácticas para el control de la información donde ayudará a detectar vulnerabilidades y amenazas a los que se encuentran expuestos, dando una pauta para que la institución los mejore y elimine dichos factores negativos de esta manera se prevé mejorar la gestión del riesgo informático.

12. ¿Existe en la institución la planificación, diseño, desarrollo, despliegue, operación, gestión y aplicación de las TI?

Tabla 18: Aplicaciones de las TI

CATEGORIA	CANTIDAD	FRECUENCIA %
Si	30	26%
No	86	74%
Total	116	100%

Fuente: Encuestas
Elaborado por: El autor

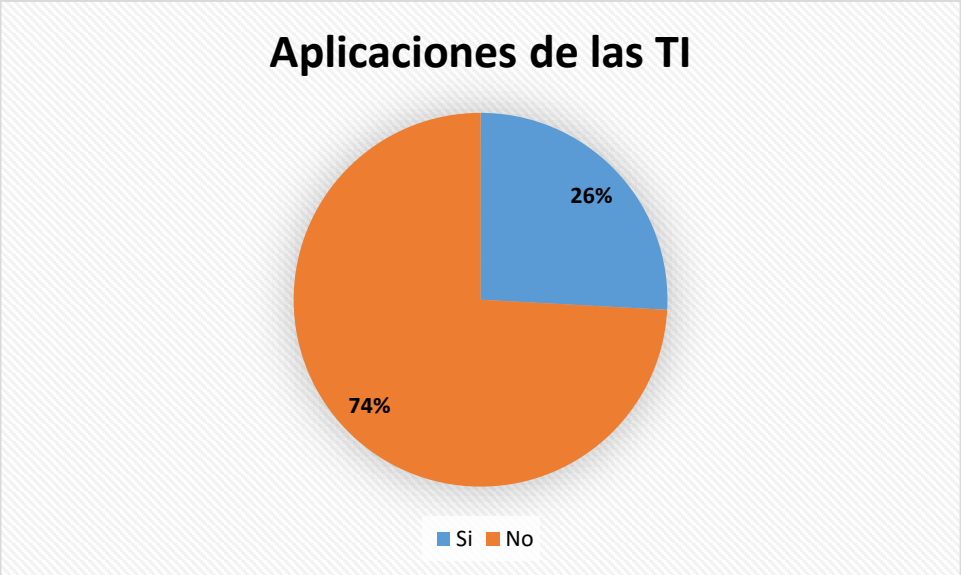


Gráfico 13: Aplicaciones de las TI
Elaborado por: El autor

ANÁLISIS. - En las 116 personas encuestadas, 86 que representan el 74% indicaron que no existe una planificación, diseño, desarrollo, despliegue, operación, gestión y aplicación de las TI y 30 que representa un 26% mencionaron que no.

INTERPRETACIÓN. - La mayoría de las personas indicaron que la institución no cuenta con una planificación, diseño, desarrollo, despliegue, operación, gestión y aplicación de las TI.

13. ¿Existe dentro de la institución un Modelo que esté basado en tareas corporativas de TI?

Tabla 19: Tareas corporativas TI

CATEGORIA	CANTIDAD	FRECUENCIA %
Si	16	14%
No	100	86%
Total	116	100%

Fuente: Encuestas
Elaborado por: El autor

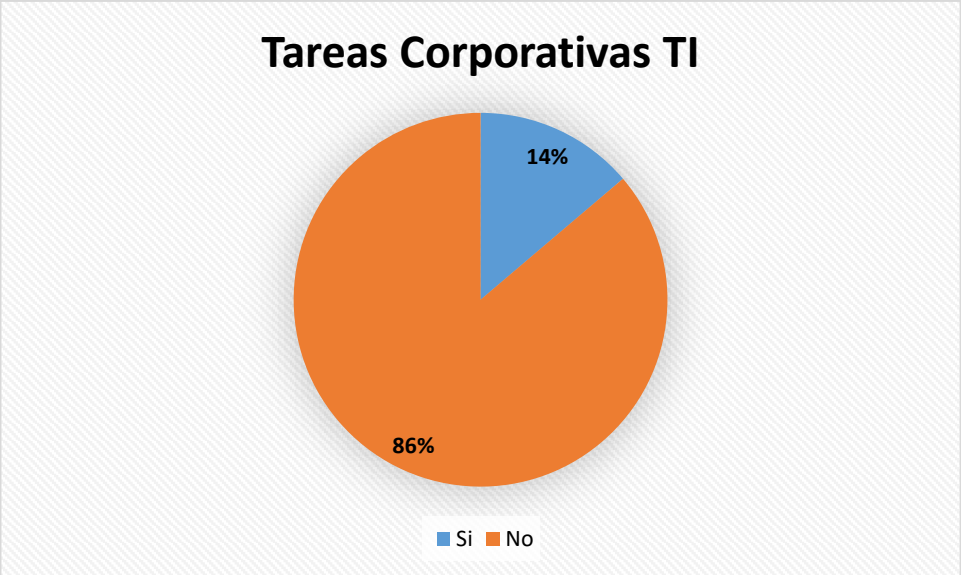


Gráfico 14: Tareas corporativas TI
Elaborado por: El autor

ANÁLISIS. - De las 116 personas encuestadas, 100 que representa el 86% aludieron que no existe un modelo basado en las tareas corporativas TI y 16 que corresponde a 14% señalaron que no.

INTERPRETACIÓN. - De los resultados obtenidos, se concluye que en las instituciones financieras no cuentan con un modelo adecuado de TI que involucre en su desarrollo tareas corporativas.

14. ¿Se encuentra el departamento de TI en el organigrama general de la cooperativa?

Tabla 20: Organigrama general

CATEGORIA	CANTIDAD	FRECUENCIA %
Si	16	14%
No	100	86%
Total	116	100%

Fuente: Encuestas
Elaborado por: El autor

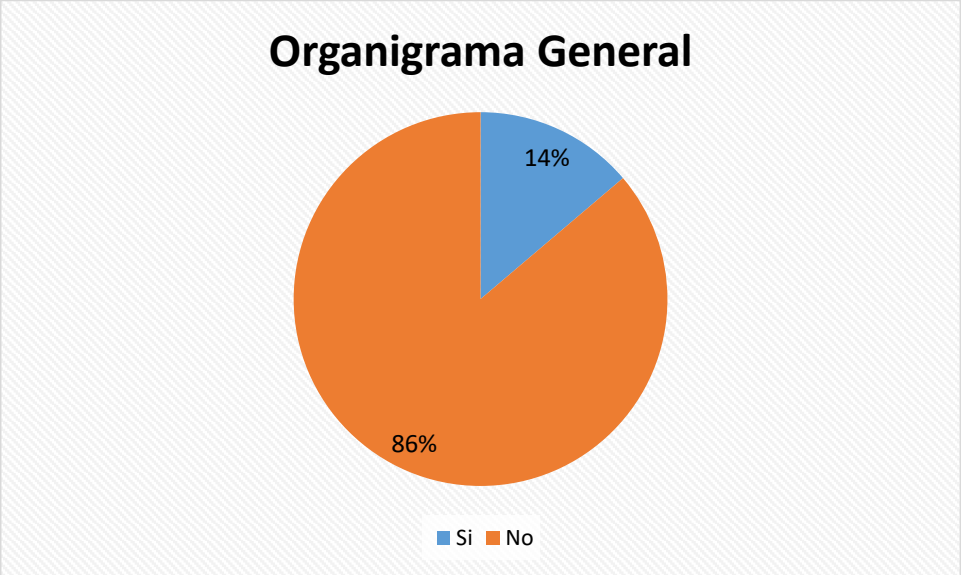


Gráfico 15: Organigrama general
Elaborado por: El autor

ANÁLISIS. - Con las 116 personas encuestadas, 16 que representan el 14% aludieron que el departamento de TI si se encuentra dentro del organigrama general de la cooperativa, mientras que 100 personas que representa el 86% manifestaron que el departamento de TI no es considerado dentro del organigrama general.

INTERPRETACIÓN. - De la investigación realizada se observa que la mayoría del personal investigado manifiesta que el departamento de TI no es considerado como parte estructural dentro de la institución.

15. ¿La institución tiene un presupuesto destinado al desarrollo y control de TI?

Tabla 21: Presupuesto destinado a TI

CATEGORIA	CANTIDAD	FRECUENCIA %
Si	16	14%
No	100	86%
Total	116	100%

Fuente: Encuestas
Elaborado por: El autor

Gráfico 16: Presupuesto destinado a TI
Elaborado por: El autor

ANÁLISIS. - Mediante las 116 encuestas aplicadas, 100 que representa un 86% indicaron que no tienen un presupuesto destinado a TI y 16 que corresponde un 14% aludieron que si cuentan.

INTERPRETACIÓN. - Con las respuestas obtenidas la mayoría de las personas indicaron que no cuentan con un presupuesto dirigido al mejor desenvolvimiento en la tecnología mediante la distribución de información, estableciendo limitantes al propio departamento de TI para solventar posibles riesgos institucionales.

4.1 Comprobación de hipótesis

Para la comprobación de la hipótesis se procederá con la prueba estadística del chi cuadrado la cual tiene la siguiente fórmula:

$$x2c = \Sigma \frac{(fo - fe)^2}{fe}$$

Donde:

fo= Frecuencia observada

fe= Frecuencia esperada

Para el desarrollo de la comprobación de hipótesis inicialmente se plantea la hipótesis de trabajo(Hi) y la hipótesis nula (Ho):

Ho = La metodología COBIT 5 **NO** incidirá en el análisis de los Riesgos Informáticos en las Cooperativas de Ahorro y Crédito de los Segmentos 2 y 3 de la ciudad de Ambato.

Hi = La metodología COBIT 5 incidirá en el análisis de los Riesgos Informáticos en las Cooperativas de Ahorro y Crédito de los Segmentos 2 y 3 de la ciudad de Ambato.

Ahora se procede a seleccionar una pregunta para la variable independiente y una para la variable dependiente con lo que se elabora una matriz cruzada, que vendría a ser la primera matriz y se denominará matriz de frecuencia observada:

Frecuencia Observada

Tabla 22. Frecuencia Observada

CATEGORIA/PREGUNTA	PREGUNTA 7	PREGUNTA 11
Si	0,00	20,00
No	0,00	96,00
Parcialmente	100,00	0,00
Desconoce	16,00	0,00

Fuente: Encuestas
Elaborado por: El autor

En base a los totales registrados en la matriz de frecuencia observada, se procede a elaborar la matriz de frecuencia esperada:

Frecuencia Esperada

Tabla 23. Frecuencia Esperada

CATEGORIA/PREGUNTA	PREGUNTA 7	PREGUNTA 11
Si	10,00	10,00
No	48,00	48,00
Parcialmente	50,00	50,00
Desconoce	8,00	8,00

Fuente: Encuestas
Elaborado por: El autor

Una vez obtenida las dos matrices se procede a elaborar la matriz para calcular nuestro Chi cuadrado calculado:

Tabla 24. Chi cuadrado

OBSERVADAS (O)	ESPERADAS (E)	O - E	(O-E)^2	(O-E)^2/E
0,00	10,00	-10,00	100,00	10,00
0,00	48,00	-48,00	2304,00	48,00
100,00	50,00	50,00	2500,00	50,00
16,00	8,00	8,00	64,00	8,00
20,00	10,00	10,00	100,00	10,00
96,00	48,00	48,00	2304,00	48,00
0,00	50,00	-50,00	2500,00	50,00
0,00	8,00	-8,00	64,00	8,00
X2C				232,00

Fuente: Encuestas
Elaborado por: El autor

Para tomar una decisión debemos relacionar con nuestro chi cuadrado tabular para lo cual necesitamos nuestro grado de libertad y nuestro alfa, nuestro alfa será de 0,95, ya que buscamos una probabilidad de ocurrencia del 95%, para nuestros grados de libertad tomamos el orden de la matriz de nuestra frecuencia observada y aplicamos la fórmula de la siguiente manera:

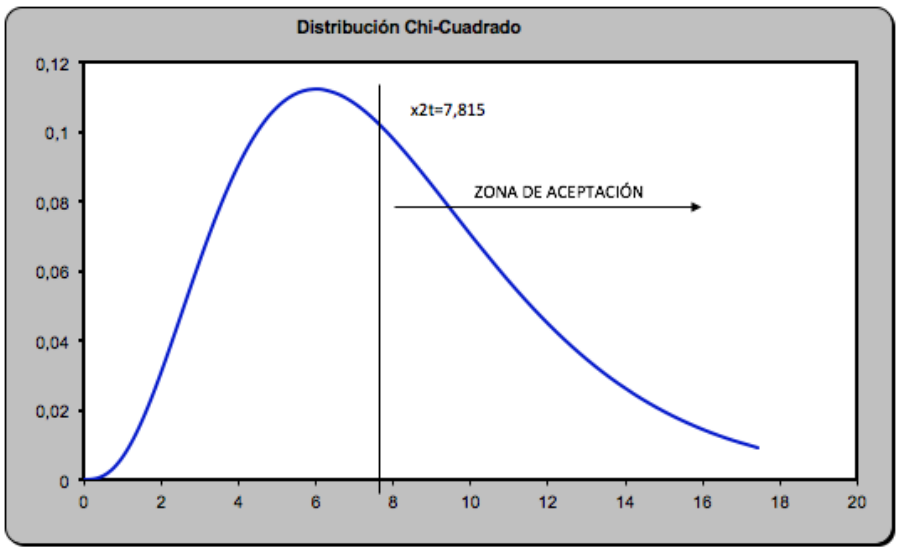
gl= (f-1)(c-1)
gl= (4-1)(2-1)
$gl = 3$

Obtenido nuestro alfa y los grados de libertad seleccionamos el valor de nuestro chi cuadrado tabular en la tabla:

n	0,995	0,99	0,975	0,95	0,9	0,75
1	7,879	6,635	5,024	3,841	2,706	1,323
2	10,597	9,210	7,378		4,605	2,773
3	12,838	11,345	9,348	7,815	,251	4,108
4	14,860	13,277	11,143		7,779	5,385
5	16,750	15,086	12,833	11,070	9,236	6,626
6	18,548	16,812	14,449	12,592	10,645	7,841
7	20,278	18,475	16,013	14,067	12,017	9,037
8	21,955	20,090	17,535	15,507	13,362	10,219
9	23,589	21,666	19,023	16,919	14,684	11,389
10	25,188	23,209	20,483	18,307	15,987	12,549
11	26,757	24,725	21,920	19,675	17,275	13,701
12	28,300	26,217	23,337	21,026	18,549	14,845

Decisión

Como nuestro chi cuadrado calculado (232,00) es mayor que nuestro chi cuadrado tabular (7,815) por ende se acepta la hipótesis de trabajo y se rechaza la nula, es decir: La implementación de la metodología COBIT 5 incidirá en el análisis de los Riesgos Informáticos en las Cooperativas de Ahorro y Crédito de los Segmentos 2 y 3 de la ciudad de Ambato.



CAPÍTULO V

5 CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones:

- Se han identificado los niveles de riesgo informáticos y se pudo determinar, mediante la encuesta realizada que: no cuentan o no conocen acerca de un manual para determinar los riesgos informáticos, donde se obtuvo un 86% en a veces y un 14% nunca, no cuentan con medidas de control de riesgo de una forma adecuada ya que se obtuvo en a veces un 61% y nunca en un 13%, cuenta con un contingente tecnológico casi siempre con un 34% y a veces 26%.

- Al analizar la situación actual de los procesos y beneficios de las TI actualmente empleadas, de los resultados obtenidos se determinaron que no existe la Planificación, diseño, desarrollo, despliegue, operación, gestión y aplicación de las TI, lo cual lo afirma la mayoría del personal investigado con un 74%, no cuentan con un modelo basado en tareas corporativas con un 86%, no cuentan con un departamento de TI con un 86%, no cuentan con un presupuesto de TI con un 86%, con respecto a si conoce y aplica las políticas de TI a veces con un 41% y nunca con un 19%.

- De los resultados que se obtuvieron de la investigación y al analizar la problemática planteada, se concluye que en las Cooperativas de Ahorro y Crédito de los segmentos 2 y 3 de la ciudad de Ambato, se ve la necesidad de implementar una metodología que permita establecer un balance entre la realización de beneficios, la utilización de recursos y los niveles de riesgo informáticos, lo cual lo podemos observar en la investigación de campo ya que al indagar acerca si la aplicación de una metodología de buenas prácticas para el control de la información, reducirá el nivel del riesgo informático con un 17% en siempre y 83% en casi siempre.

5.2 Recomendaciones:

- Al personal de Sistemas se recomienda mejorar la gestión de las TI de las instituciones para no incurrir en un riesgo operativo e informático elevado.

- Gerencia deberá coordinar con personal de empresas calificadas la adecuada capacitación al personal de las instituciones financieras acerca de la importancia de las TI y su debido control para disminuir el riego operativo.

- Al personal de TI se recomienda aplicar una metodología que permita definir los procesos más adecuados para disminuir los niveles de riesgos tecnológicos en las instituciones financieras.

- A gerencia se recomienda aplicar un modelo de buenas prácticas para la gestión de los riesgos informáticos en las Cooperativas de Ahorro y Crédito de los segmentos 2 y 3 de la ciudad de Ambato.

- Al personal de Riesgos se recomienda elaborar las políticas internas que incluyan el control y la gestión del riesgo informático.

- Auditoría debe realizar un monitoreo del modelo de gestión de los riesgos informáticos.

CAPÍTULO VI

PROPUESTA

6.1 Datos Informativos:

6.1.1 Tema:

Gestión de los riesgos informáticos en la Cooperativa de Ahorro y Crédito Indígena SAC utilizando la Metodología COBIT 5.

6.1.1 Instituciones Beneficiarias:

Cooperativa de Ahorro y Crédito Indígena SAC Ltda.

6.1.2 Ubicación:

Ambato - Ecuador

6.1.3 Equipo técnico responsable:

El investigador

6.1.4 Financiamiento:

La investigación en su totalidad será autofinanciada por el autor del mismo.

6.2 Antecedentes:

6.2.1. Antecedentes investigativos

Como menciona Vanegas & Pardo (2014, págs. 37-46) Es un marco de referencia internacional aceptado por la mayoría de empresas como buenas prácticas para el control interno de la información. COBIT ha sido diseñado para facilitar el uso de las TI desde un enfoque de inversión que debe estar bien administrado y está basado en los estándares y las mejores prácticas de la industria, y ayuda a salvar la brecha entre los riesgos del negocio, las necesidades de control y los aspectos propiamente técnicos.

COBIT provee de buenas prácticas, gracias a un marco de dominios: planificar y organizar; adquirir e implementar; entrega y soporte; y monitorear y evaluar (EAFIT, 2007). Mencionando las siguientes características:

- El análisis realizado permitió evidenciar que la mayoría de las normas y modelos aquí descritas están relacionados entre sí, aunque algunas normas presentan procesos más detallados, con un nivel más profundo que otros modelos. Asimismo, se observó que hay normas y modelos con similitudes en la definición de sus procesos, tales como actividades similares entre sí. Por otra parte, también se encontraron algunas actividades que complementaban y mejoraban las descripciones de otras actividades, dando como resultado la característica en la que un modelo es capaz de soportar a otro modelo.

- La gestión de riesgos permite evitar el fracaso de proyectos de desarrollo de software, estimulando la terminación del mismo de modo que se incrementa la calidad en los proyectos entregados, reduciendo costos y cumpliendo con las necesidades del cliente, lo que impacta positivamente en su satisfacción. Una buena gestión de riesgos tiene como habilidad entregar a tiempo los productos esperados a partir de las metas que se plantearon y con el cronograma de actividades establecido.

- Esta metodología, aunque no es oficial, esta soportada por las actividades que están descritas en los procesos de gestión de riesgos definidos en normas y estándares certificados y avaladas por organismos internacionales como la ISO, IEC, ISACA e ICONTEC, entre otros, lo que permite fácilmente certificarse en algunos de los modelos existentes que la conforman. La implementación de estos procesos determina, de alguna manera, seguir las prácticas que permitan cumplir con los atributos de calidad, alcanzando con éxito los objetivos de las organizaciones o la terminación de un proyecto de desarrollo de software.

Según Mora, León, Huilcapi & Escobar (2017) El desarrollo informático de las organizaciones representa el progreso en el logro de las metas de las organizaciones. El COBIT 5, es un modelo para auditar la gestión y el control de los sistemas de

información y tecnología, orientado a todos los sectores de una organización, es decir, administradores de las tecnologías de información (TI), usuarios y, por supuesto, a los auditores involucrados en el proceso. Indicando las siguientes conclusiones:

- Los sistemas de información representan la oportunidad para el logro de los objetivos organizaciones en congruencia con sus metas corporativas, metas de tecnologías de la información y las metas de los catalizadores, es prioridad de los administradores de sistemas informáticos y del gobierno corporativo realizar todas las acciones necesarias para lograrlas.

- COBIT 5 proporciona una visión integral y sistémica del gobierno y la gestión de la empresa TI basada en varios catalizadores. Los catalizadores son para toda la empresa y extremo a extremo, es decir, todo y a todos, internos y externos, que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionada, incluyendo las actividades y responsabilidades tanto de las funciones TI como de las funciones de negocio.

Para Martínez (2017, págs. 2-15) Este estudio propone una metodología de seguridad de la información para la gestión del riesgo informático aplicable al entorno empresarial y organizacional del sector MPYME ecuatoriano. Para el efecto, se analizan comparativamente varias metodologías de amplia divulgación, como: Magerit, CRAMM (CCTA Risk Analysis and Management Method), OCTAVE-S, Microsoft Risk Guide, COBIT 5 y COSO III. Estas metodologías son internacionalmente utilizadas en la gestión del riesgo de información; a la luz de los marcos de referencia de la industria: ISO 27001, 27002, 27005 y 31000. Mencionando las siguientes conclusiones:

- La retroalimentación de cada una de las metodologías estudiadas ha permitido asimilar las mejores cualidades y características de cada una, en las que se ha podido comprobar que la gestión de riesgos se resume en la identificación y valoración de los activos de información, la identificación y valoración de amenazas, el cálculo de riesgos, la identificación de contramedidas y el manejo del

riesgo residual; recalcando que cada una de ellas adopta las mejores prácticas de las ISO27001, 27002, 27005 y 31000; utilizadas para la gestión de la seguridad de la información y la gestión del riesgo.

- Tal como lo establece COBIT, ECU@Risk analiza aspectos relacionados con las estructuras organizativas, donde para cada empresa tendrá definida una estructura variada; y que, en función de su composición y ámbito de decisiones, las mismas podrán ubicarse en el área de gobierno o en el de gestión.

- ECU@Risk está alineada a la normativa vigente, en la que se ha considerado el análisis de los aspectos legales, partiendo del estudio de regulaciones internacionales y compararla con las leyes ecuatorianas, en las que se ha podido ver, de manera inicial, un bajo nivel de madurez en estas últimas. Las acciones que ECU@Risk considera en sus todos sus procesos son legales, pues se encuentran dentro del marco normativo vigente y no a la voluntad de cada persona, tema que fue discutido por Jaramillo Palacios en el 2014 (García Falconí, 2011). Además, cumple con la "calidad de los textos normativos", ya que incluye procedimientos claros que no van contra de la Constitución de la República del Ecuador. ECU@Risk puede ser de interés público y estar disponible en formatos accesibles para los solicitantes e interesados en él, considerando siempre los derechos de propiedad intelectual.

- Es vital que las MPYMES dentro de su marco legal organizacional considere crear conciencia a los usuarios y público en general; recolectar constantemente estadísticas y datos sobre incidentes informáticos, y registrarlos en bitácoras de control; establecer planes de capacitación continua al personal implicado en la seguridad de la información, además de una actualización permanentemente del marco normativo que contiene las políticas de seguridad de la información; y sobre todo la concienciación y compromiso de la alta gerencia.

- Dentro del tratamiento de riesgos se han propuesto aspectos que deberían considerarse en la elección de contramedidas, conociendo que estas deberán ser alcanzables, aplicables, aceptables, además de medibles y registrables. Las

políticas de seguridad resultantes de la aplicación de esta metodología, aportarán a las decisiones de gobierno que deben ser sancionadas en la empresa.

6.2.2. Análisis de las falencias de la COAC en TI

Al analizar la encuesta aplicada al personal de las COAC del segmento 2 y 3 de la ciudad de Ambato en lo referente a TI se pudo determinar el siguiente nivel de riesgo tomando en cuenta la siguiente escala:

Tabla 25. Simbología

NIVEL DE RIESGO	
ALTO (Nunca) (No)	
MODERADO (Casi Siempre y A veces)	
ACEPTABLE (Siempre) (Si)	

Fuente: Encuestas
Elaborado por: El autor

Matriz resumen de la investigación realizada mediante la técnica de la encuesta con el instrumento del cuestionario:

Tabla 26. Consolidado encuesta

No.	ITEM	CATEGORIA			
		Siempre	Casi Siempre	A Veces	Nunca
3	Las herramientas informáticas que utiliza en la institución, ya sean estas para el manejo de la información financiera y contable, información administrativa, u otra información sirven de apoyo para la toma de decisiones.	7	7	86	0
4	La institución cuenta con un diseño de procesos que recoja las necesidades de las partes interesadas tanto internas como externas	6	6	69	19
5	La información que se obtiene de los clientes o socios de la institución financiera es la necesaria para un real conocimiento de los socios	16	16	68	0
6	El personal de la institución conoce y aplica las políticas elaboradas por TI	0	40	41	19
7	La administración realiza un tratamiento adecuado para mitigar los riesgos informáticos en la institución	0	0	86	14
8	La institución cuenta actualmente con reportes de riesgo de TI	19	43	19	19
9	Se aplican medidas de control de riesgo dentro de la institución	13	13	61	13
10	Las instituciones financieras disponen del contingente tecnológico necesario, para su normal desenvolvimiento de sus funciones en cada departamento de la misma	31	34	26	9
11	Cree usted que la aplicación de una metodología de buenas prácticas para el control de la información, reducirá el nivel de riesgo informático en las instituciones financieras	17	83	0	0

Fuente: Encuestas
Elaborado por: El autor

Tabla 27. Consolidado encuesta

No.	ITEM	CATEGORIAS	
		SI	NO
1	La Cooperativa cuenta con un manual de funciones para el personal de la misma	66	34
2	La información de los procedimientos para el desarrollo de sus funciones es entendible y de su conocimiento	57	43
12	Existe en la institución la planificación, diseño, desarrollo, despliegue, operación, gestión y aplicación de las TI	26	74
13	Existe dentro de la institución un Modelo que esté basado en tareas corporativas de TI	14	86
14	Se encuentra el departamento de TI en el organigrama general de la cooperativa	14	86
15	La institución tiene un presupuesto destinado al desarrollo y control de TI	14	86

Fuente: Encuestas
Elaborado por: El autor

En las tablas 26 y 27, se observa el consolidado de las encuestas, en las cuales se puede visualizar los respectivos porcentajes obtenidos en cada opción de respuesta de cada pregunta.

Tabla 28. Tendencias encuesta

No.	ITEM	CATEGORIA			
		Siempre	Casi Siempre	A Veces	Nunca
3	Las herramientas informáticas que utiliza en la institución, ya sean estas para el manejo de la información financiera y contable, información administrativa, u otra información sirven de apoyo para la toma de decisiones.			X	
4	La institución cuenta con un diseño de procesos que recoja las necesidades de las partes interesadas tanto internas como externas			x	
5	La información que se obtiene de los clientes o socios de la institución financiera es la necesaria para un real conocimiento de los socios			x	
6	El personal de la institución conoce y aplica las políticas elaboradas por TI			x	
7	La administración realiza un tratamiento adecuado para mitigar los riesgos informáticos en la institución			x	
8	La institución cuenta actualmente con reportes de riesgo de TI		x		
9	Se aplican medidas de control de riesgo dentro de la institución			x	
10	Las instituciones financieras disponen del contingente tecnológico necesario, para su normal desenvolvimiento de sus funciones en cada departamento de la misma		x		
11	Cree usted que la aplicación de una metodología de buenas prácticas para el control de la información, reducirá el nivel de riesgo informático en las instituciones financieras		x		

Fuente: Encuestas
Elaborado por: El autor

Tabla 29. Tendencias encuesta

No.	ITEM	CATEGORIAS	
		SI	NO
1	La Cooperativa cuenta con un manual de funciones para el personal de la misma	x	
2	La información de los procedimientos para el desarrollo de sus funciones es entendible y de su conocimiento	X	
12	Existe en la institución la planificación, diseño, desarrollo, despliegue, operación, gestión y aplicación de las TI		X
13	Existe dentro de la institución un Modelo que esté basado en tareas corporativas de TI		X
14	Se encuentra el departamento de TI en el organigrama general de la cooperativa		X
15	La institución tiene un presupuesto destinado al desarrollo y control de TI		x

Fuente: Encuestas
Elaborado por: El autor

En las tablas 28 y 29, se determinó las tendencias en las respuestas en cada pregunta, de la misma manera se las sitúa en la zona de riesgo en la cual pertenecen de acuerdo a la escala de colores de la tabla 25.

Tabla 30. Nivel de Riesgo

NIVEL DE RIESGO	
ALTO	27,00%
MODERADO	60,00%
ACEPTABLE	13,00%

Fuente: Encuestas
Elaborado por: El autor

Como observación general se puede decir que las instituciones del segmento 2 y 3 en lo referente a las TI, tienen un Nivel de riesgo operativo del 60,00% siendo este moderado como lo se puede visualizar en la tabla 30.

6.3 Justificación:

La presente propuesta, nace de la necesidad de dar solución a la problemática de investigación planteada la cual denota gran interés de aplicar una metodología para las buenas prácticas de TI por parte de las instituciones financieras del segmento 2 y 3 de

la ciudad de Ambato, pero con fines aplicativos la propuesta se realizará en la Cooperativa de Ahorro y Crédito Indígena SAC Ltda. Al aplicar la metodología COBIT 5 se pretende reducir significativamente el impacto de los riesgos informáticos, logrando de esta manera tener una mayor seguridad en la información que se maneja o se transmite en la institución financiera, dando mayor confianza y veracidad a sus socios y a la institución en sí de la información con la que se cuenta.

6.4 Objetivos:

6.4.1 Objetivo General

Aplicar la metodología COBIT 5 para la gestión de los riesgos informáticos en la Cooperativa de Ahorro y Crédito Indígena SAC.

6.4.2 Objetivos Específicos

- Determinar los niveles de riesgo operativos en las instituciones financieras.
- Determinar los procesos de TI más adecuados para la disminución de riesgos tecnológicos en la institución financiera.
- Determinar los alcances de los Procesos de TI.
- Elaborar el manual de Buenas Prácticas de TI.

6.5 Análisis de factibilidad:

Para el desarrollo de la presente propuesta, se cuenta con el interés y la aprobación del personal administrativo de la Cooperativa de Ahorro y Crédito Indígena SAC Ltda. La institución facilitará la información necesaria para la elaboración de la misma. Para su desarrollo se cuenta con el recurso tecnológico necesario, el talento humano, así como el conocimiento requerido para lograr un trabajo de calidad.

6.5.1 Factibilidad Técnica

Se cuenta con la factibilidad técnica y tecnológica ya que se contó con las herramientas tecnológicas tanto en software como en hardware, para el desarrollo de la actual propuesta.

6.5.2 Factibilidad Operativa

Al contar con el interés y la aprobación de los involucrados en la investigación así como los conocimientos necesarios y al existir la información necesaria de otros autores e investigadores acerca de la temática de dicha propuesta la realización operativa de la propuesta es factible.

6.5.3 Factibilidad Económica

Todo los gastos económicos correrán por el autor de la investigación por lo cual es factible económicamente.

6.6 Fundamentación:

6.6.1 Riesgo operativo

Como menciona Martínez (2008, pág. 862) El riesgo operativo, también llamado riesgo operacional se puede definir como el riesgo de que se presente pérdidas por fallas en los sistemas administrativos y procedimientos así como errores humanos, intencionales o no. Ejemplos de eventos de riesgo operativo son: fallas en “hardware”, “software” y telecomunicaciones: errores de captura, ejecución y mantenimiento de transacciones; fallas en sistemas de seguridad: pérdida parcial o total de bases de datos sobre operaciones con clientes; fraudes internos: robo, daños a los activos fijos; reembolso a clientes y pagos de penalización; restricciones legales que pudieran fomentar el incumplimiento de las obligaciones de clientes (riesgo legal); documentación incompleta de clientes; restricciones impuestas por las autoridades financieras para participar en ciertos mercados o segmentos de mercado. Existen tres aspectos en la administración de riesgos operativos.

- El primero consiste en la asignación de capital para hacer frente a eventos relacionados con fallas operativas.
- El segundo aspecto toma en cuenta la supervisión y control para evitar que se presenten dichas fallas.
- El tercero considera los modelos y métodos utilizados para cuantificar el riesgo operativo.

Para Núñez & Chávez (2010, pág. 125) Riesgo operativo se define como el riesgo de pérdida debido a las deficiencias o a fallas de los procesos, el personal y los sistemas internos, o bien a causa de acontecimientos externos. El tipo y frecuencia de eventos que abarca es muy diverso. Del riesgo operativo se pueden destacar las siguientes características:

- El riesgo operativo es el más antiguo de todos y está presente en cualquier clase de negocio y casi en toda actividad; es inherente a toda actividad en que intervengan personas, procesos y plataformas tecnológicas; es complejo, como consecuencia de la gran diversidad de causas que lo originan; y las grandes pérdidas que ha ocasionado a la industria financiera muestran el desconocimiento que de él se tiene y la falta de herramientas para gestionarlo.
- Es conveniente indicar en este punto la principal diferencia relevante para el modelado del riesgo: en tanto que en el riesgo operativo las pérdidas ocurren durante una ventana dada, en el riesgo legal aparte de los eventos esperados que suceden con determinada frecuencia (para cuyos parámetros utilizamos información histórica), existen eventos en curso (demandas) cuya conclusión en pérdida es incierta, pero incluye una probabilidad de que suceda.

El riesgo operativo puede definirse, a grandes rasgos, como la posibilidad que tiene una compañía, empresa u organización de sufrir pérdidas de carácter financiero por diversas causas. Para evitar estos riesgos o minimizar sus consecuencias es recomendable poner en marcha un Sistema de Gestión de Riesgos basado en ISO 31000 para poder hacer frente con mayores garantías a las amenazas provocadas por fallos o insuficiencias en las personas, procesos, tecnología, sistemas internos, cuestiones legales y eventos externos imprevistos. ISOtools (2015)

6.6.2 Principales factores de riesgo operativo

Como menciona ISOtools (2015) Los riesgos operativos se dan, sobre todo, en 4 ámbitos distintos:

1. Recursos humanos

- Pérdidas financieras asociadas con negligencia, error humano, sabotaje, fraude o robo.
- Apropiación indebida de información sensible.
- Lavado de dinero.
- Ambiente laboral desfavorable.
- Errores o falta de las especificaciones necesarias en los términos de contratación del personal, entre otros factores.
- Inadecuada selección de personal por no identificar claramente el perfil que necesita la empresa en cada momento o selección de personas con competencias insuficientes o capacitación inadecuada.
- Formación de personal errónea o insuficiente.

2. Procesos Internos

- Diseño inapropiado de los procesos críticos de la organización.
- Políticas y procedimientos inadecuados o inexistentes.
- Desarrollo deficiente de las operaciones.
- Fallos de infraestructura o logísticos o que lleva a la suspensión (temporal o permanente) de la producción o la ejecución de servicios.
- Riesgos asociados a fallos en los modelos utilizados.
- Errores en las transacciones.
- Evaluación inadecuada de contratos.

- Errores de contabilidad.
- Fallos en los cálculos de los recursos necesarios para determinadas operaciones
- Incumplimiento de plazos.
- Presupuestos mal calculados o diseñados.
- Deficiencias en los procesos de gestión de documentación.

3. Tecnología de Información

- Ataques informáticos que provoquen el robo de datos de la propia empresa o de terceros.
- Fallos de hardware o software.
- Mal funcionamiento o selección incorrecta de las herramientas informáticas de la empresa.
- Pérdidas financieras derivadas del uso de inadecuados sistemas de información y tecnologías.
- Anormal desarrollo de operaciones y servicios que realiza la compañía por fallos informáticos.
- Pérdida de información o de material informático (hardware y software) por contingencias como: incendios, inundaciones o averías graves.
- Riesgos derivados a fallas en la seguridad y continuidad operativa de los sistemas informáticos.
- Errores en el desarrollo e implementación de dichos sistemas y/o su compatibilidad e integración.
- Problemas de calidad de información.
- Inadecuada inversión en tecnología.

- Falla o interrupción de los sistemas.
- Recuperación inadecuada de desastres y/o la continuidad de los planes de negocio.

4. Eventos externos

- Contingencias legales.
- Fallas en los servicios públicos.
- Desastres naturales, atentados y actos delictivos.
- Cambios en las leyes y normativos.
- Riesgo político del país.
- Revueltas sociales.

Según Calle (2019) Existen algunos factores de riesgo operativo que deben ser considerados por las organizaciones:

- Recursos humanos. - Uno de los factores de riesgo operacional son las actividades desempeñadas por las personas, ya sea por la competencia, conducta ética o atribuciones que tenga un funcionario.
- Falta de segregación de funciones.- Uno de los principios de control interno de una empresa es la segregación de funciones. Esta consiste en separar las actividades para que las responsabilidades de una o varias áreas de la compañía no recaigan en una sola persona. De ese modo ningún funcionario debe gestionar todas las etapas de una transacción.
- Administración de usuarios y contraseñas. - Los sistemas, la infraestructura, la disponibilidad de almacenamiento y el procesamiento de la red de una empresa son factores de riesgo operacional.
- Falla en los procesos.- Los flujos o las etapas de desarrollo de productos o servicios, así como el registro interno de clientes o las transacciones que no han sido ingresadas de forma correcta en el sistema pueden originar un posible riesgo operativo.

6.6.3 Como se mide el riesgo operativo

Como menciona Haro (2005, pág. 208) Para estar en posibilidad de medir el riesgo operativo y calcular una suerte de valor en riesgo (VaR) operativo, es necesario modelar el grado de severidad de la perdida esperada asumiendo que los factores de riesgo son estables. Como en riesgos de mercado, es posible determinar algunos factores de riesgos operativos que deben ser atendidos en términos de su histograma de frecuencias y por tanto de su distribución de probabilidad. Basados en datos históricos, los analistas de riesgos deben inferir cual es la curva de distribución de probabilidad más adecuada. Existen dos tipos de distribución de probabilidad a utilizar:

a) Distribuciones empíricas: utilizan la distribución de frecuencia con base en datos históricos reales. Se asemejan al método de simulación histórica, es decir, no requiere asumir algún tipo de distribución de probabilidad específica.
b) Distribuciones paramétricas: utilizan una distribución espontanea, de Poisson, Beta binomial o de Weibull, las cuales contienen fuertes supuestos matemáticos en el comportamiento de los factores de riesgo. Estas distribuciones deben ser consideradas si los datos se aproximan a alguna de estas distribuciones y sobre todo, la experiencia debe sugerir la aplicación de alguna de ellas de acuerdo con el problema específico de que se trate.

6.6.4 Proceso

Para Alonso (2014, págs. 28-29) Los procesos, se pueden definir como secuencias ordenadas y lógicas de actividades de transformación, que parten de unas entradas (datos, especificaciones, máquinas, equipos, materias primas, consumibles, etc.), para alcanzar unos resultados programados, que se entregan a quienes los han solicitado, esto es, los clientes de cada proceso. Donde:

- Procesos: Son cada una de las acciones que intervienen y se interrelacionan en el sistema y que permiten la evolución del ciclo de vida de la información, donde las entradas a un proceso del sistema pueden constituir la salida de otro y a la inversa.

- Entradas: Se definen por las necesidades de las personas y las fuentes de información procedentes, tanto internas como externas.
- Salidas: Constituyen la conclusión del ciclo de vida de la información, posibilitan disponer de productos y servicios de información con valor añadido y deben garantizar la satisfacción de las necesidades de la comunidad de usuarios a la que se vincula el sistema con las exigencias de calidad que ellos demandan o necesitan.
- Flujo de información: Es el tránsito de la información, desde las entradas por cada uno de los procesos, hasta las salidas. En el paso de la información, desde las entradas a las salidas, intervienen una serie de procesos ordenados que se relacionan estrechamente por medio de diversos flujos, con vista a que el usuario obtenga una nueva información de valor añadido. Cualquiera de estos cuatro componentes se vincula con diversos recursos: humanos, físicos, materiales y tecnológicos (hardware y software) e información en su acepción más amplia.

6.6.5 Tipo de procesos

Según Alonso (2014, pág. 36) Para detectar los procesos asociados a una determinada organización, es necesario reflexionar previamente en las posibles agrupaciones en las que pueden encajar los procesos identificados. Mediante lo siguiente:

- Procesos Estratégicos
- Procesos Clave u Operativos
- Procesos de Soporte o Apoyo

6.7 Propuesta

Análisis preliminar

Reseña Histórica

Cooperativa de Ahorro y Crédito Indígena SAC Ltda. De la Ciudad de Ambato, es una cooperativa con 36 años de experiencia en el mercado financiero, se estableció en Abril

de 1982, en el sector Palugsha, perteneciente a la parroquia Pilahuín del Cantón Ambato, se reúnen los líderes indígenas de la provincia de Tungurahua, para analizar su situación económica. Luego de varias de liberaciones, deciden crear el servicio de ahorro y crédito (SAC), con el propósito de luchar por una vida digna, libre de explotación y marginamiento. La Cooperativa de Ahorro y Crédito Indígena "SAC" Ltda. es una organización Indígena de intermediación financiera con enfoque social, orientada a mejorar las condiciones de vida, satisfacer las necesidades, expectativas de la población indígena, campesina, urbano marginal, en la actualidad cuenta con aproximadamente 40mil socios; mediante la prestación e innovación de productos financieros integrales de calidad, dentro de los principios, valores cristianos, buscando permanentemente el desarrollo integral, equitativo de su talento humano y un modelo de administración eficiente.

Misión

Mejorar la calidad de vida de nuestros socios

Visión

En el año 2020, llegar al segmento 1 con los mejores indicadores financieros

Valores

- Equidad: Dar a cada uno lo que se merece en función de sus méritos o condiciones.

- Confianza: que los socios crean en la cooperativa y tengan seguridad.

- Responsabilidad: Cumplimiento de las obligaciones adquiridas que nos ayuda a comprometernos y a actuar de una forma correcta.

- Honestidad: Respetar las normas establecidas por la institución, es decir la verdad, ser justos e íntegros.

Marco COBIT 5

COBIT es un marco de gobierno de las tecnologías de información que proporciona una serie de herramientas para que la gerencia pueda conectar los requerimientos de control con los aspectos técnicos y los riesgos del negocio. Isaca (2013)

Permite el desarrollo de las políticas y buenas prácticas para el control de las tecnologías en toda la organización. Enfatiza el cumplimiento regulatorio, ayuda a las organizaciones a incrementar su valor a través de las tecnologías, y permite su alineamiento con los objetivos del negocio. Isaca (2013)

Continuamente aumentan y se complican más los requisitos externos, tanto legales como de cumplimiento regulatorio y contractual, relacionados con el uso de la información y la tecnología en la Organización, amenazando su patrimonio si no se cumplen. Isaca (2013)

COBIT5 proporciona un marco integral, alineado con los principales estándares de control y auditoría, ayudando a las Organizaciones a lograr sus metas y entregar valor mediante un gobierno y una administración efectivos de la TI de la Organización. Ayuda a las Organizaciones a crear un valor óptimo a partir de la TI, al mantener un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos. Isaca (2013)

COBIT 5 une los cinco principios que permiten a la Organización construir un marco efectivo de Gobierno y Administración basado en una serie holística de siete habilitadores, que optimizan la inversión en tecnología e información, así como su uso en beneficio de las partes interesadas. Isaca (2013)

Como menciona Isaca (2013) Los principios y habilitadores de COBIT 5 son genéricos y útiles para las Organizaciones de cualquier tamaño, bien sean comerciales, sin fines de lucro o en el sector público.

Gráfico 17: Principios de COBIT 5
Fuente: ISCA

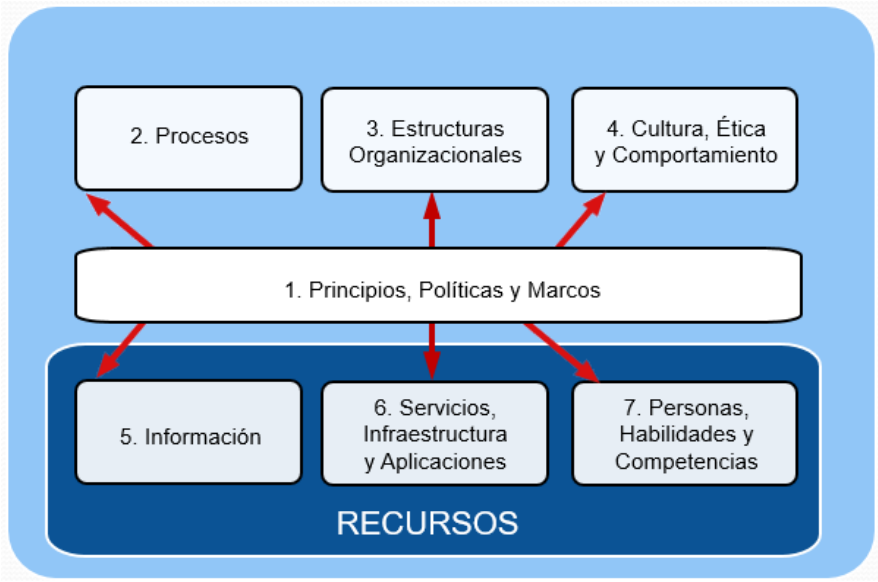


Gráfico 18: Habilidades de COBIT 5
Fuente: ISACA

Principios del COBIT 5

Para Medina (2017, pág. 134) Es la creación de valor a través del uso efectivo e innovador de las tecnologías de la información. Ante todo, es un "marco de negocios" con una visión de arriba hacia abajo respecto a las necesidades de negocio que crean una cascada de metas, proporciona un lenguaje común para la empresa y gestión TI. Las organizaciones logran construir un marco efectivo de gobierno y administración a partir de los principios que optimizan la inversión en tecnologías de información, así como su uso en beneficio de las partes interesadas que son los siguientes:

- Satisfacer las necesidades de las partes interesadas: este principio establece que todas las organizaciones existen para crear valor para sus partes interesadas, el sistema de gobierno debe considerar a todas las partes interesadas para poder tomar decisiones con respecto a la evaluación de riesgos, los beneficios y el manejo de recursos. Además permite definir las prioridades para implementar y asegurar el gobierno corporativo de las TI, con base en los objetivos de la organización y los riesgos relacionados.
- Cubrir la organización del extremo a extremo: COBIT 5 cubre todas las funciones y los procesos dentro de la organización, no solamente se concentra en la función de las TI, sino trata las tecnologías de la información y relacionadas como activos que necesitan ser manejados como cualquier otro activo, por todos en la organización.
- Aplicar un marco de referencia único integrado: COBIT 5 está alineado con los últimos marcos y normas relevantes usados por las organizaciones a nivel corporativo: COSO, COSO ERM, ISO/IEC 9000. ISO/IEC 31000 y relacionado con TI: ISO/IEC 3800, ITIL, ISO/IEC 27000, TOGAF, PMBOK/ PRINCE2, CMMI, entre otros.
- Hacer posible un enfoque holístico: un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define un conjunto de catalizadores para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. El marco de trabajo COBIT 5 define siete categorías de catalizadores:
    - Principios, políticas y marcos de trabajo

- Procesos
- Estructuras organizativas
- Cultura, ética y comportamiento
- Información
- Servicios, infraestructuras y aplicaciones
- Personas, habilidades y competencias.

- Separar el gobierno de la gestión: el marco de COBIT 5 plasma una distinción muy clara entre el gobierno y la administración.

Habilitadores de COBIT 5

Para Medina (2017, pág. 136) Los habilitadores de COBIT 5 son:

1. Los propósitos en este habilitador son:

- Trasmitir la dirección e instrucciones de los cuerpos de gobierno y dirección.
- Comunicar las reglas de la corporación
- Soportar los objetivos de gobierno y valores de la corporación definidos por el consejo y dirección ejecutiva.

2. Los principios deben ser limitados en número y expresar claramente los valores de la empresa, mientras que las políticas son una guía más detallada para llevar a la práctica los principios. Un marco de referencia de políticas que describa:

- Alcance y validez
- Consecuencias por fallar en cumplir de la política
- Formas de manejar las excepciones
- Formas en la cual una política se mide y verifica

Estructuras organizativas

Como menciona Medina (2017, pág. 36) Buenas prácticas de estructuras organizativas:

- Principios operacionales: Los acuerdos prácticos relacionados con la forma como la estructura operara la frecuencia de las reuniones, la documentación y otras reglas.

- Alcance de control: Las fronteras de los derechos de decisión de la estructura organizacional.
- Nivel de autoridad: Las decisiones que la estructura está autorizada a tomar
- Delegación de autoridad: Como los derechos para tomar decisiones son delegadas a otras estructuras que le reportan.
- Procedimientos de escalamiento: Acciones requeridas en caso de problemas en la toma de decisiones.

Aplicación metodología COBIT 5

Para la aplicación de la metodología se plantea la elaboración de una matriz en la cual se realizará un mapeo entre las Metas de TI y los Procesos de COBIT, determinando de esta manera los procesos necesarios que permitan disminuir el riesgo tecnológico en la institución desde cada dimensión del cuadro de mando integral.

Los Dominios que abarcan COBIT 5 son los siguientes:

- Evaluar, Orientar y Supervisar
- Alinear, Planificar y Organizar
- Construcción, Adquisición e implementación
- Entregar, dar servicio y soporte
- Supervisión, Evaluación y Verificación

Como procesos de TI, dentro de los Dominios de COBIT 5 se detallan los siguientes: Evaluar, Orientar y Supervisar:

- EDM01; Asegurar el establecimiento y mantenimiento del marco de gobierno
- EDM02; Asegurar la Entrega de Beneficios
- EDM03; Asegurar la Optimización del Riesgo
- EDM04; Asegurar la Optimización de los Recursos
- EDM05; Asegurar la Transparencia hacia las partes interesadas

Alinear, Planificar y Organizar:

- APO01; Gestionar el Marco de Gestión de TI
- APO02; Gestionar la estrategia
- APO03; Gestionar la arquitectura empresarial
- APO04; Gestionar la innovación
- APO05; Gestionar el portafolio
- APO06; Gestionar el presupuesto y los costes
- APO07; Gestionar los recursos humanos
- APO08; Gestionar las relaciones
- APO09; Gestionar los acuerdos de servicio;
- APO10; Gestionar los proveedores
- APO11; Gestionar la calidad
- APO12; Gestionar el riesgo
- APO13; Gestionar la seguridad

Construcción, Adquisición e implementación:

- BAI01; Gestionar los programas y proyectos
- BAI02; Gestionar la definición de requisitos
- BAI03; Gestionar la identificación y la construcción de soluciones
- BAI04; Gestionar la disponibilidad y la capacidad
- BAI05; Gestionar la introducción de cambios organizativos
- BAI06; Gestionar los cambios
- BAI07; Gestionar la aceptación del cambio y de la transición
- BAI08; Gestionar el conocimiento
- BAI09; Gestionar los activos
- BAI10; Gestionar la configuración

Entregar, dar servicio y soporte:

- DSS01; Gestionar las operaciones
- DSS02; Gestionar las peticiones y los incidentes del servicio
- DSS03; Gestionar los problemas

- DSS04; Gestionar la continuidad
- DSS05; Gestionar los servicios de seguridad
- DSS06; Gestionar los controles de los procesos del negocio

Supervisión, Evaluación y Verificación:

- MEA01; Supervisar, Evaluar y Valorar rendimiento y conformidad
- MEA02; Supervisar, Evaluar y Valorar el sistema de control interno
- MEA03; Supervisar, Evaluar y Valorar la conformidad con los requerimientos externos.

Tabla 31. Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y los Procesos de TI

DOMINIO	PROCESOS DE TI		OBJETIVOS DE TI																
			FINANCIERA						CLIENTE		INTERNA							APRENDIZAJE Y CRECIMIENTO	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
			Alineación entre TI y la estrategia de la institución	Cumplimiento y soporte de TI para el cumplimiento con leyes y regulaciones externas.	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Administración de los riesgos de la institución relacionados con TI	Realización de beneficios del portafolio de inversiones y servicios habilitados por TI.	Transparencia de costos, beneficios y riesgos de TI	Entrega de servicios de TI en línea con los requerimientos del negocio	Adecuado uso de aplicaciones, información y soluciones de tecnología	Agilidad de TI	Seguridad de información, infraestructura de procesamiento y aplicaciones	Optimización, de activos, recursos y capacidades de TI	Capacitación y soporte de procesos de la institución integrando aplicaciones y tecnología en procesos de la institución	Entrega de programas que proporcionen beneficios a tiempo, presupuesto y calidad	Disponibilidad de información confiable y útil para la toma de decisiones	Cumplimiento de TI con políticas internas	Personal de la institución y de TI competente y motivado	Conocimiento, pericia e iniciativas para la innovación de la institución.
Evaluar, Orientar y Supervisar	EDM01	Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno.																	
	EDM02	Asegurar la entrega de beneficios																	
	EDM03	Asegurar la optimización del riesgo																	
	EDM04	Asegurar la optimización de recursos																	
	EDM05	Asegurar la transparencia de los interesados																	

Alinear, Planificar y Organizar	APO01	Gestionar el marco de gestión de TI																	
	APO02	Gestionar la estrategia																	
	APO03	Gestionar la arquitectura empresarial																	
	APO04	Gestionar la innovación																	
	APO05	Gestionar el portafolio																	
	APO06	Gestionar el presupuesto y los costos																	
	APO07	Gestionar los recursos humanos																	
	APO08	Gestionar las relaciones																	
	APO09	Gestionar los acuerdos de servicio																	
	APO10	Gestionar los proveedores																	
	APO11	Gestionar la calidad																	
	APO12	Gestionar los riesgos																	
	APO13	Gestionar la seguridad																	
Construcción, Adquisición e Implementación	BAI01	Gestionar programas y proyectos																	
	BAI02	Gestionar la definición de requerimientos																	
	BAI03	Gestionar la identificación y construcción de soluciones																	
	BAI04	Gestionar la disponibilidad y capacidad																	
	BAI05	Gestionar la habilidad del cambio organizacional																	
	BAI06	Gestionar los cambios																	
	BAI07	Gestionar la aceptación y transición del cambio																	
	BAI08	Gestionar el conocimiento																	
	BAI09	Gestionar los activos																	
	BAI10	Gestionar la configuración																	
Entregar, dar Servicio y Soporte	DSS01	Gestionar las operaciones																	
	DSS02	Gestionar las solicitudes de servicio e incidentes																	
	DSS03	Gestionar los problemas																	
	DSS04	Gestionar la continuidad																	
	DSS05	Gestionar los servicios de seguridad																	

	DSS06	Gestionar los controles de procesos de la institución																	
Supervisión, Evaluación y Verificación	MEA01	Monitorear, evaluar y valorar el desempeño y conformidad																	
	MEA02	Monitorear, evaluar y valorar el sistema de control interno																	
	MEA03	Monitorear, evaluar y valorar el cumplimiento con requerimientos externos																	

Elaborado por: El autor

Alcance de los dominios de la Metodología COBIT 5:

Tabla 32. Alcance dominios COBIT 5

Dominios	Alinear, Planear y Organizar (APO)	Dominio de Gestión que cubre las estrategias y las tácticas de la institución. Identifica la manera en que TI puede contribuir mejor con los objetivos del negocio. Este dominio proporciona la dirección para la entrega de soluciones y la entrega de servicios.
	Evaluar, Orientar y Supervisar (EDM)	Asegurarse de que se logren los objetivos de la empresa evaluando las necesidades de las partes interesadas
	Construir, Adquirir e Implementar (BAI)	Iniciar, planificar, controlar y ejecutar programas y proyectos.
	Entregar, Dar Servicio y Soporte (DSS)	Lograr que los servicios de TI se entreguen de acuerdo con las prioridades del negocio y con optimización de costos, implantar de forma correcta la confidencialidad, la integridad y la disponibilidad de la información.
	Supervisar, Evaluar y Verificar (MEA)	Evaluar regularmente los procesos de TI, monitoreando la calidad y cumplimiento de los requerimientos de control.

Fuente: COBIT 5

Elaborado por: El autor

Alcance de los procesos

Tabla 33. Alcance procesos COBIT 5

DOMINIO	PROCESOS DE TI		ALCANCE DE LOS PROCESOS
Alinear, Planear y Organizar (APO)	APO01	Gestionar el Marco de Gestión de TI	Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores. Proporciona un enfoque de gestión consistente que permita cumplir los requisitos de gobierno corporativo e incluya procesos de gestión, estructuras, roles y responsabilidades organizativos, actividades fiables y reproducibles y habilidades y competencias.
	APO02	Gestionar la estrategia	Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos. Tiene como propósito alinear los planes estratégicos de TI con los objetivos del negocio. Comunicar claramente los objetivos y las cuentas asociadas para que sean comprendidos por todos, con la identificación de las opciones estratégicas de TI, estructurados e integrados con los planes de negocio.
	APO03	Gestionar la arquitectura empresarial	Establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo. Define los requisitos para la taxonomía, las normas, las directrices, los procedimientos, as plantillas y las herramientas y proporcionar un vínculo para estos componentes.

	APO04	Gestionar la Innovación	Analizar cuáles son las oportunidades para la innovación empresarial o qué mejora puede crearse con las nuevas tecnologías, servicios o innovaciones empresariales facilitadas por TI, así como a través de las tecnologías ya existentes y por la innovación en procesos empresariales y de TI. Influir en la planificación estratégica y en las decisiones de la arquitectura de empresa. Tiene como propósito lograr ventaja competitiva, innovación empresarial y eficacia y eficiencia operativa mejorada mediante la explotación de los desarrollos tecnológicos para la explotación de la información.
	APO05	Gestionar el portafolio	Ejecutar el conjunto de direcciones estratégicas para la inversión alineada con la visión de la arquitectura empresarial, las características deseadas de inversión, los portafolios de servicios relacionados, considerar las diferentes categorías de inversión y recursos y las restricciones de financiación. Evaluar, priorizar y equilibrar programas y servicios, gestionar la demanda con los recursos y restricciones de fondos, basados en su alineamiento con los objetivos estratégicos, así como en su valor y riesgo corporativo. Supervisar el rendimiento global del portafolio de servicios y programas, proponiendo ajustes si fuesen necesarios en respuesta al rendimiento de programas y servicios o al cambio en las prioridades corporativas. Optimizar el rendimiento del portafolio global de programas en respuesta al rendimiento de programas y servicios y a las cambiantes prioridades y demandas corporativas.
	APO06	Gestionar el presupuesto y los costes	Gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de TI, abarcando presupuesto, coste y gestión del beneficio, y la priorización del gasto mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costes a la empresa. Fomentar la colaboración entre TI y las partes interesadas de la empresa para catalizar el uso eficaz y eficiente de los recursos relacionados con las TI y brindar transparencia y responsabilidad sobre el coste y valor de negocio de soluciones y servicios. Permitir a la empresa tomar decisiones informadas con respecto a la utilización de soluciones y servicios de TI.

APO07	Gestionar los recursos humanos	Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada. Optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa.
APO08	Gestionar las relaciones	Gestionar las relaciones entre el negocio y TI de modo formal y transparente, enfocándolas hacia el objetivo común de obtener resultados empresariales exitosos apoyando los objetivos estratégicos y dentro de las restricciones del presupuesto y los riesgos tolerables. Basar la relación en la confianza mutua, usando términos entendibles, lenguaje común y voluntad de asumir la propiedad y responsabilidad en las decisiones claves. Crear mejores resultados, mayor confianza en la tecnología y conseguir un uso efectivo de los recursos.
APO09	Gestionar los acuerdos de servicio	Alinear los servicios basados en TI y los niveles de servicio con las necesidades y expectativas de la empresa, incluyendo identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios TI, niveles de servicio e indicadores de rendimiento. Asegurar que los servicios TI y los niveles de servicio cubren las necesidades presentes y futuras de la empresa.
APO10	Gestionar los proveedores	Administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados. Minimizar el riesgo de proveedores que no rindan y asegurar precios competitivos.

	APO11	Gestionar la Calidad	Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia. Asegurar la entrega consistente de soluciones y servicios que cumplan con los requisitos de la organización y que satisfagan las necesidades de las partes interesadas.
	APO12	Gestionar el riesgo	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa. Integrar la gestión de riesgos empresariales relacionados
	APO13	Gestionar la seguridad	Definir, operar y supervisar un sistema para la gestión de la seguridad de la información. Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.
Evaluar, Orientar y Supervisar (EDM)	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	Analizar y articular los requerimientos para el gobierno de las TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadoras, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa.
	EDM02	Asegurar la entrega de beneficios	Optimizar la contribución al valor del negocio desde los procesos de negocios, los de servicios TI y activos de las TI resultado de la inversión hecha por TI a unos costos aceptables.
	EDM03	Asegurar la optimización del riesgo	Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.
	EDM04	Asegurar la optimización de recursos	Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo.

	EDM05	Asegurar la transparencia hacia las partes interesadas	Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de las TI de la empresa son transparentes, con aprobación por las partes interesadas de las metas, las métricas y las acciones correctivas necesarias.
Construir, Adquirir e Implementar (BAI)	BAI01	Gestión de programas y proyectos	Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación. Alcanzar los beneficios de negocio y reducir el riesgo de retrasos y costes inesperados y el deterioro del valor, mediante la mejora de las comunicaciones y la involucración de usuarios finales.
	BAI02	Gestionar la definición de requisitos	Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios. Crear soluciones viables y óptimas que cumplan con las necesidades de la organización mientras minimizan el riesgo.
	BAI03	Gestionar la Identificación y Construcción de Soluciones	Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios. Establecer soluciones puntuales y rentables capaces de soportar la estrategia de negocio y objetivos operacionales.
	BAI04	Gestionar la Disponibilidad y Capacidad	Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costes. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio. Mantener la disponibilidad del servicio, la gestión eficiente de recursos y la optimización del rendimiento de los sistemas mediante la predicción del rendimiento futuro y de los requerimientos de capacidad.

BAI05	Gestionar la Facilitación del Cambio Organizativo	Maximizar la probabilidad de la implementación exitosa en toda la empresa del cambio organizativo de forma rápida y con riesgo reducido, cubriendo el ciclo de vida completo del cambio y todas las partes interesadas del negocio y de TI. Preparar y comprometer a las partes interesadas para el cambio en el negocio y reducir el riesgo de fracaso.
BAI06	Gestionar los cambios	Gestiona todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación. Posibilitar una entrega de los cambios rápida y fiable para el negocio, a la vez que se mitiga cualquier riesgo que impacte negativamente en la estabilidad e integridad del entorno en que se aplica el cambio.
BAI07	Gestionar la Aceptación del Cambio y la Transición	Aceptar formalmente y hacer operativas las nuevas soluciones, incluyendo la planificación de la implementación, la conversión de los datos y los sistemas, las pruebas de aceptación, la comunicación, la preparación del lanzamiento, el paso a producción de procesos de negocio o servicios TI nuevos o modificados, el soporte temprano en producción y una revisión post-implementación. Implementar soluciones de forma segura y en línea con las expectativas y resultados acordados.
BAI08	Gestionar el Conocimiento	Mantener la disponibilidad de conocimiento relevante, actual, validado y fiable para dar soporte a todas las actividades de los procesos y facilitar la toma de decisiones. Planificar la identificación, recopilación, organización, mantenimiento, uso y retirada de conocimiento. Proporcionar el conocimiento necesario para dar soporte a todo el personal en sus actividades laborales, para la toma de decisiones.

	BAI09	Gestionar los activos	Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento, que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para el negocio y que el software instalado cumple con los acuerdos de licencia. Contabilización de todos los activos de TI y optimización del valor proporcionado por estos activos.
	BAI10	Gestionar la configuración	Definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarios para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración. Proporcionar suficiente información sobre los activos del servicio para que el servicio pueda gestionarse con eficacia, evaluar el impacto de los cambios y hacer frente a los incidentes del servicio.
Entregar, Dar Servicio y Soporte	DSS01	Gestionar operaciones	Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas. Entregar los resultados del servicio operativo de TI, según lo planificado.
	DSS02	Gestionar Peticiones e Incidentes de Servicio	Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes. Lograr una mayor productividad y minimizar las interrupciones mediante la rápida resolución de consultas de usuario e incidentes.

	DSS03	Gestionar problemas	Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora. Incrementar la disponibilidad, mejorar los niveles de servicio, reducir costes, y mejorar la comodidad y satisfacción del cliente reduciendo el número de problemas operativos.
	DSS04	Gestionar la continuidad	Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa. Continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa.
	DSS05	Gestionar servicios de seguridad	Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad. Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.
	DSS06	Gestionar controles de proceso de negocio	Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisface todos los requerimientos relevantes para el control de la información. Mantener la integridad de la información y la seguridad de los activos de información manejados en los procesos de negocio dentro de la empresa o externalizados.
Supervisar, Evaluar y Valorar	MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad	Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada. Proporcionar transparencia de rendimiento y conformidad y conducción hacia la obtención de los objetivos.

	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno	Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento. Ofrecer transparencia a las partes interesadas claves respecto de la adecuación del sistema de control interno para generar confianza en las operaciones, en el logro de los objetivos de la compañía y un entendimiento adecuado del riesgo residual.
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general. Asegurar que la empresa cumple con todos los requisitos externos que le sean aplicables.

Fuente: COBIT 5

Elaborado por: El autor

Aplicación:

Realizando el mapeo entre los objetivos de TI y los procesos de TI, utilizando la metodología COBIT 5, se logra identificar los principales procedimientos que permitan definir los controles aplicables a la institución dentro de sus políticas.

Tabla 34. Aplicación de la matriz COBIT 5 en la institución

DOMINIO	PROCESOS DE TI		OBJETIVOS DE TI																	
			FINANCIERA						CLIENTE		INTERNA							APRENDIZAJE Y CRECIMIENTO		
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
			Alineación entre TI y la estrategia de la institución	Cumplimiento y soporte de TI para el cumplimiento con leyes y regulaciones externas.	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Administración de los riesgos de la institución relacionados con TI	Realización de beneficios del portafolio de inversiones y servicios habilitados por TI.	Transparencia de costos, beneficios y riesgos de TI	Entrega de servicios de TI en línea con los requerimientos de la institución	Adecuado uso de aplicaciones, información y soluciones de tecnología	Agilidad de TI	Seguridad de información, infraestructura de procesamiento y aplicaciones	Optimización, de activos, recursos y capacidades de TI	Capacitación y soporte de procesos de la institución integrando aplicaciones y tecnología en procesos de la institución	Entrega de programas que proporcionen beneficios a tiempo, presupuesto y calidad	Disponibilidad de información confiable y útil para la toma de decisiones	Cumplimiento de TI con políticas internas	Personal de la institución y de TI competente y motivado	Conocimiento, pericia e iniciativas para la innovación de la institución.	VALORACIÓN TOTAL
OBJETIVOS A CONSIDERAR			x	x	x	x		x	x	x		x		x		x				
Evaluar, Orientar y Supervisar	EDM01	Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno.	2	1	2	1		1	2			1		1		1				12
	EDM02	Asegurar la entrega de beneficios	2		1			2	2	1						1				9
	EDM03	Asegurar la optimización del riesgo	1	1	1	2		2	1	1		2		2		1				14

	EDM04	Asegurar la optimización de recursos	1	2	1	1		1	1	1		2		2		2				14
	EDM05	Asegurar la transparencia de los interesados	1	1	2			2	2							1				9
Alinear, Planificar y Organizar	APO01	Gestionar el marco de gestión de TI	2	2	1	1		2	1	2		1		1		1				14
	APO02	Gestionar la estrategia	2		1	1			2	1				1		1				9
	APO03	Gestionar la arquitectura empresarial	2		1	1		1	1	1		1		1		1				10
	APO04	Gestionar la innovación	1			1				2				1		1				6
	APO05	Gestionar el portafolio	2		1	1		1	1	1										7
	APO06	Gestionar el presupuesto y los costos	1		1	1		2	1	1						1				8
	APO07	Gestionar los recursos humanos	2	1	1	1			1			1				2				9
	APO08	Gestionar las relaciones	2		1	1		1	2	1				2		1				11
	APO09	Gestionar los acuerdos de servicio	1			1		1	2	1		1		1		2				10
	APO10	Gestionar los proveedores		1		2		1	2	1		2		1		1				11
	APO11	Gestionar la calidad	1	1		1			2	1				1		1				8
	APO12	Gestionar los riesgos		2		2		2	1	1		2		2		2				14
	APO13	Gestionar la seguridad		2		2		2	1	1		2		1		2				13
Construcción, Adquisición e Implementación	BAI01	Gestionar programas y proyectos	2	1	1	2		1	1	1		1		2		2				14
	BAI02	Gestionar la definición de requerimientos	2	1	1	1			2	1		1		2		1				12
	BAI03	Gestionar la identificación y construcción de soluciones	1			1			2	1				1		1				7
	BAI04	Gestionar la disponibilidad y capacidad				1			2	1						2				6
	BAI05	Gestionar la habilidad del cambio organizacional	1		1				1	2				1						6
	BAI06	Gestionar los cambios			1	2			2	1		2		1		1				10
	BAI07	Gestionar la aceptación y transición del cambio				1			1	2				2		1				7
	BAI08	Gestionar el conocimiento	1						1	1		1				1				5
	BAI09	Gestionar los activos		1		1		2	1			1				1				7
	BAI10	Gestionar la configuración		2		1		1		1		1				2				8
Entregar, dar Servicio y Soporte	DSS01	Gestionar las operaciones	1	1	1	2		1	2	1		1		2		1				13
	DSS02	Gestionar las solicitudes de servicio e incidentes				2			2	1		1				1				7

	DSS03	Gestionar los problemas		1		2			2	1				1		2				9
	DSS04	Gestionar la continuidad	1	1		2			2	1		1		1		2				11
	DSS05	Gestionar los servicios de seguridad	1	2	2	2		1	1	1		2		1		1				14
	DSS06	Gestionar los controles de procesos de la institución	2	1	1	2		1	2	1		1		1		1				13
Supervisión, Evaluación y Verificación	MEA01	Monitorear, evaluar y valorar el desempeño y conformidad	1	1	1	2		1	2	1		1		2		1				13
	MEA02	Monitorear, evaluar y valorar el sistema de control interno		2		2		1	1	1		1		1		1				10
	MEA03	Monitorear, evaluar y valorar el cumplimiento con requerimientos externos		2		2			1			1		1		1				8

Elaborado por: El autor

Para el mapeo realizado en el presente estudio, se utiliza la siguiente escala:

– A una relación fuerte o importante entre los objetivos de TI y los procesos de COBIT 5 se asignará el valor de 2.

– A una relación secundaria o menos importante entre los objetivos de TI y los procesos de COBIT 5 se asignará el valor de 1.

Estos valores son considerados de acuerdo al Anexo 3, que es la propuesta de ISACA para la aplicación de la metodología COBIT 5.

Para la selección de los procesos principales se considera los aquellos cuya valoración final tienen como resultado 13 y 14.

Principales procedimientos de TI de la Institución Financiera

Realizado el mapeo entre los procesos de TI y los objetivos de TI se seleccionaron: EDM03, EDM04, APO01, APO12, APO13, BAI01, DSS01, DSS05, DSS06, MEA01 como los principales que permitan alcanzar los objetivos necesarios para la disminución de riesgos de TI dentro de la institución.

Tabla 35. Procesos de TI en la institución financiera

EVALUAR ORIENTAR Y SUPERVISAR		
EDM03	Asegurar la optimización del riesgo	14
EDM04	Asegurar la optimización de recursos	14
ALINEAR, PLANIFICAR Y ORGANIZAR		
APO01	Gestionar el marco de gestión de TI	14
APO12	Gestionar los riesgos	14
APO13	Gestionar la seguridad	13
CONSTRUCCIÓN, ADQUISICIÓN E IMPLEMENTACIÓN		
BAI01	Gestionar programas y proyectos	14
ENTREGAR, DAR SERVICIO Y SOPORTE		
DSS01	Gestionar las operaciones	13
DSS05	Gestionar los servicios de seguridad	13
DSS06	Gestionar los controles de procesos de la institución	14
SUPERVISIÓN, EVALUACIÓN Y VERIFICACIÓN		
MEA01	Monitorear, evaluar y valorar el desempeño y conformidad	13

Fuente: COBIT 5
Elaborado por: El autor

Alcance de los procesos de TI seleccionados

Tabla 36. Alcance de procesos seleccionados

EVALUAR ORIENTAR Y SUPERVISAR		
EDM03	Asegurar la optimización del riesgo	Asegurar que la aceptación y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.
EDM04	Asegurar la optimización de recursos	Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo.
ALINEAR, PLANIFICAR Y ORGANIZAR		
APO01	Gestionar el marco de gestión de TI	Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.
APO12	Gestionar los riesgos	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa. Integrar la gestión de riesgos empresariales relacionados
APO13	Gestionar la seguridad	Definir, operar y supervisar un sistema para la gestión de la seguridad de la información. Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.
CONSTRUCCIÓN, ADQUISICIÓN E IMPLEMENTACIÓN		
BAI01	Gestionar programas y proyectos	Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación. Alcanzar los beneficios de negocio y reducir el riesgo de retrasos y costes inesperados y el deterioro del valor, mediante la mejora de las comunicaciones y la involucración de usuarios finales.
ENTREGAR, DAR SERVICIO Y SOPORTE		
DSS01	Gestionar las operaciones	Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas. Entregar los resultados del servicio operativo de TI, según lo planificado.
DSS05	Gestionar los servicios de seguridad	Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad. Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.
DSS06	Gestionar los controles de procesos de la institución	Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisface todos los requerimientos relevantes para el control de la información. Mantener la integridad de la información y la seguridad de los activos de información manejados en los procesos de negocio dentro de la empresa o externalizados.
SUPERVISIÓN, EVALUACIÓN Y VERIFICACIÓN		
MEA01	Monitorear, evaluar y valorar el desempeño y conformidad	Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada. Proporcionar transparencia de rendimiento y conformidad y conducción hacia la obtención de los objetivos.

Fuente: COBIT 5
Elaborado por: El autor

Matriz de evaluación de los procesos seleccionados de COBIT 5

Con cada proceso seleccionado, se define una matriz en la cual se describirán los porcentajes de cumplimiento tanto de la situación actual como los requeridos para lograr el objetivo o meta, las evidencias de cumplimiento y avances realizados, y observaciones que se puedan relacionar respecto a cada proceso.

Tabla 37. Matriz de evaluación de los procesos seleccionados

CODIGO	PROCESO	% ACTUAL	% META	EVIDENCIAS	OBSERVACIONES
EVALUAR ORIENTAR Y SUPERVISAR					
EDM03	Asegurar la optimización del riesgo				
EDM04	Asegurar la optimización de recursos				
ALINEAR, PLANIFICAR Y ORGANIZAR					
APO01	Gestionar el marco de gestión de TI				
APO12	Gestionar los riesgos				
APO13	Gestionar la seguridad				
CONSTRUCCIÓN, ADQUISICIÓN E IMPLEMENTACIÓN					
BAI01	Gestionar programas y proyectos				
ENTREGAR, DAR SERVICIO Y SOPORTE					
DSS01	Gestionar las operaciones				
DSS05	Gestionar los servicios de seguridad				
DSS06	Gestionar los controles de procesos de la institución				
SUPERVISIÓN, EVALUACIÓN Y VERIFICACIÓN					
MEA01	Monitorear, evaluar y valorar el desempeño y conformidad				

Elaborado por: El autor

Matriz de determinación de riesgo

Con los procesos de COBIT seleccionados y con la revisión de la situación actual en la institución, se propone las actividades a realizar para mitigar el riesgo identificado, así como el área o persona responsable de elaborar la tarea dentro de cada proceso.

Tabla 38. Matriz operativa de la propuesta

Dominio	Proceso	Descripción	Situación actual	Actividad	Responsable
EDM03	Asegurar la optimización del riesgo	Pretender la aceptación y la tolerancia al riesgo de la institución para que estos sean entendidos, comunicados y gestionados.	No se tiene una visión clara de riesgo informático por parte de la institución, no se han evaluado todos los riesgos a los que los recursos de TI de la institución están expuestos.	Definir un plan estratégico de TI en el que se identifiquen los posibles riesgos de TI y su tratamiento. Definir un modelo de gobierno de TI	Encargado de la gestión de las TI en la institución
EDM04	Asegurar la optimización de recursos	Asegurar que las capacidades relacionadas con las TI están disponibles para lograr los objetivos a un costo óptimo	No existe una planificación detallada para los recursos de TI. Las aprobaciones de inversión se realizan desde la Alta Gerencia sin que tenga una planificación de dicha inversión.	Definir un plan estratégico de TI. Definir el POA y presupuesto de TI	Encargado de la gestión de las TI en la institución
APO01	Gestionar el marco de gestión de TI	Identificar la misión y la visión corporativa de TI. Implementar y mantener mecanismos para la gestión de la información y el uso de TI para apoyar los objetivos de gobierno	No se tiene un plan estratégico de tecnología alineado con el plan estratégico de la institución. Existe la predisposición de establecer políticas, procedimientos y procesos de cumplimiento, sin embargo no se encuentran totalmente definidos ni documentados	Definir un plan estratégico de TI. Definir un modelo de gobierno de TI Definir políticas y procedimientos de TI	Encargado de la gestión de las TI en la institución
APO12	Gestionar los riesgos	Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la alta gerencia de la institución.	No se tiene una evaluación de riesgos ni los procesos definidos para las decisiones de negocio. La institución no toma en cuenta los impactos en el negocio asociados a las vulnerabilidades de	Definir el modelo de Gobierno de TI Implementar la gestión de riesgos de TI	Encargado de la gestión de las TI en la institución Jefe de Riesgos.

			seguridad. El área de riesgos no ha establecido como relevante la adquisición de soluciones de TI.		
APO13	Gestionar la seguridad	Definir, implementar y supervisar un sistema para la gestión de la seguridad de la información.	Se tiene establecido una política de seguridad de la información, sin embargo la misma se encuentra desactualizada y no se ha comunicado a todo el personal de la institución.	Definir el modelo de Gobierno de TI. Definir políticas y procedimientos de TI. Implementar la gestión de riesgos de TI. Actualizar y sociabilizar las políticas actuales.	Encargado de la gestión de las TI en la institución Jefe de Riesgos.
BAI01	Gestionar programas y proyectos	Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa.	El proceso y la metodología de administración de proyectos de TI no han sido establecidos y comunicados. Los proyectos de TI no se monitorean, con cronogramas y mediciones de presupuesto y desempeño definidos y actualizados. La estrategia general de TI aún no incluye una definición consistente de los riesgos, calidad y aseguramiento.	Difundir el enfoque de administración de proyectos	Encargado de la gestión de las TI en la institución
DSS01	Gestionar las operaciones	Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externos, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.	Las operaciones de soporte de TI son informales e intuitivas y no son documentadas.	Definir y Aplicar SLA's y OLA's. Definir políticas y procedimientos de TI. Implementar la gestión de riesgos de TI. Implementar la gestión de continuidad del negocio	Encargado de la gestión de las TI en la institución Jefe de Riesgos.
DSS05	Gestionar los servicios de seguridad	Proteger la información de la institución para mantener aceptable el nivel de riesgo	Los servicios de terceros pueden no cumplir con los requerimientos específicos de	Definir el modelo de Gobierno de TI.	Encargado de la gestión de las TI en la institución

		de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.	seguridad de la empresa. Existe una política de TI definida donde existen aspectos limitados de seguridad de información. La seguridad de TI es vista primordialmente como responsabilidad y disciplina de TI, y el negocio no ve la seguridad de TI como parte de su propia disciplina.	Definir políticas y procedimientos de TI. Implementar la gestión de riesgos de TI.	Jefe de Riesgos.
DSS06	Gestionar los controles de procesos de la institución	Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisface todos los requerimientos relevantes para el control de la información. Identificar los requisitos de control de la información y gestionar y operar los controles adecuados para asegurar que la información y su procesamiento satisfacen estos requerimientos.	No se tienen definidos y levantados procesos tecnológicos para la determinación de controles de la información. Estos procesos deben estar mapeados con los procesos de negocio de la institución.	Definir el plan estratégico de TI. Definir políticas y procedimientos de TI 7. Implementar la gestión de riesgos de TI.	Encargado de la gestión de las TI en la institución Jefe de Riesgos.
MEA01	Monitorear, evaluar y valorar el desempeño y conformidad	Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.	El Jefe de TI reconoce una necesidad de recolectar y evaluar información sobre los procesos de monitoreo, sin embargo, no se han realizado procesos de auditoría y control. El monitoreo por lo general se realiza de forma consecuente en algún incidente que ha ocasionado pérdida o irregularidades dentro de la institución.	Definir y Aplicar SLA's y OLA's. Definir políticas y procedimientos de TI. Planificar procesos de auditoría interna/externa.	Encargado de la gestión de las TI en la institución Gerencia. Auditoría

Elaborado por: El autor

Análisis de lo Actual vs lo Propuesto

No	ITEM	ACTUAL				PROPUESTO			
		Siempre	Casi Siempre	A Veces	Nunca	Siempre	Casi Siempre	A Veces	Nunca
3	Las herramientas informáticas que utiliza en la institución, ya sean estas para el manejo de la información financiera y contable, información administrativa, u otra información sirven de apoyo para la toma de decisiones.			X			x		
4	La institución cuenta con un diseño de procesos que recoja las necesidades de las partes interesadas tanto internas como externas			x			x		
5	La información que se obtiene de los clientes o socios de la institución financiera es la necesaria para un real conocimiento de los socios			x			x		
6	El personal de la institución conoce y aplica las políticas elaboradas por TI			x			x		
7	La administración realiza un tratamiento adecuado para mitigar los riesgos informáticos en la institución			x			x		
8	La institución cuenta actualmente con reportes de riesgo de TI		x			x			
9	Se aplican medidas de control de riesgo dentro de la institución			x			x		

10	Las instituciones financieras disponen del contingente tecnológico necesario, para su normal desenvolvimiento de sus funciones en cada departamento de la misma		x			x			
11	Cree usted que la aplicación de una metodología de buenas prácticas para el control de la información, reducirá el nivel de riesgo informático en las instituciones financieras		x			x			

No.	ITEM	CATEGORIAS		CATEGORIAS	
		SI	NO	SI	NO
1	La Cooperativa cuenta con un manual de funciones para el personal de la misma	x		x	
2	La información de los procedimientos para el desarrollo de sus funciones es entendible y de su conocimiento	X		X	
12	Existe en la institución la planificación, diseño, desarrollo, despliegue, operación, gestión y aplicación de las TI		X	X	
13	Existe dentro de la institución un Modelo que esté basado en tareas corporativas de TI		X	X	
14	Se encuentra el departamento de TI en el organigrama general de la cooperativa		X	X	
15	La institución tiene un presupuesto destinado al desarrollo y control de TI		x	X	

Riesgo Actual

NIVEL DE RIESGO	
ALTO	27,00%
MODERADO	60,00%
ACEPTABLE	13,00%

Riesgo posterior a la aplicación de las recomendaciones

NIVEL DE RIESGO	
ALTO	0,00%
MODERADO	40,00%
ACEPTABLE	60,00%

Conclusiones:

- Al plantear la propuesta, el personal administrativo de la Cooperativa Indígena SAC no consideraba el riesgo informático como parte fundamental en la gestión de riesgos debido a que analizaban únicamente indicadores y reportes financieros. No se consideraban los riesgos y pérdidas que puede ocasionar la no adecuada gestión de los recursos de TI. Al determinar los principales procesos utilizando la metodología COBIT 5 para el tratamiento de dichos riesgos se pudo proponer distintos planes de acción o actividades que, al ser comunicados, entendidos, ejecutados y monitoreados por cada persona dentro de la institución, se obtendría como resultado la disminución del impacto que pudieran provocar si no se llegase a tratar el riesgo analizado.

- La aplicación de la propuesta basada en la metodología COBIT 5 permitió determinar los principales procesos de TI para el tratamiento de los riesgos informáticos en la institución, los cuales son: Asegurar la optimización de riesgo (EDM03), asegurar la optimización de recursos (EDM04), gestionar el marco de gestión de TI (APO01), gestionar los riesgos (APO12), gestionar la seguridad (APO13), gestionar programas y proyectos (BAI01), gestionar las operaciones (DSS01), Gestionar los servicios de seguridad (DSS05), gestionar los controles y procesos de la institución (DSS06), y; monitorear, evaluar y valorar el desempeño y conformidad (MEA01).

- Se determina de forma teórica y práctica que la aplicación de la metodología COBIT 5 permitió, en primera instancia establecer los riesgos informáticos presentes, y posteriormente crear alternativas de solución para minimizar el impacto de dichos riesgos.

- Al basarse la propuesta en una metodología aceptada internacionalmente y que abarca varios estándares normativos, permitirá a la institución brindar mayor confianza a sus clientes manejando de una forma ordenada y responsable los principios de seguridad de la información: confidencialidad, integridad y disponibilidad.

Recomendaciones:

- Al personal de Riesgos conjuntamente con el personal de Sistemas, aplicar las matrices propuestas en lapsos periódicos de tiempo, es decir por lo menos una vez al año para obtener como resultado una oportuna identificación y mitigación de los riesgos informáticos.

- A Gerencia, disponer la incorporación de la aplicación de la metodología COBIT 5 como buena práctica dentro de los procedimientos de la institución enfocándose no solo en la mitigación de riesgos sino también en lograr que el área de TI se alinee a las estrategias y objetivos institucionales.

- A la parte directiva, realizar un control interno que garantice el cumplimiento de todo el personal de la institución de las políticas y procedimientos de TI que permitan la correcta gestión tecnológica y adecuado tratamiento de los riesgos.

- Al personal de Sistemas conjuntamente con Auditoría Interna, elaborar y actualizar constantemente los distintos planes de acción propuestos como actividades para el cumplimiento de cada uno de los procesos definidos.

Bibliografía

Ing. Jhonny Bernao Atiencia Larrea (2013), *El Riesgo Operativo Y Su Impacto En El Control Interno Del Banco Nacional De Fomento Sucursal Ambato*. Universidad Técnica de Ambato, Ambato - Ecuador.

Junta de Regulación Monetaria Financiera. (2016) Resolución No. 128-2015-F.

Super Intendencia de Bancos y Seguros, *Libro I.- Normas Generales para la Aplicación de la ley General de Instituciones del Sistema Financiero, Titulo X.- de la Gestión y Administración de Riesgos.*

Ing. Diana Priscila Ortega Romero (2015), *El Riesgo Operativo Y Su Impacto En El Estado De Resultados De Las Cooperativas De Ahorro Y Crédito - Segmento Uno (Con Casa Matriz En La Provincia De Tungurahua.* Ambato (Ecuador).

COBIT 5. An ISACA Framework- *Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*

Guías para la gestión de la seguridad de TI /TEC TR 13335-1, 1996

Jimmy Arturo Brito Domínguez (2009), *Creación de un Marco de Control para la Administración del Riesgo Operativo relacionado con la Tecnología de Información como modelo para las Cooperativas de Ahorro y Crédito del Ecuador*. Escuela Superior Politécnica del Litoral, Guayaquil - Ecuador.

Diego Fernando Cevallos Guerra (2015), *La Mejores prácticas aplicadas a un Análisis de Riesgos de seguridad de la información para las Entidades Financieras Controladas por La Superintendencia de Economía Popular y Solidaria (Cooperativas de Ahorro y Crédito) que conforman el grupo de Asistencia Tecnológica Cooperativa (Asistecooper)*. Escuela Superior Politécnica del Ejército, Sangolquí - Ecuador.

Rivas, G. A. (1889). *Auditoría informática.* Madrid : Diaz de Santos .

Isaca. (03 de Febrero de 2013). *Administración de empresa de tecnologías de la información.* Obtenido de http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/ISAudit-and-Assurance/Documents/2202_gui_Spa_0415.pdf

Gaitán, R. E., & Niebel, B. W. (2015). *Administración de riesgos E.R.M. y la auditoría interna.* Colombia : ECOE.

Corporación Nacional de Finanzas Populares y Solidarias. (2011). *Ley orgánica de economía popular y solidaria del sistema finaciero.* Ecuador: Corporación Nacional de Finanzas Populares y Solidarias.

Junta de Regulación Monetaria Financiera. (2017). *La Junta de política y regulación monetaria y financiera.* Ecuador: Junta de Regulación Monetaria Financiera.

Karina García Reyes , Erica Prado Vite, Rosa Salazar Cantuñí, & Jacinto Mendoza Rodríguez. (2018). Cooperativas de Ahorro y Crédito del Ecuador y su incidencia en la conformación del Capital Social (2012-2016). *Espacios* , 5.

Superintendencia de Economía Popular y Solidaria. (13 de Febrero de 2015). *Nueva Segmentación Sector Financiero Popular y Solidario.* Obtenido de http://www.seps.gob.ec/noticia?nueva-segmentacion-sector-financiero-popular-y-solidario

Medina, D. T. (2017). *Introducción a la ingeniería de software, planeación y gestión de proyectos informaticos. .* Mexico : Copyright.

Larrea, J. B. (2013). *El riesgo operativo y su impacto en el control interno del Banco Nacional de Fomento Sucursal Ambato.* Ambato: Universidad Tecnica de Ambato .

Domínguez, J. A. (2009). *Creación de un marco de control para la administración del riesgo operativo relacionado con la tecnología de información con modelo para las cooperativas de ahorro y crédito del Ecuador.* Guayaquil: Escuela Superior Politécnica del Litoral.

Guerra, D. F. (2015). *Las mejores prácticas aplicadas a un análisis de riesgos de seguridad de la información para las entidades financieras controladas por la*

Superintendencia de Economía Popular y Solidaria (Cooperativas de Ahorro y Crédito). Sangolqui : Universidad de las Fuerzas Armadas ESPE.

Aguilar, N. M. (2011). El paradigma crítico y los aportes de la investigación acción participativa en la transformacion de la realidad social: Un analisis desde las ciencias sociales. . *Cuestiones Pedagógicas* , 344.

Asamblea Constituyente . (2008). *Constitución de l República del Ecuador* . Ecuador: Asamblea Constituyente .

República del Ecuador Superintendencia de Bancos . (2005). *Normas generales para la aplicacion de la ley general de instituciones del sistema financiero.* Ecuador: República del Ecuador Superintendencia de Bancos .

Tarazona, C. H. (2007). Amenazas informaticas y seguridad de la información. *Derecho Penal y Criminología* , 137.

Yesid A. Olave C. , & Luis C. Gómez F. (2006). Administración de tecnología de información: Oportunidad profesional y desatención curricular. *Scientia et Technica* , 379.

Utel . (02 de Agosto de 2013). *Ingeniería industrial y administración en línea*. Obtenido de https://www.utel.edu.mx/blog/menu-profesional/administracion-de-tecnologias-de-la-informacion-en-linea/

Hernádez, S. R., Fernandez, C. C., & Baptista, P. L. (2010). *Metodologia de la Investigacion* . Mexico: Mc Graw Hill - Quinta Edicion.

Tamayo, M. T. (2004). *El Proceso de la investigacion cientifica: Incluye evaluacion y administracion de proyectos de investogacion.* Mexico: Limusa .

Iglesias, E. P. (1998). *Tecnologías de la información en el control de gestión.* Madrid: Diaz de Santos .

Daniel Pérez, & Matthias Dressler. (2007). Tecnologías de la información para la gestión del conocimiento. *Intangible Capital* , 37-38.

Naciones Unidas . (2003). *Manual de Organización Estadística: El Funcionamiento y la organización de una oficina de estadisticas.* . Nueva York : Naciones Unidas .

Piattini, M. G., & Peso, E. d. (2001). *Auditoría Infórmatica: Un enfoque práctico 2da edición apliada y revisada.* Madrid: Alfaomega.

Valdés, J. T. (1988). *Contratos, riesgos y seguros informáticos.* México: Universidad Nacional Autónoma de México.

Carpentier, J. F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas.* . Barcelona : eni .

Fábrega, J. C., Helena Montiel , Eulalia Planas , & Juan Vílchez . (2009). *Análisis del riesgo en instalaciones industriales.* Barcelona : UPC.

Castro, A. R., & Bayona, Z. O. (2011). Gestión de Riesgos tecnológicos basadaen ISO 31000e ISO 27005y su aporte a lacontinuidad de negocios. *Ingeniería* , 57.

Superintendencia de Economía Popular y Solidaria . (2018). *Una mirada al desarrollo de la economía popular y solidaria.* Quito: Superintendencia de Economía Popular y Solidaria .

Villacres, W. H., & Chacha, J. P. (2015). *El riesgo de crédito y la morosidad de la Cooperativa de Ahorro y Crédito Coorambato Cía. Ltda. del cantón Ambato.* Ambato : Universidad Técnica de Ambato .

Criollo, J. A. (2016). *El riesgo operativo y la liquidez en el área de créditos de la Cooperativa de Ahorro y Crédito Indígena SAC Ltda., de la ciudad de Ambato.* Ambato: Universidad Técnica de Ambato .

Cesar Augusto Salazar Mejía, & Dolores del Carmen Esparza Jaya. (2016). *El riesgo operativo y la rentabilidad en la Cooperativa de Ahorro y Crédito Cámara de Comercio de Ambato Ltda.* Ambato: Universidad Técnica de Ambato.

Villavicencio, A. (2007). *Relación entre la ausencia de tratamiento térmico de la leche con la contaminación microbiológica del queso fresco en el cantón pillaro.* . Ambato: Universidad Técnica de Ambato .

Nogales, Á. F. (2004). *Investigación y técnicas de mercado.* . Madrid: Esic .

Martínez, F. V. (2008). *Riesgos financieros y economicos.* Mexico : Cengace Learning

José Antonio Núñez Mora, & José Juan Chávez Gudiño. (2010). Riesgo operativo: esquema de gestión y modelado del riesgo. *Análisis Económico* , 125.

ISOtools . (16 de Noviembre de 2015). *¿Qué se entiende por riesgo operativo en una organización?* Obtenido de https://www.isotools.org/2015/11/16/que-se-entiende-por-riesgo-operativo-en-una-organizacion/

Calle, J. P. (30 de Marzo de 2019). *4 FACTORES DE RIESGO OPERACIONAL*. Obtenido de https://www.riesgoscero.com/blog/4-factores-de-riesgo-operacional

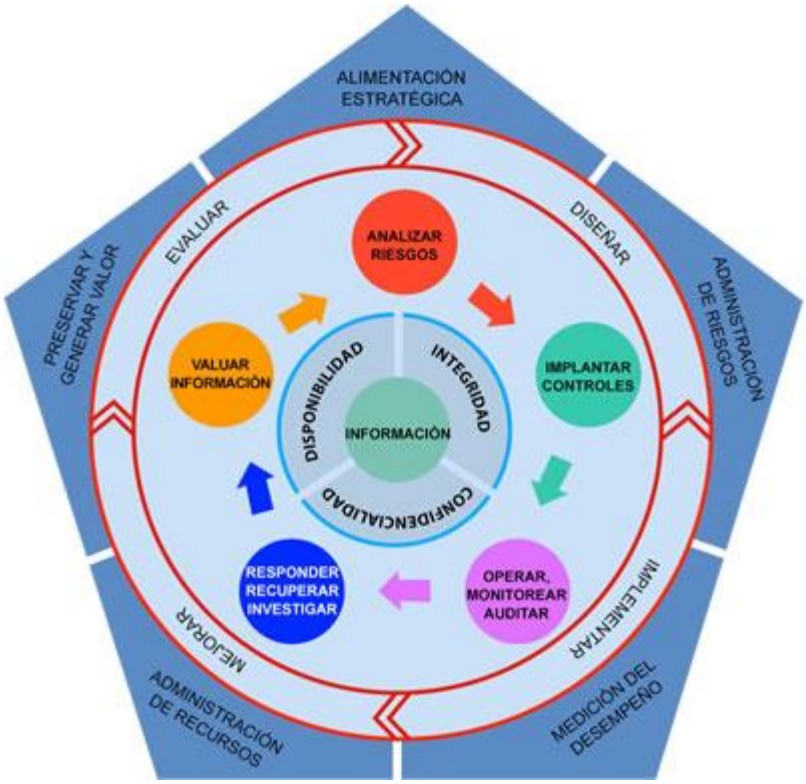
Haro, A. d. (2005). *Medición y control de riesgos financieros.* España : Limusa .

Alonso, P. L. (2014). *Gestión de las Empresas por Procesos.* Barcelona: ETSEIB.

ANEXOS

Anexo 1:

MANUAL DE BUENAS PRACTICAS DE TI



Elaborado por: ING. CHRISTIAN BARRERO	**Fecha de elaboración:**
Revisado por:	

APROBACIÓN POR CONSEJO DE ADMINISTRACIÓN	
Presidente.	Secretario.
Fecha de Aprobación:	Acta No.

CONCEPTOS:

¿Qué es un SGSI?

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye la norma ISO 27001.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso es el que constituye un SGSI, que podría considerarse, como el sistema de calidad para la seguridad de la información.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. En estos términos se basa todo lo referente a la seguridad de la información:

• Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
• Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
• Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran. Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial.

¿Para qué sirve un SGSI?

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

DEFINICIÓN DEL PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN:

Con las premisas anteriores se define el presente Plan de Gestión de Seguridad de la Información de la Cooperativa de Ahorro y Crédito "SAC LTDA.".
Se consideran los distintos tipos de seguridad: Física, Lógica Activa y Pasiva:

- Seguridad Física: Es aquella que trata de proteger todo el hardware de la institución, como servidores, cableado, routers, etc.
- Seguridad Lógica: Protege el software, es decir los sistemas informáticos y los datos de información.
- Seguridad Activa: Es el conjunto de medidas que previenen e intentan evitar daños a los sistemas informáticos.
- Seguridad Pasiva: Complementa a la seguridad pasiva para minimizar daños.

Es necesario recordar e informar al personal, la política en relación a la utilización de equipos y a la realización de copias o al uso ilegal de programas informáticos. La duplicación no autorizada o el uso sin licencia de cualquier programa informático son ilegales y puede exponer al personal y a la cooperativa a asumir una responsabilidad civil y penal en virtud de la ley de derechos de autor.

TÉRMINOS Y DEFINICIONES

Los términos y definiciones indicados, son basados en las principales definiciones dadas por la norma ISO 27001, las normativas de los distintos organismos de control para las instituciones financieras y el modelo de buenas prácticas desarrollado por ISACA que es COBIT 5.

Seguridad de la Información: conjunto de mecanismos que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella.

Gestión de la Seguridad de la Información: políticas y procedimientos para administrar sistemáticamente los datos sensibles de una organización, minimizar el riesgo y asegurar la continuidad del negocio mediante la limitación proactiva del impacto ante una brecha de seguridad, incluyendo la gestión del comportamiento del personal, los procesos y la tecnología, de forma comprensiva para convertirse en parte de la cultura organizacional.

Seguridad informática: medidas de protección de la información en los sistemas, medios, redes y equipos tecnológicos y de comunicaciones.

Incidente de seguridad de la información: 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.

Proceso crítico: Es el indispensable para la Seguridad de la Información y las operaciones de la institución, y cuya falta de identificación o aplicación deficiente puede generarle un impacto financiero negativo o poner en riesgo su sostenibilidad en el tiempo.

POLÍTICAS GENERALES

La Cooperativa de Ahorro y Crédito Indígena SAC adoptará como referencia para la Gestión de la Seguridad de la Información la aplicación de buenas prácticas internacionales definidas en la metodología COBIT 5 en concordancia con la normativa emitida por la Superintendencia de Economía Popular y Solidaria y en concordancia con la norma ISO 27001:2013

Toda información generada, ingresada, procesada, transmitida u obtenida por cualquier medio en los equipos de la Cooperativa, es de propiedad de la Cooperativa de Ahorro y Crédito Indígena SAC, por lo que todo usuario de la misma deberá suscribir un Acuerdo de Confidencialidad previo a su acceso.
El área de Tecnología determinará e implementará las medidas de seguridad informática requeridas, y realizará el monitoreo permanente de su correcto funcionamiento, de ser el caso se realizará una revisión con el responsable del área de Riesgos.

La Jefatura de Riesgos deberá monitorear periódicamente el cumplimiento de las políticas de seguridad de la información en las personas, procesos y tecnología de

información de la Cooperativa, y coordinará la verificación de la efectividad de las medidas de seguridad informática implementadas.

La presente Política y el Proceso de Gestión de la Seguridad de la Información serán evaluados al menos de forma anual, para verificar su rendimiento, efectividad y alineamiento a los objetivos estratégicos institucionales.

NORMAS PARA EL USO DEL EQUIPO DE CÓMPUTO

- El equipo de cómputo será entregado en buenas condiciones y listo para usar. La persona que lo recibe es la única responsable del mismo.
- Se firmará un acta de Entrega – Recepción al momento de recibir el equipo de cómputo, dicha Acta tendrá adjunto el documento correspondiente a las Normas básicas para el correcto uso de equipos.
- No se puede mover los equipos de cómputo del área asignada para ésta, sin previa autorización de Gerencia General y de los encargados de Activos Fijos de la Cooperativa.
- Las unidades de USB y CDROM de los computadores estarán desactivados, en caso de tener la necesidad de utilizarlos realizar la solicitud al área de Sistemas.
- Los archivos que genere el usuario deberán ser guardados en una carpeta ubicada en un directorio diferente al disco C, el personal de la Unidad de Sistemas está autorizado a borrar la información que se encuentre fuera de esta carpeta, deslindándose de toda responsabilidad acerca del resto de documentos almacenados.
    - Para aplicar está política, el personal de Sistemas realizará los procedimientos necesarios para la creación de la carpeta, de preferencia tendrá el nombre de “Mis Documentos”.
- La información almacenada en el equipo es de responsabilidad del usuario a quién se le ha asignado, por lo que debe hacer uso de la misma según los manuales de ética de la Institución.

NORMAS DEL USO DE LAPTOP O COMPUTADORAS PORTATILES

- El personal que utiliza una laptop de la institución, es el único responsable de los daños, defectos o pérdida del equipo y accesorios.
- Una laptop puede ser sustraída con mayor facilidad desde la oficina, dado su tamaño y peso, por esta razón siempre se debe colocar un candado de seguridad para portátiles.
- El personal que utiliza una laptop de la institución está en la obligación de guardar en un lugar seguro y bajo llave el equipo para precautelar la pérdida o robo del mismo.

- Se prohíbe al personal lleve fuera una laptop de la institución sin autorización por escrito de Gerencia General y la persona encargada de Activos Fijos.
- El usuario propietario será responsable de la información almacenada en la portátil y el buen uso de la misma.
- Se solicita que las portátiles se mantengan con el candado de seguridad sujeto al escritorio.

DE LAS NORMAS Y PROCEDIMIENTOS DE USO DE SOFTWARE

- Está prohibido instalar cualquier programa en los equipos de la Cooperativa sin previa autorización de la Unidad de Sistemas, así sea de distribución libre.
- Todo el software propiedad de la institución deberá ser usado exclusivamente para asuntos relacionados con las actividades de la Cooperativa
- En caso de producirse algún problema con el sistema se deberá comunicar inmediatamente a la Unidad de Sistemas.
- Se prohíbe a los empleados realizar copias no autorizadas de programas informáticos. Así como la carga o descarga desde internet de programas informáticos no autorizados.
- Si se descubre que un empleado ha copiado programas informáticos o información en forma ilegal, este puede ser sancionado, suspendido o despedido de la cooperativa.
- Si el usuario tiene información que requiera ser respaldada, debe comunicarse a Sistemas para establecer el procedimiento a seguir para el custodio de la misma.

DEL ACCESO A LA RED

- Está terminantemente prohibido utilizar la red para asuntos que no sean los relacionados con los de la Cooperativa.
- Está prohibido correr programas que disminuya el rendimiento de la Red. Y si es necesario comuníquelo a la Unidad de Sistemas.
- No se puede manipular, borrar, corregir archivos compartidos a través de la red sin previa autorización del propietario. Los archivos como videos, fotografías y otros documentos ajenos a la institución, serán eliminados.
- No está permitido obtener copias de archivos, códigos, contraseñas o información ajena; ni suplantar a otra persona en una conexión que no le pertenece o enviar información a nombre de otra persona sin consentimiento del titular de la cuenta.
- Respetar la integridad de los sistemas de computación. Esto significa que ningún usuario podrá realizar acciones orientadas a infiltrarse, dañar o atacar la seguridad informática de la Institución, a través de ningún medio.

- No obtener ni suministrar información sin la debida autorización, no dar a conocer códigos de seguridad tales como contraseñas a otras personas, o entorpecer por ningún medio el funcionamiento de los sistemas de información y telecomunicaciones de la Institución.
- La creación de nuevas redes o reconfiguración de las existentes, solo podrá ser realizada por personal autorizado o por la Unidad de Sistemas y con previa autorización de la Gerencia General de la Institución.

DE LAS NORMAS DE FUNCIONAMIENTO

- En caso de que el usuario requiera ausentarse de su puesto de trabajo, es su obligación bloquear su equipo de trabajo mientras se encuentre ausente. su ausencia. ausentarse por varios minutos se deberá dejar cerrando todas las aplicaciones críticas. Y con protección de contraseña segura.
- La Unidad de Sistemas visitará su departamento y lugar de trabajo periódicamente para revisar y determinar los programas informáticos utilizados: Si se encontrare copias sin licencias, o material ajeno a la institución estos serán eliminados.

DE LAS NORMAS DE CLAVES

- Los equipos de cómputo de la Institución se encuentran configurados bajo dos niveles de seguridad, el primero es la clave de acceso al Sistema Operativo, y el segundo las claves de acceso a las aplicaciones del usuario final, los usuarios de este sistema son los responsables del cuidado e ingreso de estas claves.
- El sistema Financial cada vez que requiera cambiar de clave la solicitará automáticamente, el usuario debe ingresar la clave que considere conveniente y segura, procurando evitar colocar el nombre, apellido, fecha de cumpleaños, o algún dato personal que sean conocidos por los demás compañeros.
- Las claves deben contener en lo posible combinaciones de letras mayúsculas, minúsculas y números
- Los usuarios no deben comentar a nadie las claves de acceso al Sistema, las contraseñas son personales e intransferibles.
- Está terminantemente prohibido ingresar al Sistema con claves de otras personas.
- No anotar la contraseña en un papel que pueda estar al alcance de algún compañero. La contraseña debe ser memorizada en el menor tiempo posible.

DE LA UTILIZACIÓN DE DISPOSITIVOS DE ALMACENAMIENTO EXTERNO

- El personal de la Institución no está autorizado a usar ningún dispositivo de almacenamiento externo sea este cd rom, flash memories, etc. En caso de requerir el uso de estos medios comunicarse con el personal de la unidad de Sistemas de la Institución.

- El personal de Sistemas debe chequear los dispositivos de almacenamiento de información externos a utilizar con el objeto de verificar que estén libres de virus.

- Si el dispositivo de almacenamiento tiene virus el personal de Sistemas procederá a utilizar el antivirus de la Institución o darle formato en caso de que no sea posible limpiar el virus.

DE LOS PROCESOS INTERNOS

- Diariamente se procede a realizar el cierre del día. El personal que labora en la institución está autorizado a utilizar el Sistema Financial durante el horario asignado.
- Si el personal de la Institución requiere extender su tiempo de labores, debe comunicar con anticipación al personal de Sistemas, caso contrario no se responsabiliza de las operaciones que pudieren quedar inconclusas fuera del horario señalado.
- El personal autorizado para operar los equipos según sus funciones son los descritos en el Orgánico Funcional de la Institución y/o el personal que ha sido previamente autorizado por escrito de la Gerencia General quienes a su vez son responsables de los bienes asignados.
- Se establece que los empleados de la Institución son propietarios y responsables de la información manejada (ingresada, eliminada o modificada).
- Todo personal que requiera movilizar un equipo fuera de las instalaciones de la Institución, requiere del permiso y autorización de Gerencia o Jefatura y es responsable del bien asignado, hasta la devolución del mismo.

DEL ACCESO A INTERNET

- El uso del Internet será de uso exclusivo para actividades propias de la Cooperativa.
- El acceso y niveles de uso al internet como del correo electrónico, estará establecido de acuerdo a la función que desempeña en la institución.

- Si se requiere modificar el nivel de acceso y/o uso este debe ser autorizado por el Jefe de la Oficina o el Gerente General en forma escrita y bajo las condiciones y los horarios que ellos lo establezcan.
- Se prohíbe el manejo de correos electrónicos personales para asuntos de la institución.
- No se debe abrir correos o archivos adjuntos de remitentes desconocidos, pues podrían ser virus.
- No se debe entregar ningún tipo de información personal, solicitados a través de los correos electrónicos.
- Queda estrictamente prohibido utilizar cualquier aplicación como: descargadores de música, videos, juegos, escuchar música en línea, visitar páginas para adultos y/o sexo explícito, ya que este tipo de prácticas tienen el riesgo de contener virus, spyware y otro tipo de aplicaciones, las mismas que reducen el rendimiento de los aplicativos y servicio de Internet.

DE LA INFORMACION

Cada usuario es el responsable de cada uno de los sistemas de información que mantiene la Institución y que debe proceder según los siguientes lineamientos:

1. Deberá identificar toda la información confidencial que corresponda a su área de responsabilidad directa cualquiera sea su forma y medio de conservación, debiendo clasificar según los siguientes tres criterios:

CONFIDENCIALIDAD:

1. PÚBLICO: Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea de la Institución o no.

2. RESERVADA – USO INTERNO: Información que puede ser conocida y utilizada por todos los empleados y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas para la Institución.

3. RESERVADA: Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la Institución.

INTEGRIDAD:

1. Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatividad.

2. Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves.

3. Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas o graves.

DISPONIBILIDAD:

1. Información cuya inaccesibilidad no afecta la operatividad durante un mes.

2. Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas.

3. Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas.

4. Información cuya inaccesibilidad permanente durante 2 horas podría ocasionar pérdidas significativas.

2. Deberá autorizar el acceso a la información a toda persona o grupo que requiera. Este acceso contemplará los privilegios respectivos de usuario a su función, coordinando para esto con las áreas que involucren su operación.
3. Podrá delegar su función a personal idóneo, pero conservarán la responsabilidad del cumplimiento de la misma. Además, deberán verificar la correcta ejecución de las tareas asignadas. Esta delegación estará programada conjuntamente con el área de Recursos Humanos y los mandos directivos que lo requieran.

4. Apoyar al Área Tecnológica en la generación de los controles necesarios para el almacenamiento, procesamiento, distribución y uso de la información, como de la implementación de soluciones si el caso lo amerite.

El usuario que no aplique normas de confidencialidad y seguridad de la información de la Cooperativa, será sancionado de acuerdo a disposiciones de Gerencia General o Consejo de Administración, quienes se reservan el derecho de aplicar cualquier trámite judicial.

Anexo 2:

ACUERDO DE CONFIDENCIALIDAD

En mi condición de empleado y en consideración de la relación laboral que mantengo con la **Cooperativa de Ahorro y Crédito "SAC Ltda."**, así como del acceso que se me permite a sus Bases de Información, constato que:

1) Soy consciente de la importancia de mis responsabilidades en cuanto a no poner en peligro la integridad, disponibilidad y confidencialidad de la información que maneja la Cooperativa. En concreto entiendo y me comprometo a cumplir los Procedimientos de Seguridad de los Sistemas de Información que corresponden a mi función en la Cooperativa.

2) Me comprometo a cumplir, asimismo, todas las disposiciones relativas a la políticas internas en materia de uso y divulgación de información, y a no divulgar ningún tipo de información que reciba a lo largo de mi relación con la empresa, inclusive aun después de que finalice dicha relación, tanto sea información propia de la empresa, como de sus clientes o proveedores, bases de datos, códigos fuentes, cualquiera que sea la forma de acceso a tales datos o información y el soporte en el que consten, quedando absolutamente prohibido obtener copias sin previa autorización.

3) Entiendo que el incumplimiento de cualesquiera de las obligaciones que constan en el presente documento, intencionadamente o por negligencia, podrían implicar en su caso, las sanciones disciplinarias correspondientes por parte de la Cooperativa y los posibles reclamos legales por parte de la misma de los daños o perjuicios causados.

Dado en la Ciudad de Ambato, a los XX días del mes de XXXXXX del 20XX.

NOMBRE:	FIRMA:
CEDULA IDENTIDAD No.	

Anexo 3:

Mapeo entre objetivos de TI y procesos de COBIT 5

Figura 23—Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y los Procesos

			Meta relacionada con las TI																
			Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionan beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
	Procesos de COBIT 5		Financiera						Cliente		Interna							Aprendizaje y Crecimiento	
Evaluar, Orientar y Supervisar	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	Asegurar la Entrega de Beneficios	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Asegurar la Optimización del Riesgo	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Asegurar la Optimización de los Recursos	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Asegurar la Transparencia hacia las partes interesadas	S	S	P			P	P						S	S	S		S
Alinear, Planificar y Organizar	APO01	Gestionar el Marco de Gestión de TI	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	Gestionar la Estrategia	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	Gestionar la Arquitectura Empresarial	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	Gestionar la Innovación	S			S	P			P	P		P	S		S			P
	APO05	Gestionar el portafolio	P		S	S	P	S	S	S	S		S		P				S
	APO06	Gestionar el Presupuesto y los Costes	S		S	S	P	P	S	S			S		S				
	APO07	Gestionar los Recursos Humanos	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	Gestionar las Relaciones	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	Gestionar los Acuerdos de Servicio	S			S	S	S	P	S	S	S	S		S	P	S		
	APO10	Gestionar los Proveedores		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO11	Gestionar la Calidad	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO12	Gestionar el Riesgo		P		P		P	S	S	S	P			P	S	S	S	S
	APO13	Gestionar la Seguridad		P		P		P	S	S		P				P			

Figura 23—Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y los Procesos *(cont.)*

			Meta relacionada con las TI																
			Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
		Procesos de COBIT 5	Financiera						Cliente		Interna							Aprendizaje y Crecimiento	
Construcción, Adquisición e Implementación	BAI01	Gestionar los Programas y Proyectos	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Gestionar la Definición de Requisitos	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Gestionar la Identificación y la Construcción de Soluciones	S			S	S		P	S			S	S	S	S			S
	BAI04	Gestionar la Disponibilidad y la Capacidad				S	S		P	S	S		P		S	P			S
	BAI05	Gestionar la introducción de Cambios Organizativos	S		S		S		S	P	S		S	S	P				P
	BAI06	Gestionar los Cambios			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Gestionar la Aceptación del Cambio y de la Transición				S	S		S	P	S			P	S	S	S		S
	BAI08	Gestionar el Conocimiento	S				S		S	S	P	S	S			S		S	P
	BAI09	Gestionar los Activos		S		S		P	S		S	S	P			S	S		
	BAI10	Gestionar la Configuración		P		S		S		S	S	S	P			P	S		
Entregar, dar Servicio y Soporte	DSS01	Gestionar las Operaciones		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio				P			P	S		S				S	S		S
	DSS03	Gestionar los Problemas		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Gestionar la Continuidad	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Gestionar los Servicios de Seguridad	S	P		P			S	S		P	S	S		S	S		
	DSS06	Gestionar los Controles de los Procesos del Negocio		S		P			P	S		S	S	S		S	S	S	S
Supervisión, Evaluación y Verificación	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno		P		P		S	S	S		S				S	P		S
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos		P		P	S		S			S					S		S