FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

ANÁLISIS DE RIESGOS DE LOS PROCESOS DEL ÁREA DE TI DE LA COOPERATIVA DE AHORRO Y CRÉDITO “PEDRO MONCAYO LTDA.”

AUTORES

FANY CACUANGO ULCUANGO

ERIKA ELIANA MORA FLOR

AÑO

2017

FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

ANÁLISIS DE RIESGOS DE LOS PROCESOS DEL ÁREA DE TI DE LA COOPERATIVA DE AHORRO Y CRÉDITO “PEDRO MONCAYO LTDA.”

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingenieras en Sistemas de Computación e Informática

Profesor Guía

Mgt. Eddy Mauricio Armas Pallasco

Autores

Fany Cacuango Ulcuango

Erika Eliana Mora Flor

Año

2017

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con las estudiantes, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.”

_____

Eddy Mauricio Armas Pallasco
Magister en Gerencia de Sistemas y TI
C.C. 171171580-3

DECLARACIÓN DEL PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

Tannia Jacqueline Álava Freire
Magister en Administración Tecnológica
CC. 170629916-9

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaramos que este trabajo es original, de nuestra autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

Fany Cacuango Ulcuango	Erika Eliana Mora Flor
C.C. 171117061-1	C.C. 171032870-7

AGRADECIMIENTOS

Quiero agradecer primero a Dios por haberme acompañado paso a paso cada día de mi vida, y luego a mis profesores de la Universidad de las Américas que compartieron su conocimiento y experiencias profesionales y de vida, un especial agradecimiento a Marco Galarza por su apoyo constante a lo largo de este proceso, y a Eddy Armas quién me guio hasta finalizar este proyecto.

Agradezco a mi familia por su constante apoyo y por su motivación diaria para que finalice la carrera.

A todos mil gracias de todo corazón.

Fany

AGRADECIMIENTOS

A Dios por todas las bendiciones recibidas durante esta etapa durísima de mi vida.

A mis amados padres que sin ellos no hubiera tenido una razón para esforzarme conseguir un anhelo suspendido en el tiempo.

A Marco Galarza y Eddy Armas, quienes con su apoyo y orientación me ayudaron a no claudicar y culminar con un sueño que parecía imposible y que ahora se convirtió en una realidad palpable.

Erika

DEDICATORIA

Dedico este trabajo a mis padres por ser quienes han estado motivándome para finalizar la carrera, sin ellos no lo habría logrado.

Fany

DEDICATORIA

A mis Padres Adorados: Rafael y Alicia, cuyo único anhelo ha sido que culmine esta carrera profesional.

A mis queridos sobrinos: Mateo, Fabricio, Ana Paula y Valentina, para que siempre tengan presente que no importa ni la edad ni las adversidades de la vida, cuando uno quiere alcanzar un sueño y un anhelo, solo se necesita constancia y perseverancia para lograrlo.

Erika

RESUMEN

En la investigación de este trabajo de titulación, se pretende evaluar el grado de madurez de las actividades tecnológicas, analizar los riesgos con criticidad alta existentes en el Departamento de Tecnología de la Información y Comunicaciones, y elaborar un plan de mejoras que permita a la Cooperativa de Ahorro y Crédito “Pedro Moncayo Ltda.” cumplir con el Plan Estratégico actual.

Para el análisis de riesgos se utilizará la metodología de COBIT 5 para Riesgos (ISACA, 2013), la misma que es apropiada para determinar los problemas, amenazas y vulnerabilidades que pueden afectar al servicio y provocar pérdidas económicas, de confiabilidad y de incumplimientos con las leyes, regulaciones o normativas emitidos por la “Superintendencia del Sistema Cooperativo y Financiero Popular y Solidario”.

Este trabajo de titulación consta de 6 capítulos que se explicarán a continuación:

En el capítulo I, Introducción, se describe los antecedentes, situación de conflicto y problemática actual del Departamento de Tecnología de la Información y Comunicaciones; así como, se plantean el objetivo general y los específicos, alcance y justificación de este proyecto de investigación.

En el capítulo II, Marco Teórico, se establece los fundamentos teóricos utilizados en este proyecto de titulación.

En el capítulo III, se explica la situación actual de la Cooperativa de Ahorro y Crédito “Pedro Moncayo Ltda.” y del Departamento de Tecnología de la Información y Comunicaciones y se evalúa el grado de madurez de las actividades tecnológicas ejecutadas en este departamento.

En el capítulo IV, se identifican y analizan los riegos, en base a la metodología COBIT 5 para Riesgos (ISACA, 2013), utilizando Balanced Scorecard, para

establecer la criticidad de las amenazas y vulnerabilidades, de acuerdo a una escala y a parámetros de impacto o consecuencia y probabilidad o frecuencia que podrían causar pérdidas económicas, de confiabilidad e imagen corporativa, e incluso el incumplimiento de las normas, regularizaciones y reglamentos emitidos por los entes control para COAC “Pedro Moncayo Ltda.”

En el capítulo V, Plan de Mejora, se indican, como producto final, los planes de acción a ejecutar para eliminar, mitigar o minimizar los riesgos identificados con criticidad “Alta”.

En este capítulo VI, Conclusiones y Recomendaciones, se detalla las conclusiones y recomendaciones obtenidas como resultado de este proyecto.

ABSTRACT

In the research of this titling work, it is tried to evaluate the degree of maturity of the technological activities, to analyze the risks with high criticality existing in the Department of Information Technology and Communications, and to elaborate an improvement plan that allows the Cooperative of Savings and Credit "Pedro Moncayo Ltda." Comply with the current Strategic Plan.

For risk analysis, the COBIT 5 Risk Methodology (ISACA, 2013) will be used, which is appropriate to determine the problems, threats and vulnerabilities that may affect the service and cause economic loss, reliability and non-compliance with Laws, regulations or regulations issued by the "Superintendence of the Cooperative and Popular and Solidary Financial System".

This titling work consists of 6 chapters that will be explained next:

Chapter I, Introduction, describes the background, situation of conflict and current problems of the Department of Information Technology and Communications; As well as the general and specific objectives, scope, and justification of this research project.

In chapter II, Theoretical Framework, establishes the theoretical foundations used in this titling project.

In Chapter III, the current situation of the "Pedro Moncayo" Savings and Credit Cooperative and the Department of Information Technology and Communications is explained and the degree of maturity of the technological activities carried out in this department is evaluated.

Chapter IV, Risk Assessment, identifies and analyzes the risks, based on the COBIT 5 methodology for Risks (ISACA, 2013), using a Balanced Score Card, to establish the criticality of threats and vulnerabilities, according to a Scale and

parameters of impact or consequence and probability or frequency that could cause economic losses, reliability and corporate image, and even failure to comply with the rules, regulations and regulations issued by the control entities for COAC "Pedro Moncayo Ltda.”

Chapter V, Improvement Plan, indicates the action plans to be implemented to eliminate, to mitigate or minimize the risks identified only with "High" criticality.

In this chapter VI, Conclusions and Recommendations, the conclusions and recommendations obtained because of this project are detailed.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1 Capítulo I. Introducción

En este capítulo se explicará los antecedentes, situación de conflicto y se detallará la problemática; así como, se plantearán los objetivos, alcance y justificación de este proyecto de investigación.

1.1. Antecedentes.

El Gobierno Nacional del Ecuador, consiente de los problemas financieros ocurridos en años anteriores en el sector de la Economía Popular y Solidaria "SEPS", ha impulsado un nuevo modelo institucional que se encuentra controlado y regulado por la Superintendencia del Sistema Cooperativo y Financiero Popular y Solidario, mediante la Ley Orgánica de la Economía Popular y Solidaria y del Sector Financiero Popular y Solidario, LOEPS, por lo que todas las Cooperativas de Ahorro y Crédito del país tienen que cumplir las nuevas regulaciones, leyes y normativas vigentes.

La Cooperativa de Ahorro y Crédito Pedro Moncayo Ltda., COAC, con el propósito de alinearse con estas normativas y regulaciones indicadas en LOEPS, ha elaborado el "Plan Estratégico 2015 – 2017" (Dávila R., 2014), en donde se establecen las áreas de iniciativa estratégica, entre estas áreas se encuentra el Departamento de Tecnología de Información y Comunicaciones dentro de la perspectiva de "aprendizaje y desarrollo".

El Departamento de Tecnología de Información y Comunicaciones mantiene un objetivo estratégico dentro de este plan y para cumplirlo necesita fortalecer sus procesos; por lo que, requiere identificar el grado de madurez y analizar los riesgos inherentes de estas actividades tecnológicas, para establecer un plan de mejoras en base a los inconvenientes y/o problemas encontrados.

1.2. Contexto de la investigación

1.2.1. Cooperativa de Ahorro y Crédito Pedro Moncayo Ltda.

La Cooperativa de Ahorro y Crédito Pedro Moncayo Ltda., “COAC” fue creada en el año de 1.964 hace 51 años por un grupo de tabacundeños emprendedores liderados por Monseñor Isaías Barriga, un pionero ligado a la iglesia católica, con el propósito de organizar sus recursos económicos a través del ahorro y obtener beneficios como el crédito para dinamizar una economía activa dentro de sus hogares y del sector.

Esta Cooperativa de Ahorro y Crédito de acuerdo con su propósito el ser un ente financiero sin fines de lucro y convencer a los habitantes del Cantón Pedro Moncayo y sitios aledaños, ha logrado posicionarse en los primeros sitiales dentro del cooperativismo, avalado por la calidad de servicio brindado a sus socios y clientela en general.

1.2.2. Estructura Organizacional

Actualmente la Cooperativa de Ahorro y Crédito Pedro Moncayo Ltda., “COAC”, se encuentra conformada por una Asamblea General de socios, organismo que es la Máxima Autoridad de la Cooperativa, el Consejo de Administración constituido por tres Comités: Administración Integral de Riesgos, Adquisiciones, y Cumplimiento y por la Comisión de Educación; el Consejo de Vigilancia; la Gerencia General; 12 departamentos con 3 áreas administrativas, operativas y del negocio. Entre éstos departamentos se mencionan los departamentos de Tecnología de Información y Comunicaciones, Negocios y Operaciones, por ser los principales participantes en los procesos a investigar en este trabajo de titulación.

En la siguiente figura se indica la estructura organizacional de COAC.

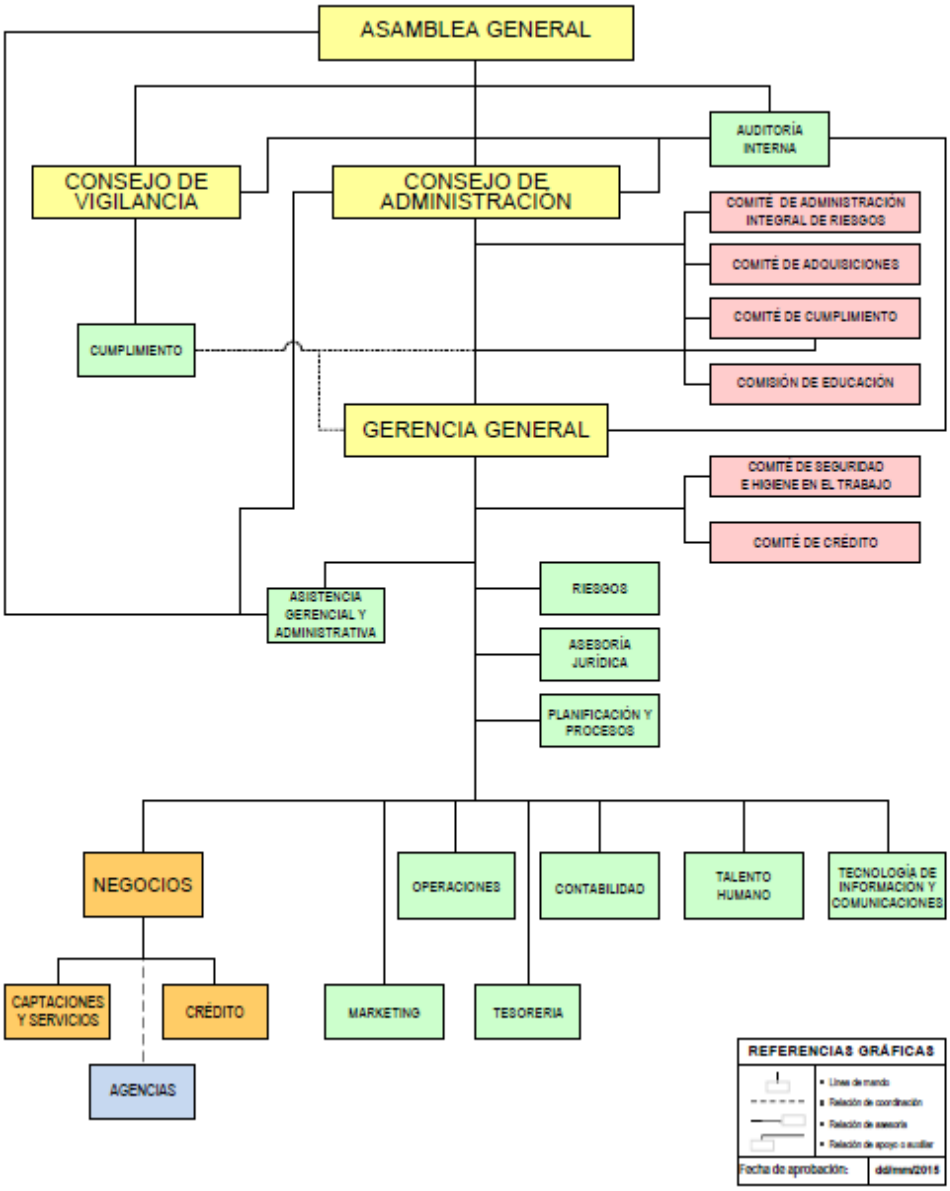


Figura 1. Estructura Organizacional COAC Ltda.

Tomado de COAC Ltda. *(Organigrama P Moncayo, 2016)*.

1.2.3. Misión

La misión de COAC Ltda., indicada en el Plan Estratégico 2015 – 2017 es:

> Entregar productos y servicios financieros de excelencia, contribuyendo al mejoramiento del bienestar integral de nuestros socios y clientes,

> satisfaciendo sus necesidades de una manera solidaria, ágil, oportuna y efectiva, retribuyendo así la confianza y fidelidad que tienen con la Institución, basados en los principios universales del cooperativismo. (pág. 7)

1.2.4. Visión

La visión establecida en el informe del Plan Estratégico 2015 – 2017 es:

> Ser una Institución financiera del sector de la economía popular y solidaria, sólida y en permanente crecimiento en la zona norte de la provincia de Pichincha y en la provincia de Imbabura, siendo un referente en el buen servicio y atención a nuestros socios y clientes, con productos y servicios de excelencia que cumplan con sus expectativas, aportando a su bienestar y desarrollo. (pág. 8)

1.2.5. Productos y Servicios

Los productos y servicios que ofrece la Cooperativa de Ahorro y Crédito “Pedro Moncayo Ltda.” a sus asociados son los siguientes:

<u>Productos</u>

- Inversiones
- Crédito
  - Crédito Inmediato
  - Crédito Productivo
  - Crédito Educativo
  - Microcrédito
  - Crédito Excelente
  - Créditos de Consumo
  - Crédito Hipotecario
- Cuentas de Ahorro

<u>Ahorro Infantil</u>

Cuenta Cosecha

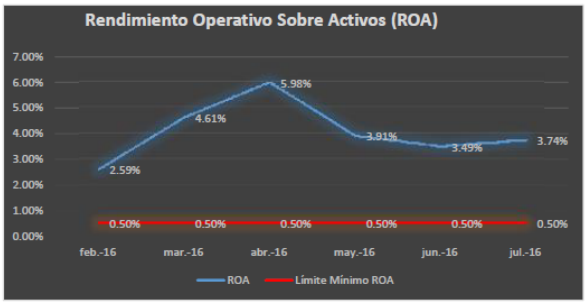
Servicios

- Servicios Complementarios
  - Transferencias Interbancarias
  - Pagos de Impuestos y Servicios Básicos
  - Pagos a terceros
- Servicios Virtuales para los siguientes productos:
  - Crédito Hipotecario
  - Cuenta Ahorro Cosecha
  - Cuenta Ahorro Crecer

La Cooperativa “Pedro Moncayo” Ltda., maneja indicadores financieros que le permiten identificar riesgos y oportunidades de negocio para alcanzar las metas y objetivos estratégicos.

- Activos

INDICADORES		
FECHA	ROA	Límite Mínimo ROA
feb-16	2.59%	0.50%
mar-16	4.61%	0.50%
abr-16	5.98%	0.50%
may-16	3.91%	0.50%
jun-16	3.49%	0.50%
jul-16	3.74%	0.50%
ago-16		
sep-16		
oct-16		
nov-16		
dic-16		

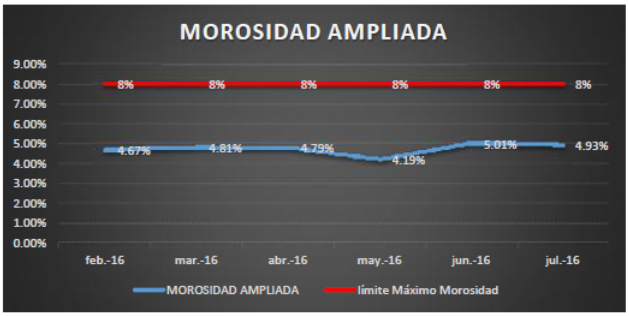


Representa la rentabilidad y eficiencia en la utilización de los activos. La Cooperativa registra indicadores superiores al mínimo establecido del 0,50%, lo que demuestra una adecuada administración de los activos institucionales

Figura 2. Rendimiento Operativo sobre Activos a agosto del 2016
Tomado de *(COAC Pedro Moncayo Ltda - Transparencia, 2016)*

- Morosidad

FECHA	MOROSIDAD AMPLIADA	límite Máximo Morosidad
feb-16	4.67%	8%
mar-16	4.81%	8%
abr-16	4.79%	8%
may-16	4.19%	8%
jun-16	5.01%	8%
jul-16	4.93%	8%
ago-16		
sep-16		
oct-16		
nov-16		
dic-16		



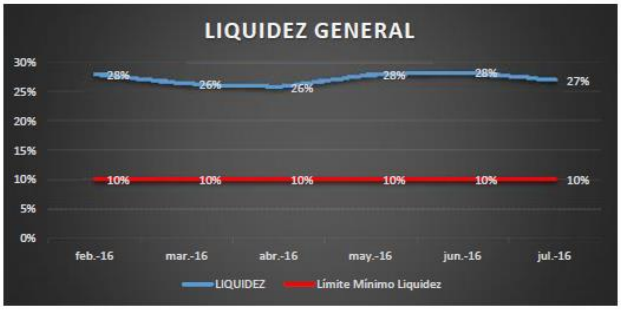
La Cooperativa realiza un exaustivo y profesional analisis para la colocación de la cartera. La institución registra un promedio del índice de morosidad del 4,73% muy por debajo del límite establecido (8%) y de la media del sector financiero demostrando una adecuada administración de la cartera de crédito

Figura 3. Morosidad Ampliada a agosto del 2016

Tomado de (COAC Pedro Moncayo Ltda - Transparencia, 2016)

- Liquidez General

FECHA	LIQUIDEZ	Límite Mínimo Liquidez
feb-16	28%	10%
mar-16	26%	10%
abr-16	26%	10%
may-16	28%	10%
jun-16	28%	10%
jul-16	27%	10%
ago-16		
sep-16		
oct-16		
nov-16		
dic-16		



Los socios tiene la seguridad, que al acudir a la institución pueden retirar sus dineros de forma inmediata. La Cooperativa registra un índice promedio de liquidez del 27 %, muy por encima del límite establecido, por lo que que la institución puede hacer frente a los retiros inmediatos de los socios sin inconvenientes

Figura 4. Liquidez General a agosto del 2016

Tomado de (COAC Pedro Moncayo Ltda - Transparencia, 2016)

1.2.6. Áreas de Iniciativa Estratégicas

Basados en el “Cuadro de Mando Integral” del Balanced Scorecard para COAC Ltda., indicado en el Plan Estratégico 2015 – 2017 (Dávila R., 2014, pág. 9), se identificaron como áreas de iniciativa estratégicas a las siguientes:

Perspectiva	Áreas de Iniciativa Estratégica
Resultados financieros y sociales	1. Gestión del Balance Social 2. Gestión Financiera
Clientes	3. Satisfacción de socios y clientes 4. Gestión comercial y de mercado
Procesos	5. Fortalecimiento organizacional
Aprendizaje y desarrollo	6. Gestión del Talento Humano 7. Gestión de Tecnología de Información y Comunicaciones

Figura 5. Áreas de Iniciativa Estratégicas

Tomado de Plan Estratégico de (Cooperativa de Ahorro y Crédito Pedro Moncayo Ltda., 2016)

1.2.7. Área de Tecnología de Información y Comunicaciones

Las actividades por los que es responsable el área de Tecnología de Información y Comunicaciones son las siguientes:

- Administración del centro de datos y seguridad informática,
- Soporte al usuario

Para cumplir con las actividades que tienen definidas existen los siguientes cargos o roles:

- ✓ Jefe de Sistemas
- ✓ Asistente de Sistemas

1.3. Problema de investigación: Situación Conflicto y Hecho Científico

Al estar el Departamento de Tecnología de la Información y Comunicaciones dentro de las áreas de iniciativas estratégicas, ha identificado un objetivo que se

encuentra incluido en la “Perspectiva de Aprendizaje y Desarrollo” como parte del “Mapa Estratégico del Balanced Scorecard (BSC) o Cuadro de Mando Integral (CMI) de Kaplan y Norton” (PLAN ESTRATÉGICO 2015 - 2017). Este objetivo es el siguiente:

> Objetivo 7: Fortalecer la gestión de Tecnología de la Información y Comunicaciones.
>
> 1. Diseñar e implementar un esquema de medición de satisfacción de usuarios internos de TIC.
> 2. Implementar los recursos claves para la gestión de TIC.
> 3. Definir e implementar un modelo de gestión de TIC basado en buenas prácticas.
> 4. Adecuar la infraestructura del Centro de Cómputo (pág. 15)

Para cumplir con este objetivo, el Departamento de Tecnología de Información y Comunicaciones necesita realizar ajustes tecnológicos y operativos en las actividades que ejecuta, debido a que actualmente los mismos no se alinean con el “Plan Estratégico 2015 - 2017” que COAC Ltda., quiere alcanzar.

En el caso de la actividad de administración del centro de datos y seguridad informática, actualmente no existe una documentación sobre: políticas, estándares, procedimientos e instructivos que permitan garantizar la operatividad del centro de datos. Tampoco cuentan con infraestructura tecnológica de seguridad para proteger la información crítica y vital de los socios de la Cooperativa.

En el proceso de soporte al usuario cuyas actividades consisten principalmente en la instalación de redes de datos, enlaces, interfaces de red, telefonía, instalación, configuración y administración de plataformas, sistemas y aplicaciones a nivel de hardware y software, entre otros; y al ser tareas ejecutadas por el Jefe y el Asistente de Sistemas únicamente, han provocado en

algunas ocasiones retrasos en la atención a los usuarios finales, los cuales al final tienen una percepción de mala calidad del servicio que brinda el departamento.

Por tal motivo, en esta investigación se determinará el grado de madurez y se realizará un análisis de riesgos de las actividades del Departamento de Tecnología de la Información y Comunicaciones para establecer un plan de mejora en base a los resultados obtenidos, utilizando como metodología COBIT 5 para Riesgos (ISACA, 2013).

El presente trabajo de titulación puede contribuir con el objetivo planteado por el área de Tecnología de Información y Comunicaciones y alinearse con el "Plan Estratégico 2015 – 2017" que la Cooperativa de Ahorro y Crédito "Pedro Moncayo" quiere alcanzar, esta afirmación se hace en base a lo siguiente:

- Es evidente que el Departamento de Tecnología de la Información y Comunicaciones es el responsable de la operatividad de la Cooperativa, lo que significa que es vital mantener todas las actividades tecnológicas disponibles para no afectar al negocio.

- Es concreto debido a que el resultado obtenido del análisis de riesgos les permitirá tomar acciones correctivas a corto, mediano y largo plazo, ya sea con procesos operativos o con proyectos tecnológicos.

- Es factible establecer un plan de mejora en base a las recomendaciones señaladas en el informe de resultados del análisis de riesgos de las actividades tecnológicas evaluadas.

1.4. Objetivo General

Realizar un plan de mejoras para el Departamento de Tecnología de la Información y Comunicaciones que se alineen a los objetivos estratégicos del negocio, a través del análisis de riesgos de los procesos identificados en el “Plan Estratégico 2015 - 2017” de la Cooperativa de Ahorro y Crédito “Pedro Moncayo Ltda.”

1.5. Objetivos Específicos

- Identificar el grado de madurez de las actividades tecnológicas del Departamento de Tecnología de la Información y Comunicaciones, en base a la situación actual de la Cooperativa de Ahorro y Crédito “Pedro Moncayo Ltda.”

- Analizar los riesgos inherentes de las actividades tecnológicas, utilizando un marco de referencia o un estándar.

- Elaborar un plan de mejora en base al resultado del análisis de riesgos de las actividades tecnológicas evaluadas y con criticidad “Alta”.

1.6. Justificación

Las constantes estafas y fraudes sufridos por el sector económico popular en años anteriores debido a la falta de una regulación eficiente al sistema cooperativo y financiero popular del país, obligó al Gobierno Nacional garantizar a todos los asociados de las Cooperativas de Ahorro y Crédito, un control adecuado de todas las áreas, servicios y productos que ofrecen estas instituciones financieras a sus socios, a través de la Ley Orgánica de la Economía Popular y Solidaria y del Sector Financiero Popular y Solidario (LOEPS, 2000), emitida por SEPS (Sistema Cooperativo y Financiero Popular y Solidario, 2011).

La Cooperativa de Ahorro y Crédito Pedro Moncayo Ltda., orientada al servicio sin fines de lucro y calidad total y, en base a sus principios, misión y visión ha decidido evaluar los riesgos tecnológicos de las actividades de información del Departamento de Tecnología de la Información y Comunicaciones, debido a que toda la información personal y transaccional de los socios se encuentra almacenada y recolectada en este departamento y en empresas proveedoras de servicios tecnológicos.

De esta manera la Cooperativa COAC, podrá utilizar el informe con las recomendaciones de las actividades tecnológicas, que se obtendrán como resultado del estudio de este proyecto de titulación y así realizar las mejoras a los procesos que consideren necesarios y obligatorios para cumplir con las regulaciones y normativas vigentes en el país para el Sistema Cooperativo y Financiero Popular y Solidario.

2 Capítulo II. Marco Teórico

En este capítulo se señalará los fundamentos teóricos que avala esta investigación; en otras palabras, se detallarán los términos, conceptos y metodologías para identificación y análisis de riesgos que se utilizarán dentro de este proyecto de titulación.

2.1 Ley Orgánica de Economía Popular y Solidaria

Las Cooperativas de Ahorro y Crédito están regidas por normas emitidas por los entes de control, específicamente por la ley Orgánica de Economía Popular y Solidaria, LOEPS. Esta ley fue aprobada el 13 de abril del 2011 y está vigente desde 17 febrero 2012.

La ley Orgánica de Economía Popular y Solidaria crea la Superintendencia de Economía Popular y Solidaria (SEPS, 2011), como organismo técnico de control

con jurisdicción nacional, cuyo propósito es el de fiscalizar a las organizaciones pertenecientes a la economía popular y solidaria; es decir, cooperativas, asociaciones y organizaciones comunitarias.

2.1.1 Estructura del proyecto de Ley

Ley está compuesta por 7 títulos:

i) Del ámbito, objetos y principios
ii) De la Economía Popular y Solidaria
iii) Del Sector Financiero Popular y Solidario
iv) De los organismos de Integración e Entidades de Apoyo
v) Del Fomento, Promoción e Incentivos
vi) De las relaciones con el Estado
vii) De las Obligaciones e Infracciones y Sanciones

El documento oficial de la Ley Orgánica de Economía Popular y Solidaria, LOEPS, está compuesta por: 179 artículos, y 33 disposiciones.

Por tal motivo, la Cooperativa de Ahorro y Crédito “Pedro Moncayo Ltda.”, amparada en estos artículos y disposiciones, especialmente en el artículo 34 numeral 12 y por medio de su Consejo de Administración podrá: “Aprobar el plan estratégico, el plan operativo anual y su presupuesto y someterlo a conocimiento de la Asamblea General”. Además, a través del artículo 94: “Información”, en donde se detalla que: “Las cooperativas de ahorro y crédito pondrán a disposición de los socios y público en general, la información financiera y social de la entidad, conforme a las normas emitidas por la Superintendencia”, según lo estipulado en LOEPS (MIES, 2012).

2.2 Riesgo

2.2.1 Definición

El riesgo “Es algo desconocido que, si se produce, afecta en forma negativa o positiva los objetivos del proyecto. Por lo tanto, un evento incierto puede ser algo bueno o algo malo” (Lledó, 2013, pág. 286).

El riesgo “se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas” (Ciifen, 2011)

Los factores que lo componen son la amenaza y la vulnerabilidad, mientras que el riego se expresa como: Riesgo = Amenaza x Vulnerabilidad.

Entendiéndose por amenaza a las “circunstancias o eventos que pueden desencadenar eventos de pérdida” y por vulnerabilidad los “acontecimientos que contribuyen a la magnitud o frecuencia de eventos de pérdida que ocurren” (Marco de Riesgos de TI, 2009, pág. 26).

2.2.2 Tipos de Riesgo

Se tiene los siguientes tipos:

- Riesgos objetivos, pueden ser calculados matemáticamente; mantienen cierta precisión.

- Riesgo subjetivo, es el grado de incertidumbre ante un evento sujeto estrictamente a la apreciación personal. No requiere de mediciones.

- Riesgos financieros, están asociados a pérdidas económicas.

- Riesgos no financieros, no tienen pérdidas económicas.

- Riesgos dinámicos, son aquellos que se producen por cambios en la economía y tecnología.

- Riesgos estáticos, son causados por desastres naturales, actos deshonestos o errores humanos.

- Riesgos fundamentales, afectan a grandes grupos de la sociedad siendo causados por fenómenos económicos, políticos, naturales.

- Riesgos particulares, son eventos individuales y afectan a personas, empresa.

- Riesgos puros, los resultados posibles son perder o no perder, producen pérdidas tangibles (propiedades, personas) o sobre responsabilidad de terceros.
- Riesgos especulativos, mantienen la posibilidad de perder o ganar.

2.2.3 Gestión de Riesgos

Gestión de Riesgos, es el procedimiento sistemático de identificar, analizar, responder y controlar los riesgos. En cuanto a los objetivos, (Project Management Institute, 2014) tiene la siguiente definición: “Los objetivos de gestión de riesgos consisten en aumentar la probabilidad y el impacto de eventos positivos, y disminuir la probabilidad y el impacto de los eventos negativos en el proyecto” (pág. 309)

2.2.3.1 Procesos de Gestión de Riesgos

Basados en (COBIT 5 para Riesgos, 2013), la gestión de riesgo se apoya en los siguientes procesos:

a. Planificar la Gestión de los Riesgos: Es el proceso de definir como realizar las actividades de gestión de riesgo de un proyecto.

b. Identificar los Riesgos: Es el proceso de determinar los riesgos que pueden afectar al proyecto y documentar sus características.

c. Realizar el Análisis Cualitativo de Riesgo: Es el proceso de priorizar riesgos para análisis o acción posterior evaluando y combinando la probabilidad de ocurrencia e impacto de dichos riesgos.

d. Realizar el Análisis Cuantitativo de Riesgo: Es el proceso de analizar numéricamente el efecto de los riesgos identificados sobre los objetivos generales.

e. Planificar la Respuesta de Riesgo: Es el proceso de desarrollar opciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto.

f. Controlar los Riesgos: Es el proceso de implementar los planes de respuesta a los riesgos. dar seguimiento a los riesgos identificados, monitorear los riesgos residuales, identificar nuevos riesgos y evaluar la efectividad del proceso de gestión de riesgos a través del proyecto.

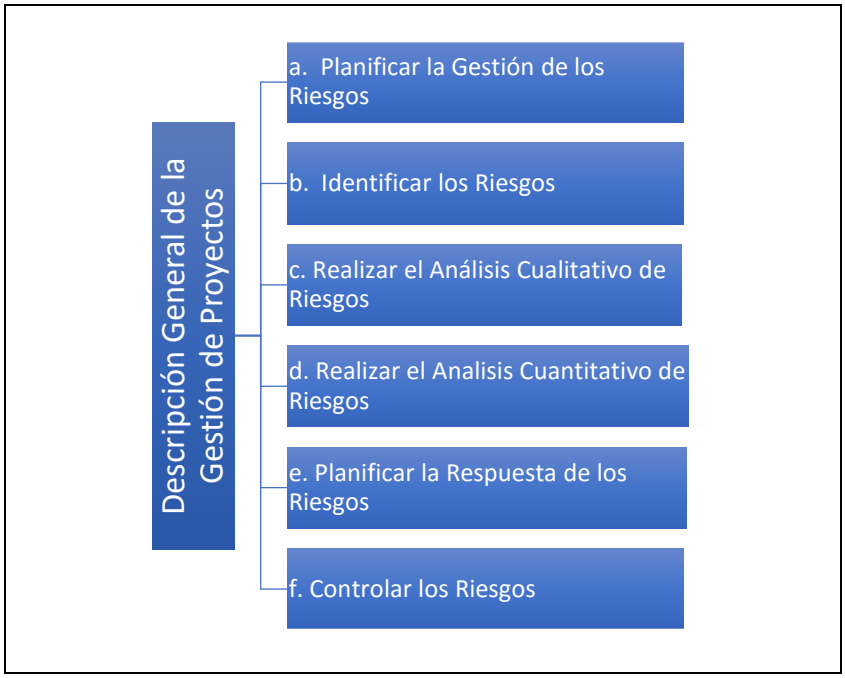


Figura 6. Descripción General de la Gestión de Proyectos
Adaptado de (COBIT 5 para Riesgos, 2013)

2.3 Marco de Referencia

2.3.1 Marco de Referencia COBIT - Control of Objectives for Information and related Technology

La primera versión de COBIT fue publicada por ISACA (Information Systems Audit and Control Association) en 1996, su última edición es el framework COBIT 5 liberada en abril 2012 que integra los marcos de trabajo Val IT, Risk IT, BMIS (Business Model for Information Security) e ITA (IT Assurance Framework). Además, para el desarrollo de sus procesos se apoya en marcos de referencias, estándares y mejores prácticas de COSO, ISO-9000, ISO-31000, ISO-38500, ITIL, TOGAF, IS0-27000 entre otros.

COBIT 5 es una herramienta que apoya a las organizaciones pequeñas o grandes a alcanzar sus objetivos para el gobierno y la gestión de tecnología de

información, TI. De acuerdo a lo indicado en (COBIT 5 Framework Spanish, 2012) “ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos”, (pág. 13).

2.3.2 Principios de COBIT 5

COBIT 5 se basa en 5 principios que son guía para el gobierno y gestión de TI en la empresa. La Figura 7 detalla los 5 principios.

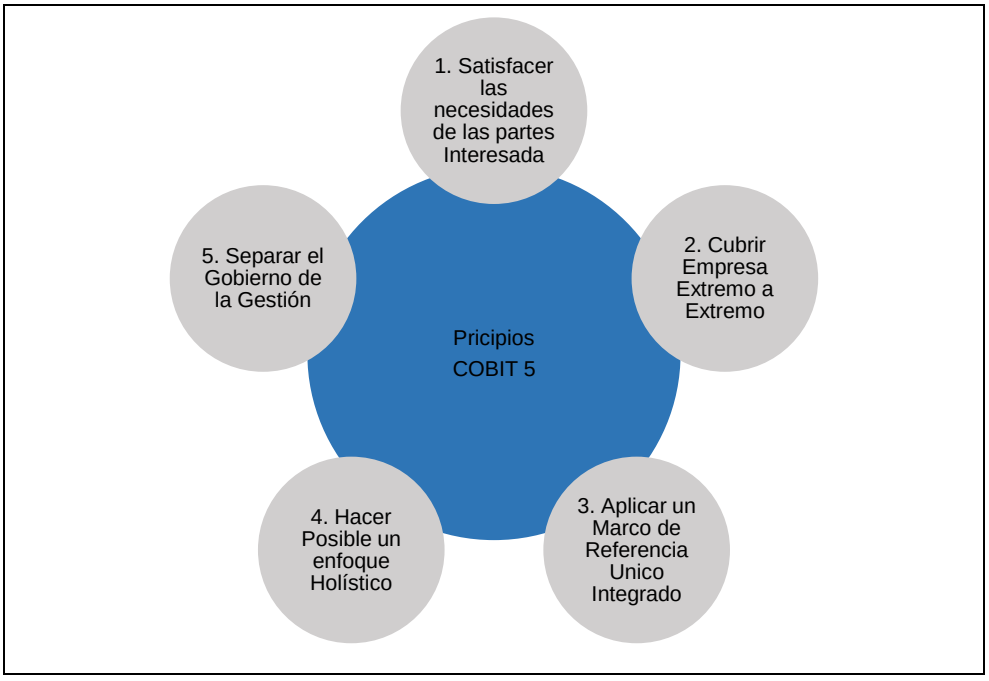


Figura 7. Principios de COBIT 5
Adaptado de *(COBIT 5 Framework Spanish, 2012, pág. 13)*

A continuación, se explica cada uno de los principios en base a (COBIT 5 Framework Spanish, 2012):

Principio 1. Satisfacer las Necesidades de las Partes Interesadas.

Toda empresa crea valor como objetivo de Gobierno “manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos” (pág. 14)

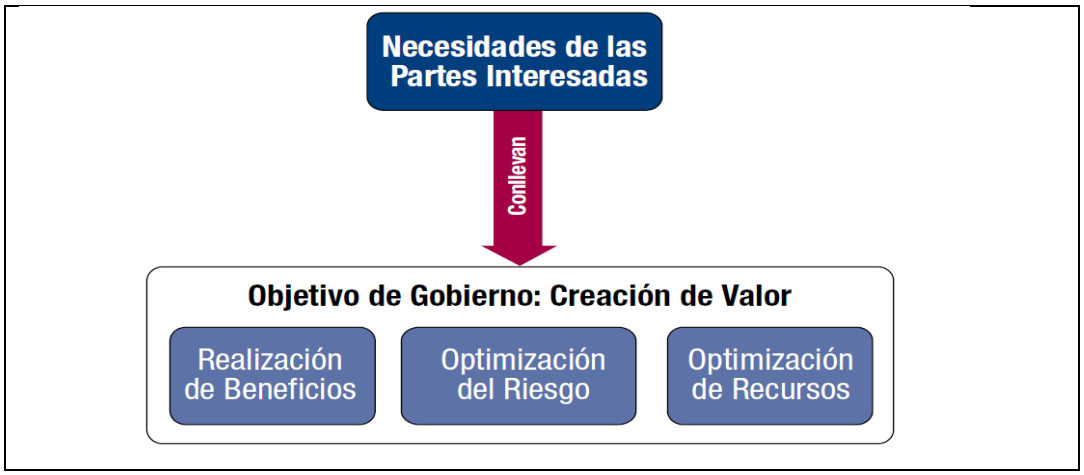


Figura 8. Objetivo de Gobierno
Tomado de (COBIT 5 Framework Spanish, 2012, pág. 17)

Principio 2. Cubrir Empresa de Extremo a Extremo

Aplica a todos los procesos y funciones dentro de la empresa y considera la información y las tecnologías relacionadas como otro activo, y considera que los catalizadores relacionados con TI para el gobierno y la gestión de ser aplicada en toda la empresa. (pág. 14)

Principio 3. Aplicar un marco de referencia único Integrado.

En este principio COBIT ha incluido buenas prácticas y estándares relevantes tales como:

- COSO (Committee of Sponsoring Organizations of the Treadway Commission): que ha sido reconocido como un marco apropiado y exhaustivo para el control interno.

- VAL IT: Proporciona un marco de control global para Gobierno de TI.

- RISK IT: Permite al negocio identificar y valorar los riesgos del negocio relacionados con TI.

- BMIS: (Business Model for Information Security)

- Estándares ISO: para control de calidad de proceso, administración de riesgos, estándares de gobierno corporativo IT, para la seguridad de información los que aplica COBIT: ISO/IEC 9000, ISO/IEC 31000, ISO-38500, ISO 27000

- ITIL: mejores prácticas para servicios de TI con un enfoque de procesos de TI.

- TOGAF, The Open Group Architecture Framework, que proporciona un enfoque para el diseño, planificación, implementación y gobierno de una arquitectura empresarial de información. (pág. 15)

Principio 4. 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 (*enablers*)” para apoyar la implementación de un sistema de gobierno y gestión global de TI para la empresa. Los catalizadores se definen en líneas generales como, cualquier cosa que puede ayudar a conseguir las metas 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 (pág. 14)

Principio 5. Separar el Gobierno de la Gestión.

COBIT 5 hace distinción entre gobierno y gestión cumplen tipos de actividades y estructuras organizacionales diferentes.

- Gobierno: Es responsabilidad de la junta directiva liderada por el presidente.
- Gestión: Está bajo la supervisión de la dirección ejecutiva liderada por el CEO. (pág. 14)

2.3.3 Modelo de Referencia de Procesos

Se basa en 5 dominios, uno para la gobernabilidad y cuatro para la gestión. Los dominios son:

1. Evaluar, Orientar y Supervisar (EDM)
2. Alinear, Planificar y Organizar (PAO)
3. Construir, Adquirir e Implementar (BAI)
4. Entregar, dar Servicio y Soporte (DSS)
5. Supervisar, Evaluar y Valorar (MEA)

A continuación, la Figura 9 describe los dominios y los 37 procesos.

Figura 9. Modelo de Referencia de Procesos

Tomado de (ISACA, 2012, pág. 33)

2.3.4 Modelo de Madurez de procesos

El modelo de madurez de los procesos está basado en la ISO/EC 15504; permitirá medir el desempeño de los procesos de gobierno y gestión de TI.

Los niveles de medición son:

0. Proceso incompleto. - El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.

1. Proceso ejecutado (un atributo). – El proceso implementado alcanza su propósito.

2. Proceso gestionado (dos atributos). – El proceso ejecutado descrito anteriormente está ya implementado de forma gestionada (planificado, supervisado y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.

3. Proceso establecido (dos atributos). – El proceso gestionado descrito anteriormente está ahora implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso.

4. Proceso predecible (dos atributos). – El proceso establecido descrito anteriormente ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.

5. Proceso optimizado (dos atributos). – El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con los metas empresariales presentes y futuros.

Tabla 1.

Niveles de Madurez con Atributos de medición

Nivel Madurez	**Atributos de Medición RISK IT**					
	Conocimiento y comunicación	**Responsabilidad y rendición de cuentas**	**Fijación y medición de objetivos**	**Políticas, normas y procedimientos**	**Conocimientos y experiencia**	**Herramientas y automatización**
	A1	A2	A3	A4	A5	A6
0- Proceso Incompleto	X					
1- Proceso Ejecutado	X	X				
2- Proceso Gestionado	X	X	X			
3- Proceso Establecido	X	X	X	X		
4- Proceso Predecible	X	X	X	X	X	
5- Proceso Optimizado	X	X	X	X	X	X

2.4 Métodos investigativos

Como diseño metodológico, este proyecto de titulación consideró un enfoque cualitativo, que según (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2010, pág. 9), señalan que este método se utiliza cuando “El investigador pregunta cuestiones abiertas, recaba datos expresados a través del lenguaje escrito, verbal y no verbal, así como visual, los cuales describe y analiza y los convierte en temas que vincula, y reconoce sus tendencias personales”.

La aplicación de este enfoque cualitativo, se hizo a través de entrevistas a los involucrados de las áreas de iniciativa estratégica de la Cooperativa de Ahorro y Crédito “Pedro Moncayo Ltda.”, especialmente los que intervienen en los Procesos Operativos, tales como: Jefe del área de Negocios, Jefe del área de Operaciones. Además del Gerente General, Jefe de Talento Humano y por supuesto, el Jefe y Asistente del Departamento de Tecnología de la Información y Comunicaciones.

Como complemento a la óptica cualitativa, también se utilizó el enfoque cuantitativo para interpretar y analizar la información recopilada, y así, poder identificar el grado de madurez y cuantificar los riesgos existentes de las actividades actuales del Departamento de “TIC”.

El método cuantitativo, según (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2010, pág. 13), indica que “Los datos se obtienen por observación, medición y documentación de mediciones. Se utilizan instrumentos que han demostrado ser válidos y confiables en estudios previos o se generan nuevos basados en la revisión de la literatura y se prueban y ajustan.”

Con estos resultados, se elaborará un plan de mejoras que ayudará a “TIC” alinearse con el Plan Estratégico de COAC “Pedro Moncayo Ltda.”, y también permitirá sustentar los objetivos planteados en este trabajo de investigación.

2.5 Metodologías de análisis de Riesgo

Para el análisis de riesgo existen varias metodologías las mismas que tienen bases científicas y que permitirán ejecutar los análisis de riesgo.

Dentro de esta sección se desarrollará las metodologías:

- OCTAVE
- CRAMM
- MARGERIT
- RISK IT

Al finalizar el estudio de las metodologías de análisis de riesgo se tendrá el conocimiento para: identificar, analizar y mitigar riesgos alienados a los objetivos estratégicos de la Cooperativa de Ahorro y Crédito Pedro Moncayo Ltda., y se podrá efectuar una comparación en base a sus ventajas y desventajas de aplicabilidad práctica de las metodologías.

2.5.1 OCTAVE

Desarrollada en EEUU por la Universidad Carnegie Mellón en el año 2011. Es una metodología que tiene un conjunto de herramientas, técnicas y métodos de evaluación basados en el riesgo de la seguridad de la información y planes de mitigación basado en los riesgos operacionales de seguridad de la organización.

OCTAVE tiene 3 metodologías:

- Metodología OCTAVE
- Metodología OCTAVE-S
- Metodología OCTAVE-Allegro

2.5.1.1 Metodología OCTAVE: Desarrolladas para empresas grandes.

Se aplica en 3 fases:

Fase I: Construcción de perfiles de amenazas basadas en activos.
Fase II: Identificación de vulnerabilidades en la infraestructura.
Fase III: Desarrollo de estrategias y planes de seguridad.

2.5.1.2 Metodología OCTAVE-S: Desarrolladas para pequeñas empresas

OCTAVE-S está dirigida por un equipo pequeño, interdisciplinario (de tres a cinco personas) de una de las organizaciones de personal que se reúnen y analizan la información, produciendo una estrategia de protección y planes de mitigación basado en los riesgos de seguridad organizaciones operativas únicas. Para llevar a cabo con eficacia OCTAVE-S, el equipo debe tener un amplio conocimiento del negocio de las organizaciones y los procesos de seguridad, por lo que será capaz de realizar todas las actividades por sí mismo (Miguel Angel Mendoza, 2015).

2.5.1.3 Metodología OCTAVE-Allegro

Es una técnica simplificada de la metodología OCTAVE, según (Caralli, Stevens, Young, & Wilson, 2007), permite agilizar y optimizar el proceso de evaluación de riesgos de seguridad de la información para que una organización puede obtener resultados satisfactorios con una pequeña inversión en tiempo, la gente, y otros recursos limitados.

Fase 1: Desarrollar criterios de medición de riesgo consistentes con la misión de la organización, los objetivos de la meta, y los factores críticos de éxito.

Fase 2: Crear un perfil de cada activo de información crítica que establece límites claros para el activo, identifica sus requisitos de seguridad, e identifica todos sus envases.

Fase 3: Identificar las amenazas a cada activo de información en el contexto de sus contenedores.
Fase 4: Identificar y analizar los riesgos para los activos de información y empezar a desarrollar enfoques de mitigación.

2.5.2 CRAMM - CCTA Risk Analysis and Management Method

Desarrollada por el Reino Unido en la década de 1980 por la Agencia Central de Cómputo y Telecomunicaciones (CCTA). Está basada en las mejores prácticas de la administración pública británica, es aplicable a grandes empresas públicas y privadas.

El modelo de análisis y gestión de riesgo puede resumirse en:

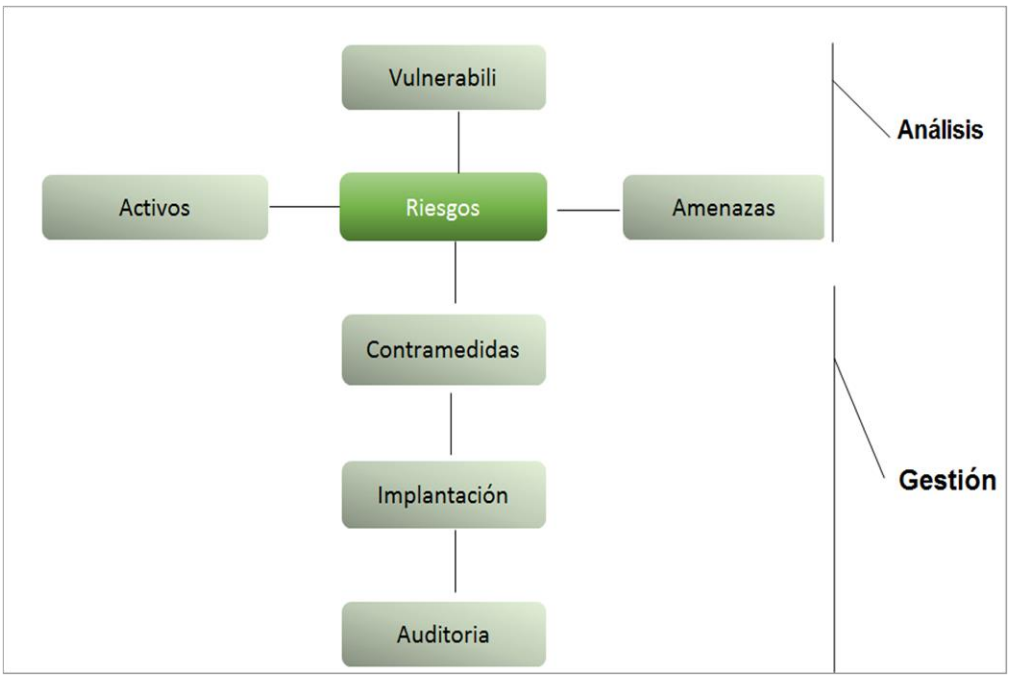


Figura 10. Modelo de análisis y gestión de riesgo de CRAMM
Adaptado de (Huerta, 2012)

CRAMM realiza tres tipos de análisis:

1. Análisis de Expertos de CRAMM
2. Análisis CRAMM expreso.

3. Análisis BS7799 (ISO 27001), (Internic, 2015)

La metodología CRAMM define 3 fases para el análisis de riesgo:

- Fase I: Establecimientos de Objetivos de Seguridad
- Fase II: Evaluación de riesgos
- Fase III: Identificación y selección de contramedidas

Los entregables de la metodología CRAMM son:

- Documentos de inicio de proyecto
- Informes de análisis de riesgo
- Informes de Gestión de riesgos
- Plan de implementación

El cálculo de riesgo se aplica a cada grupo de activos frente a las amenazas en una escala es de 1 a 7 donde 1 es la escala más baja y 7 indica un nivel muy alto requisito en la seguridad (SANS Institute, 2007).

2.5.3 MAGERIT

Es una metodología desarrollada en España por El Consejo Superior de Administración Electrónica por el año 1997, “que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados” (Gutierrez Amaya, s.f.). Cuanta con la aplicación, PILAR (Proceso Informático-Lógico para el análisis y gestión de riesgos.

2.5.3.1 Organización de los libros

La metodología está basada en 3 libros:

Libro I - Método: Está estructurado por 8 capítulos, en donde se “describe las tareas a realizar para acometer proyectos de análisis y gestión de riesgos aportando una guía para el desarrollo de análisis de riesgos, aspectos prácticos y consejos para facilitar la tarea” (Huerta, Introducción al análisis de riesgos – Metodologías, 2012).

- Capítulo I: Introducción
- Capítulo II: Visión de Conjunto
- Capítulo III: Método de análisis de riesgo
- Capítulo IV: Proceso de Gestión de riesgo
- Capítulo V: Proyecto de Análisis de Riesgo
- Capítulo VI: Plan de Seguridad
- Capítulo VII: Desarrollo de Sistema de Información
- Capítulo VIII: Consejos Prácticos

El libro se complementa con información de 5 apéndices (PAe, s.f).

Libro II - Catálogo de Elementos: El segundo libro, “recoge el catálogo de elementos implicados en el análisis de riesgos tales como: una categorización de activos, las dimensiones aplicables (DICAT), criterios para valoración de activos como procesos de negocio o datos, catálogo de amenazas y un catálogo de medidas a implantar para mitigar los riesgos a los que están expuestos los sistemas de información. Por último, indica cómo desarrollar un informe” (Huerta, Introducción al análisis de riesgos – Metodologías, 2012).

El libro está compuesto por los siguientes capítulos:

- Capítulo I: Introducción
- Capítulo II: Tipos de Activos
- Capítulo III: Dimensiones de valores
- Capítulo IV: Criterios de Valoración
- Capítulo V: Amenazas

- Capítulo VI: Salvaguardas
- Capítulo VII: Desarrollo de Sistema de Información
- Capítulo VIII: Consejos Prácticos

Adicionalmente contienen 4 apéndices (PAe, s.f)

Libro III - Guía de Técnicas, este libro según Huerta (2012) proporciona técnicas para el análisis de riesgos tales como: Algoritmos de análisis, árboles ataque, análisis coste-beneficio, diagramas de flujo, tablas de procesos o técnicas de trabajo. El uso de la herramienta asociada a esta metodología PILAR implementa muchas de estas soluciones técnicas

La Guía Técnica está compuesta por los siguientes capítulos:

- Capítulo I: Introducción.
- Capítulo II: Técnicas específicas.
- Capítulo III: Técnicas Generales, (PAe, s.f) .

2.5.3.2 Objetivos de Magerit

La metodología persigue los siguientes objetivos:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.

2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).

3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos:

4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

2.5.4 RISK IT, COBIT 5

RISK IT es un marco basado en un conjunto de principios y guías, procesos de negocio y directrices de gestión efectiva de riesgo TI (Marco de Riesgos de TI, 2009, pág. 7).

2.5.4.1 Estructura de RISK IT

RISK IT se compone de los dominios: Gobierno de riesgo, Evaluación de Riesgo Respuesta de riesgo

La siguiente figura presenta los dominios y procesos que definen el marco de gobierno.

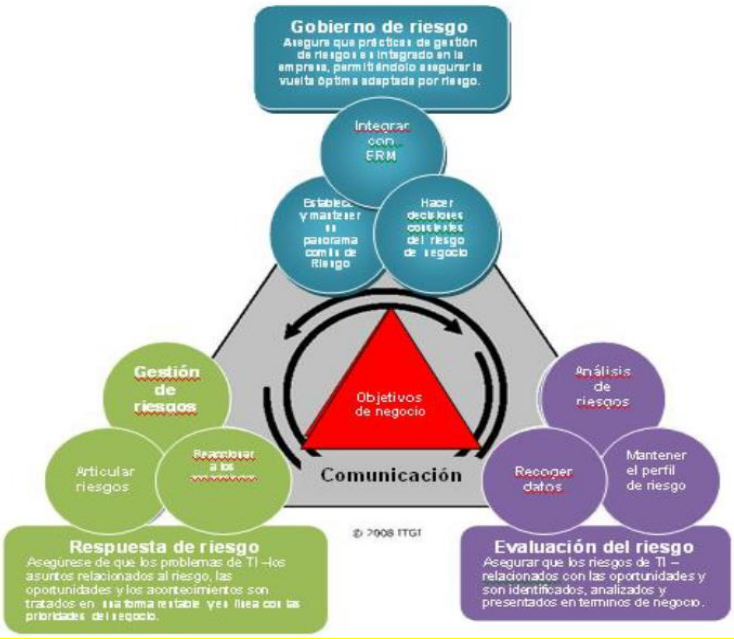


Figura 11. Marco de Referencia RISK
Tomado de (Marco de Riesgos de TI, 2009, pág. 15)

Según Risk IT los dominios de control son tres:

1. **Gobierno de riesgos (RG)**

Cubre componentes tales como:

- El apetito del riesgo y la tolerancia al riesgo.
- Responsabilidades y rendición sobre la gestión de riesgo de TI
- Sensibilización y Comunicación
- Cultura de riesgo. (ISACA , 2009, pág. 17).

Los procesos son tratados a mayor detalle con:

- RG1 Establecer y mantener una vista de riesgo común.
- RG2 Integrar con ERM.
- RG3 Tomar decisiones conscientes de los riesgos del negocio. (ISACA , 2009, pág. 9)

2. Evaluación de riesgos (RE)

Los componentes de dominio de evaluación son:

- Descripción del impacto de la organización
- Escenarios de Riesgo

Los procesos son tratados dentro de los siguientes componentes:

- RE1 Recopilar los datos.
- RE2 Analizar los riesgos.
- RE3 Mantener perfil de riesgo. (ISACA , 2009, pág. 9).

3. Respuesta de Riesgos (RR)

Los componentes esenciales de Respuesta de Riesgo son:

- Riesgo
- Definición de respuesta de riesgo y Priorización

A mayor detalle se puede describir en los siguientes procesos:

- RR1 Articular los Riesgo
- RR2 Manejar riesgos
- RR3 Reaccionar a acontecimientos. (ISACA , 2009, pág. 9)

2.5.4.2 Gestión de Riesgos (RG)

Asegurar que las actividades de gestión de riesgos se alinean con la capacidad objetiva de la empresa de TI relacionados con la pérdida de liderazgo y la tolerancia subjetiva de ella. (ISACA , 2009, pág. 46)

Gestión de Riesgos está basado en tres procesos:

RG1 Establecer y mantener una vista de riesgo común.

- RG1.1 Realizar una evaluación de riesgos de TI en toda la empresa
- RG1.2 Proponer los umbrales de tolerancia de riesgo de TI
- RG1.3 Aprobar la tolerancia al riesgo.
- RG1.4. Alinear la política de riesgos de TI.
- RG1.5 Promover la cultura consiente de los riesgos de TI.
- RG1.6 Promover una comunicación efectiva de los riesgos de TI, (ISACA , 2009, pág. 47)

RG2 Integrar con ERM.

- RG2.1 Establecer la rendición de cuentas de la gestión de los riesgos de TI en toda la empresa.
- RG2.2 Coordinar la estrategia de riesgos de TI y la estrategia de riesgo empresarial.
- RG2.3 Adaptar las prácticas de riesgos de TI a las prácticas de riesgo de la empresa.
- RG2.4 Proporcionar recursos adecuados para la gestión de riesgos.
- RG2.5 Garantizar el aseguramiento independiente sobre la gestión de riesgos. (ISACA , 2009, pág. 57)

RG3 Tomar decisiones conscientes de los riesgos del negocio.

- RG3.1 Obtener ganancia de la gestión de compra para el enfoque de análisis de riesgos.

- RG3.2 Aprobar los resultados del análisis de riesgo.
- RG3.3 Incorporar la consideración de los riesgos de TI en la toma de decisiones estratégicas de negocio.
- RG3.4 Aceptar el riesgo de TI.
- RG3.5 Priorizar actividades de respuesta a los riesgos de TI. (ISACA, 2009, pág. 57).

2.5.4.3 Gestión de Evaluación (RE)

Permite conocer a las empresas el impacto del negocio y los escenarios de riesgos a ser gestionados y por qué.

Los procesos de Gestión de evaluación de riegos tienen los siguientes procesos:

RE1 Recopilar datos.

- RE1.1 Establecer y mantener un modelo para la recolección de datos.
- RE1.2 Recopilar datos sobre el entorno externo.
- RE1.3 Recopilar datos sobre eventos de riesgo.
- RE1.4 Identificar factores de riesgo. (ISACA, 2009, pág. 66)

RE2 Analizar los riesgos.

- RE2.1 Definir Alcance del Análisis de Riesgos.
- RE2.2 Estimar los riesgos de TI.
- RE2.3 Identificar las opciones de respuesta de riesgo.
- RE2.4 Realizar una revisión de pares de los resultados de análisis de riesgos de TI. (ISACA, 2009, pág. 66)

La matriz de apoye para el levantamiento de roles y responsabilidades se basa en la Figura 12, la misma dependiendo de la necesidad de la institución puede ser adaptada.

Figura 20-Ejemplo de I cuadro RACI (RE2)

Cuadro RACI **Funciones**

Actividades principales

	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RE2.1. Definir el alcance de los riesgos de TI		I	R	C	I	C	A	R	C		C
RE2.2.Estimar riesgos de TI		I	R	C	C	I	A/R	R	R		C
RE.2.3 Identificar las opciones de respuesta de riesgo.			C	C	C	R	A	R	R		I
RE2.4 Realizar una revisión por pares de análisis de riesgos de TI.			A/R				I		I		I

A **RACI** chart identifies who is **R**esponsible, **A**ccountable,

Figura 12. Matriz RACI

Tomado de (ISACA , 2009, pág. 39)

RE3 Mantener el perfil de riesgo.

- RE3.1. Mapear los recursos de TI para procesos de negocio.
- RE3.2 Determinar la criticidad de negocio de los recursos de TI.
- RE3.3 Entender las capacidades de TI
- RE3.4 Actualizar los componentes de los escenarios de riesgos de TI.
- RE3.5 Mantener el registro de los riesgos de TI y el mapa de riesgos de TI.
- RE3.6 Diseñar y comunicar los indicadores de riesgo de TI. (Zuñiga & Mauricio, 2016)

2.5.4.4 Respuesta de los riesgos

El objetivo de definir una respuesta al riesgo es llevar el riesgo al mismo nivel que el apetito de riesgo definido para la empresa después del análisis de riesgo.

Los riesgos pueden ser manejados de acuerdo a:

- Evitar riesgos
- Reducción de Riesgos / Mitigación
- Riesgo Compartido / Transferencia
- Aceptación del Riesgo

RR2 Manejar los riesgos

- RR2.1 Controles del inventario.
- RR2.2 Supervisar la alineación operacional de los umbrales de tolerancia al riesgo.
- RR2.3Responder a la exposición al riesgo descubierto y la oportunidad.
- RR2.4 Implementar los controles.
- RR2.5 Informar el progreso del plan de acción de riesgos de TI. (Zuñiga & Mauricio, 2016)

RR3 Reaccionar a acontecimientos

- RR3.1 Mantener los planes de respuesta a incidentes.
- RR3.2 Supervisión de riesgos de TI
- RR3.3 Iniciar planes de respuesta a incidentes
- RR3.4 Comunicar las lecciones aprendidas de eventos de riesgo.

2.5.4.5 Evaluación de Riesgos

Una evaluación de riesgos basada en RISK IT utiliza los siguientes métodos:

- Criterios de información de COBIT
- Cuadro de mando integral – Balanced Scorecard

El método está basado en cubrir las perspectivas de: cliente, financiero, interno y de crecimiento para alcanzar los objetivos del Departamento “TI”.

Figura 13. Balanced Scorecard
Tomado de (WordPress, 2012)

Los criterios de información COBIT 5 que considera el BSC son:

- Eficiencia
- Eficacia
- Confidencialidad
- Integridad
- Disponibilidad
- Cumplimiento
- Confiabilidad

- Cuadro de mando integral extendida – Balanced Scorecard extendida
- Westerman
- COSO
- Análisis de Factores de Riesgo de la Información. (ISACA , 2009)

2.5.4.6 Escenarios de Riesgo TI

Los escenarios pueden derivarse de dos mecanismos

1. Un enfoque de arriba abajo, en el que se parte de los objetivos generales y se realiza un análisis de los escenarios de riesgos de TI más relevantes y probables que impacten los objetivos de negocio. Si los criterios de impacto están bien alineados con los controladores de valor real de la organización, los escenarios de riesgo relevantes se desarrollarán.

2. Un enfoque de abajo arriba, en el que se utiliza una lista de escenarios genérico para definir un conjunto de escenarios más concretos y personalizados, aplicados a la situación de la organización individua

2.5.4.7 Guía del Profesional

Según Guía Profesional (Risk-IT-Overview, 2009) se basa en:

- Revisión del modelo de procesos de Risk IT

- Risk IT to COBIT y Val IT

Cómo usarlo:

1. La definición de un universo de Gestión de Riesgos de Riesgos y de alcance
2. El apetito de riesgo y tolerancia al riesgo
3. Conciencia del riesgo, comunicación y presentación de informes
4. Expresar y describir Riesgo
5. Escenarios de riesgo
6. Respuesta a los Riesgos y Priorización
7. Un análisis de riesgos de flujo de trabajo
8. Mitigación de Riesgos de TI Uso de COBIT y Val IT

- Mapping: RISK IT a otros RISK IT Framework and standards
- Glosario, (ISACA, 2009).

2.6 Medición o Escalas

La asignación de escalas para identificar riesgos se apoyará en los métodos cualitativo y cuantitativo.

Considerará la información que se recolecte para categorizar problemas y riegos, el resultado de los mismos permitirá identificar los riesgos que impacten a las áreas de: Negocio, Operaciones y al departamento de “TIC” de la Cooperativa.

A continuación, se indica la forma de priorizar los riesgos y problemas:

Riesgos, se utilizó los criterios de información de COBIT:

- Eficiencia

- Eficacia
- Confidencialidad
- Integridad
- Disponibilidad
- Cumplimiento
- Confiabilidad

Problemas, se aplicará los siguientes criterios de medición.

Se considerará 3 mediciones: Alta, Media y Baja las mismas que están basados bajo los criterios de COBIT 5. La Tabla 2 detalla los criterios de medición.

Tabla 2.

Medición para priorización de problemas

Medición	Descripción
Alta	Afecta a la Cooperativa en: Eficacia, Eficiencia, Confidencialidad, Ingtegridad, Disponibilidad, Cumplimiento y Confiabilidad
Media	Afecta a procesos parciales a la operación normal de la cooperativa, se medirá en base a: Eficacia, Eficiencia, Disponibilidad, Cumplimiento y Confiabilidad
Baja	Todo está operativo sin impacto, se medirá en base a: Eficacia, Eficiencia, Cumplimiento y Confiabilidad

Para aplicar la calificación de riesgos se utilizará la Matriz de Riesgos o también llamada Matriz de Probabilidad del Impacto (MPI), la cual es una combinación de Medición y Priorización de Riesgos.

Tabla 3.

Matriz de puntaje de Probabilidades e Impacto

CÓD. RIESGO	RIESGO	PROBLEMA IDENTIFICADO	AMENAZA	VULNERABILIDAD	CONTROLES EXISTENTES IDENTIFICADOS	CRITICIDAD	PROBABILIDAD	IMPACTO
R1	Pérdida económica	P01. No existe documentación sobre la operación de las actividades de "TIC".	P01-A1- La actividad de monitoreo se lo lleva de manera empírica, es decir, no tiene están documentadas.	P01-V1. El conocimiento del flujo y la operativa de este proceso lo tiene el Jefe del área de Tecnología de la Información y Comunicaciones	1. Actividad se lo tienen de forma empírica	Alto	5,0	4,0

La Tabla 3 está basado en el Anexo 3, la información tiene la medición de pesos que se aplicara a los riesgos considerando el impacto y la probabilidad.

El impacto se mide de acuerdo a las escalas de medición indicados en la Tabla 4, en base al tiempo y costo, y al peso: bajo (1 - 2), medio (3 - 4) y alto (5),

Tabla 4.

Valores de Impacto

Impacto	Bajo (1 a 2)	Medio (3 y 4)	Alto (5)
Tiempo	Operación Continua	Afecta a la operación sin afectar al cliente	Afecta a la operación y a los clientes.
Costo	Puede ser controlado y administrado	Afecta a la disponibilidad de la aplicación	Implicaciones de costos monetarios con pérdidas económicas y reputación de imagen corporativa.

La probabilidad que se aplicará es subjetiva, dado que no existe información histórica de las actividades TI que ejecutan el Jefe y el Analista de Sistemas del Departamento de "TIC". A continuación, se describe en la Tabla 5.

Tabla 5.

Matriz de Probabilidades u Ocurrencias

Probabilidad	Estado	Peso	Descripción
Improbable	Bajo	1 a 2	No se presentaría en ningún escenario
Probable	Medio	2 a 4	Se daría bajo cierta condiciones y frecuencia

Frecuente	Alto	5	Se presentaría frecuentemente afectando a la operación y a los clientes

Una vez generada la Matriz de Mapeo de Riesgos, en base al impacto y a la probabilidad, se representará gráficamente los factores de riesgo, mediante un plano cartesiano con las siguientes condiciones:

- El eje de las X identificará la Probabilidad de Ocurrencia del factor de riesgo
- El Eje de las Y identificará el Impacto que este factor tiene sobre los objetivos estratégicos, actividades del departamento de "TIC" de COAC "Pedro Moncayo Ltda."

Lo citado, se representa en la figura 14:

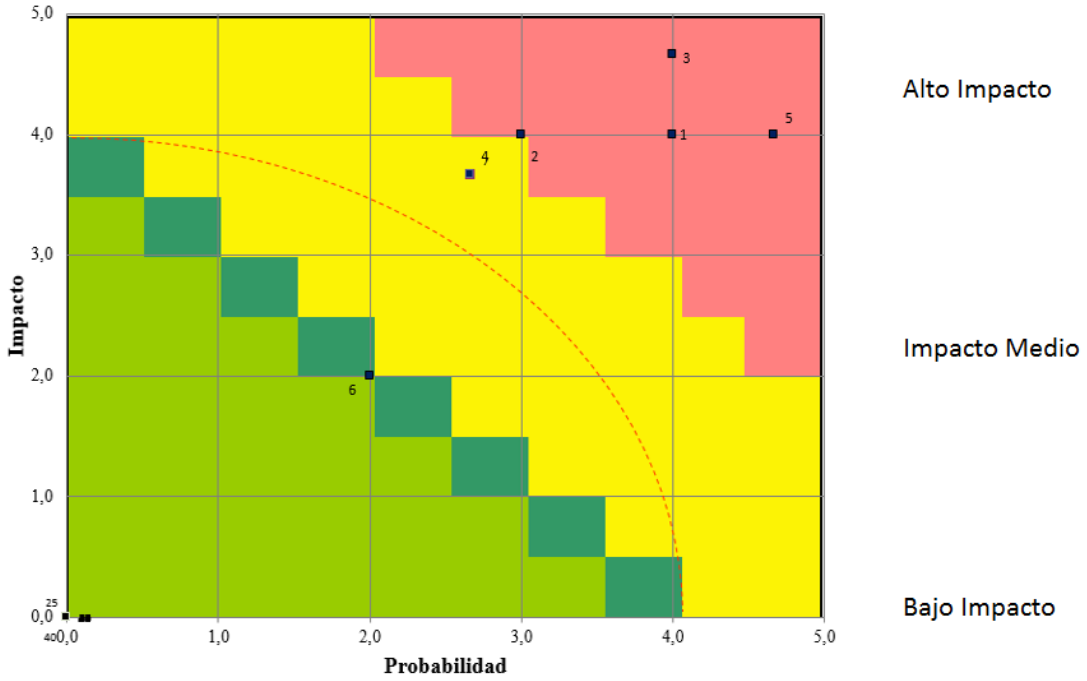


Figura 14. Plano Cartesiano de los Factores de Riesgos
Adaptado de (ISACA , 2009, pág. 17)

2.7 Tabla comparativa

Se realizará un cuadro comparativo de las metodologías desarrolladas en el capítulo 2.5 basándose en:

- Alcance la de la metodología, para cubrir el análisis y gestión de riesgo.
- Tipo de análisis: Medición tipo cualitativo y cuantitativo.
- Tipo de riesgo: Los tipos que se evalúan es: objetivo, financiero, no financiero, especulativo los mismos que se encuentran detallados en el capítulo 2 sección 2.2.2.
- Evaluación: Se considera las ventajas y desventajas de la metodología.

La medición que se aplica para los puntos 1, 2, 3 es:

- Aplicable, cubre todo el ámbito de evaluación
- No Aplicable, no cubre el ámbito de evaluación.
- Parcial, cubre parcialmente el ámbito de evaluación.
- No definido, no se conoce como se aplica el ámbito de evaluación.

Tabla 6.

Tabla Comparativa

Metodología	Alcance Considerado		Tipo de Análisis		Tipo de Riesgo				Evalaución	
	Análisis Riesgo	Gestión Riesgo	Cualitativo	Cuantitativo	Objetivos	Financieros	No Financieros	Especulativos	Desventaje	Ventajas
OCTAVE	Aplicable	Aplicable	Parcial	Parcial	Aplicable		No Aplica	No Aplica	- Se debe pagar costos de Licencia - La cooperativa no lo considera para medición de sus riesgos - Se limita a la seguridad de TI	-Identifica riesgo de seguridad que no permita cumplir con los objtivos estratégicos. - Determina riesgos de la seguridad de información. - Apoya a la empresa cumplir con la seguridad de la información. - Facilita la certificación ISO17999 - Ejecutan análisis y gestión de riesgos
CRAMM	Aplicable	Aplicable	Aplicable	Aplicable	Aplicable		No Aplica	No Aplica	- Se debe pagar costos de Licencia - La cooperativa no lo considera para medición de sus riesgos	- Facilita la certificación ISO17999 e sb 7799 - Ejecutan análisis y gestión de riesgos
MARGERIT	Aplicable	Aplicable	Aplicable	Aplicable	Aplicable		No Aplica	No Aplica	- Aplia a nivel local (solo se aplica España), no tiene certificado intenacional. - No se aplica a Empresas multinacionales - La cooperativa no lo considera para medición de sus riesgos	- Tiene herramienta para efectuar el análisis de riesgo PILAR, CHINCHON - Facilita la certificación ISO17999 - Ejecutan análisis y gestión de riesgos
RISK IT	Aplicable	Aplicable	Aplicable	Aplicable	Aplicable	Aplicable	Aplicable	Aplicable		- Ejecuta las mejores prácticas para identificar, gobernar y mitigar riesgos. - Se adapta a cualquier empresa. - Facilita la certificación ISO/IEC 27005, ISO 31000, ISO 73 'Tiene herramientas: Guia Práctica del Profesional Mapa de Riesgos (Nivele de ejeución) - Apoya a cumplir los objetivos estratégicos de la organización - Es requisito de la cooperativa

En base a la Tabla 5 se considera la metodología Risk IT para la evaluación de riesgos en el Departamento “TI” de la Cooperativa de Ahorro y Crédito Pedro Moncayo Ltda., los ítems evaluados para la aplicación de la metodología son:

- Requerimiento de la cooperativa
- Aplicabilidad en cualquier tipo de empresa: pequeña, mediana, grande
- Permite alcanzar y alinease a los objetivos estratégicos de empresa.

2.8 Justificación de la metodología aplicada

La Cooperativa de Ahorro y Crédito “Pedro Moncayo Ltda.”, para alcanzar sus objetivos estratégicos planteados hasta el año 2017 y cumplir con su visión, especialmente el “Ser una Institución financiera del sector de la economía popular y solidaria, sólida y en permanente crecimiento…” (02 Plan estratégico PM 2015 2017, 2016, pág. 8), ha visto la necesidad de realizar un estudio de la situación actual del Departamento de Tecnología de la Información y Comunicaciones, que le permita identificar los riesgos inminentes y el grado de madurez de las actividades de esta área y en sí de la Cooperativa en general.

Para apoyar este estudio investigativo y en base a los fundamentos teóricos planteados en este capítulo, se ha seleccionado el Marco de Riesgos de TI, “RISK IT” de COBIT 5, debido a que:

- El uso del marco de referencia COBIT 5, es un requerimiento de la Cooperativa dentro de este trabajo de investigación, dado su objetivo primordial que es el obtener “productos y servicios de excelencia” (02 Plan estratégico PM 2015 2017, 2016, pág. 8), que permitan alcanzar los resultados planteados del negocio y del mercado, mediante la optimización de los riesgos identificados y a través de los recursos tecnológicos.

- El marco de riesgos de TI está destinado a un público amplio, ya que la gestión de riesgo es una práctica global y un requisito estratégico en toda organización, que por supuesto, ayudará a implementar el gobierno de TI con eficiencia y efectividad y mejorar los procesos internos y externos del negocio.

- La metodología de riesgos de TI permite tener una orientación de principio a fin sobre la forma de tomar decisiones sobre los riesgos inminentes de manera integrada, mediante la gestión de riesgos empresariales (ERM), aprovechando las buenas prácticas que proveen los marcos de referencia COBIT 5, VAL IT, RISK IT.

La aplicación de mejores prácticas para la gestión de riesgo de TI proporcionará beneficios tangibles de negocio, por ejemplo: menor número de eventos esperados y fracasos, el aumento en la calidad de información, una mayor confianza de las partes interesadas

2.9 Cronograma de Proyecto

En esta sección se detalla el cronograma de trabajo del proyecto de titulación.

Nombre de tarea	Comienzo	Fin	Nombres de los recursos	Duración
Pry_COAC "Pedro Moncayo Ltda."	**vie 23/9/16**	**vie 16/12/16**		**61 días**
Inicio	**vie 23/9/16**	**vie 23/9/16**		**1 día**
Ejecución	**lun 26/9/16**	**vie 9/12/16**		**55 días**
Capítulo I – INTRODUCCIÓN	**lun 26/9/16**	**mar 27/9/16**		**2 días**
Entrega Capítulo	mar 27/9/16	mar 27/9/16	Profesor; Erika Mora; Fany Cacuango	0 días
Capítulo II - MARCO TEÓRICO	**mié 28/9/16**	**mar 4/10/16**		**5 días**
Entrega Capítulo	mar 4/10/16	mar 4/10/16	Profesor; Erika Mora;Fany Cacuango	0 días
Capítulo III - ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA COOPERATIVA	**mié 5/10/16**	**vie 21/10/16**		**13 días**
Entrega Capítulo	vie 21/10/16	vie 21/10/16	Erika Mora; Fany Cacuango; Profesor	0 días
Capítulo IV - EVALUACIÓN DE RIESGOS	**lun 24/10/16**	**vie 25/11/16**		**25 días**

Entrega Capítulo	vie 25/11/16	vie 25/11/16	Erika Mora; Fany Cacuango; Profesor	0 días
Capítulo V - PLAN DE MEJORA	**lun 28/11/16**	**vie 2/12/16**		**5 días**
Entrega Capítulo	vie 2/12/16	vie 2/12/16	Erika Mora; Fany Cacuango; Profesor	0 días
Capítulo VI - CONCLUSIONES Y RECOMENDACIONES	**lun 5/12/16**	**vie 9/12/16**		**5 días**
Entrega Capítulo	vie 9/12/16	vie 9/12/16	Erika Mora; Fany Cacuango; Profesor	0 días
Entrega Borrador Trabajo de Titulación	vie 9/12/16	vie 9/12/16	Erika Mora; Fany Cacuango; Profesor	0 días
Cierre	**lun 12/12/16**	**vie 16/12/16**		**5 días**
Entrega Trabajo de Titulación	vie 16/12/16	vie 16/12/16	Erika Mora; Fany Cacuango; Profesor	0 días

3 Capítulo III. Análisis de la situación actual de COAC y del Departamento de "TIC"

En este capítulo se analizará la situación actual de la Cooperativa y del Departamento de "TIC", utilizando como parte de la metodología RISK IT, el "ámbito gobernanza del riesgo - RG", (ISACA , 2009, pág. 9), Además, se identificará el grado de madurez de las actividades que mantiene como parte de su trabajo este departamento.

3.1 Gobierno de COAC "Pedro Moncayo Ltda."

En base a lo expuesto en el capítulo II, sección 2.5.4.4, sobre los ámbitos o dominios de riesgos, específicamente sobre los de gobierno de riesgos, "RG", la Cooperativa de Ahorro y Crédito "Pedro Moncayo Ltda.", ha realizado su Plan Estratégico 2015 – 2017, creado en base al "Cuadro de Mando Integral del Balance Scorecard de Kaplan y Norton" en donde se encuentran identificadas las áreas de iniciativa estratégicas, sus objetivos estratégicos y sus estrategias, que a continuación se detallan de acuerdo al (02 Plan estratégico PM 2015 2017, 2016):

Perspectiva: Resultados financieros y sociales

Objetivo 1. Implementar un modelo de gestión del Balance Social.

1. Definir el modelo para la gestión del Balance Social.
2. Implementar el modelo para la gestión del Balance Social. (pág. 14)

Objetivo 2. Mejorar el desempeño financiero de la Cooperativa.

1. Mejorar el modelo de evaluación de los indicadores financieros.
2. Mejorar el modelo de evaluación de la ejecución presupuestaria. (pág. 14)

Perspectiva: Clientes

Objetivo 3. Mejorar el nivel de satisfacción de socios y clientes.

1. Desarrollar e implementar un modelo para medir y gestionar la satisfacción integral de socios y clientes. (pág. 14)

Objetivo 4. Incrementar los resultados de negocios y de mercado.

1. Ampliar la cobertura de mercado.
2. Desarrollar nuevos productos y servicios.
3. Fortalecer la gestión comercial y de mercado.
4. Realizar la búsqueda y consecución de fuentes externas de fondeo. (pág. 14)

Perspectiva: Procesos

Objetivo 5: Lograr el cumplimiento de los proyectos de fortalecimiento organizacional.

1. Fortalecer competencias de los miembros del Gobierno Corporativo.
2. Definir y aplicar las mejores prácticas de Buen Gobierno Corporativo.
3. Actualizar e implementar la estructura orgánica de la Cooperativa.
4. Actualizar e implementar el Manual Orgánico Funcional.
5. Actualizar e implementar el Manual de Funciones por Cargo.
6. Definir e implementar un modelo de mejoramiento de procesos y mejorar los procesos críticos de la Cooperativa.
7. Actualizar la normativa interna en general.
8. Mejorar la infraestructura física de la Matriz y Agencias.
9. Fortalecer el sistema de comunicación institucional. (pág. 15)

Perspectiva: Aprendizaje y desarrollo

Objetivo 6: Mejorar el desempeño del talento humano.

1. Mejorar los subsistemas de Administración de Talento Humano por Competencias.
2. Mejorar el clima laboral. (pág. 15)

Objetivo 7: Fortalecer la gestión de Tecnología de la Información y Comunicaciones.

1. Diseñar e implementar un esquema de medición de satisfacción de usuarios internos de TIC.
2. Implementar los recursos claves para la gestión de TIC.
3. Definir e implementar un modelo de gestión de TIC basado en buenas prácticas.
4. Adecuar la infraestructura del Centro de Cómputo. (pág. 15)

Dentro de este Plan Estratégico incluye todo lo referente a establecer y mantener una visión de los riesgos, “RG1”, integrarlos dentro de la estructura organizativa de la cooperativa, “RG2” y plantear los objetivos estratégicos basados en los riesgos inminentes del negocio, “RG3”.

3.1.1 Mapa de Procesos de COAC “Pedro Moncayo Ltda.”

La Cooperativa cuenta con los siguientes procesos establecidos dentro del Mapa General de Procesos:

Procesos Gobernantes

- Planificación institucional
- Gestión organizacional
- Administración integral de riesgos

Estos procesos están bajo responsabilidad de los Consejos de Vigilancia y de Administración, Gerencia General, Comités de Administración Integral de Riesgos, de Adquisiciones, de Cumplimiento, de Seguridad e Higiene en el Trabajo, de Crédito y la Comisión de Educación.

Procesos de Apoyo

- Gestión de producto y mercado
- Administración general
- Comercialización de productos y servicios
- Gestión de atención y servicio al cliente
- Gestión operativa de riesgos
- Gestión de evaluación y control
- Gestión de operaciones
- Gestión del talento humano
- Administración financiera y contable
- Gestión de tecnología de información

Las áreas involucradas en estos procesos son:

- Operaciones
- Contabilidad
- Riesgos
- Asesoría Jurídica
- Planificación y Procesos
- Marketing
- Tesorería
- Talento Humano
- Tecnología de Información y Comunicaciones

Procesos Operativos

- Gestión de captaciones, es el proceso operativo utilizado por el Departamento de Captaciones y Servicios, en donde ofrecen productos como inversiones y cuentas de ahorro. Para captar clientes se ofrecen estos

productos dentro y fuera de la Cooperativa; en otras palabras, los Ejecutivos de Captaciones van a ofrecer y vender los productos directamente a potenciales clientes o socios.

- Gestión de colocaciones de créditos, este proceso consiste en crear y ofrecer créditos, en base a las necesidades de los socios, después de realizar un estudio de mercado del negocio.

- Gestión de servicios complementarios, dentro de este proceso se establece convenios con otras instituciones financieras o empresas de servicios que permitan a los socios de la Cooperativa realizar pagos de impuestos o servicios básicos.

Estos procesos se encuentran en el área de Negocios, específicamente en los departamentos de Captaciones y Servicios, Crédito y Agencias.

A continuación, se presenta el gráfico del Mapa de Procesos:

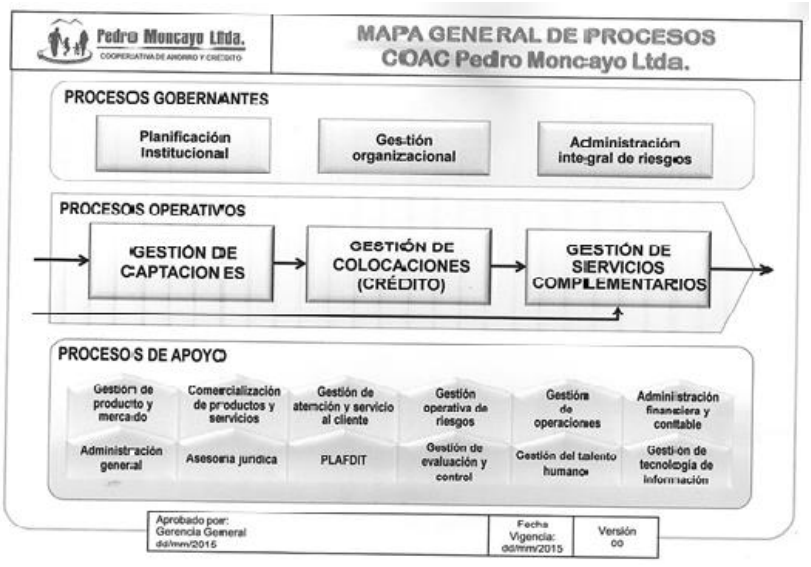


Figura 15. Mapa de Procesos de COAC "Pedro Moncayo Ltda."
Tomado de *(02 Plan estratégico PM 2015 2017, 2016)*

3.1.2 Portafolio de Productos y Servicios

El Portafolio de Servicios de COAC “Pedro Moncayo Ltda.”, correspondientes a los Procesos Operativos: Gestión de captaciones, Gestión de colocaciones de créditos y Gestión de servicios complementarios son los siguientes:

Tabla 7.

Productos y Servicios COAC "Pedro Moncayo Ltda."

Productos		**Descripción**
1. Inversiones	1.1. Inversiones a Plazo Fijo	Inversiones a través de pólizas a plazo fijo desde 30 días con un monto mínimo de $500,00 dólares americanos.
2. Créditos	2.1. Crédito Inmediato	Crédito de entrega inmediata de un monto máximo de $1.000,00 dólares americanos a 12 meses y con cuotas fijas.
	2.2. Crédito Productivo	Crédito dirigido a socios que son agricultores y ganaderos. El pago se ajusta al periodo productivo con cuotas trimestrales, semestrales entre otros.
	2.3. Crédito Educativo	Crédito para cubrir gastos educativos existentes al inicio de clases.
	2.4. Microcrédito	Crédito orientado a clientes que no tuvieron oportunidad de préstamos en la banca tradicional y que son dueños de pequeños y medianos negocios.
	2.5. Crédito Excelente	Crédito dirigido a socios con un excelente record crediticio dentro de la Cooperativa. El monto a prestar es de hasta $5.000,00 dólares americanos.
	2.6. Créditos de Consumo	Créditos otorgados a personas que tienen dependencia laboral para financiar la adquisición de bienes de consumo, pago de servicios, pago de deudas, adquisición de muebles, viajes, gastos familiares, enfermedades, etc.
	2.7. Crédito Hipotecario	Crédito a corto plazo, destinado a personas que quieran obtener casa, departamento nuevo a usado, compra de terreno.
3. Cuentas de Ahorro	3.1. Ahorro Infantil	Cuenta de ahorro creada para los hijos de los socios. El valor mínimo para aperturar es de $15,00 dólares americanos.
	3.2. Cuenta Cosecha	Cuenta de ahorro creada para los socios, que les permite tener beneficios de créditos. El valor mínimo para aperturar es de $40,00 dólares americanos.
Servicios		**Descripción**
1. Servicios Complementarios	1.1. Transferencias Interbancarias	Servicio para realizar transferencias interbancarias con cualquier institución financiera
	1.2. Pagos de Impuestos y Servicios Básicos	Servicio para pago de impuestos SRI, RISE, matrícula vehicular, pensiones alimenticias, bono solidario. Pago de servicios básicos como: luz, agua y teléfono.
	1.3. Pagos a terceros	Servicio para pago de televisión por cable, Yanbal, Avon, L'bel, Esika, operadoras telefónicas: Claro y Movistar, entre otros
2. Servicios Virtuales	2.1. Crédito Hipotecario	Crédito a corto plazo, destinado a personas que quieran obtener casa, departamento nuevo a usado, compra de terreno. Este crédito puede solicitar a través de la plataforma virtual.

	2.2. Cuenta Ahorro Cosecha	Cuenta de ahorro creada para los socios, que les permite tener beneficios de créditos. El valor mínimo de esta cuenta es de $40,00 dólares americanos. Esta cuenta puede ser creada a través de la plataforma virtual.
	2.3. Cuenta Ahorro Crecer	Cuenta de ahorro creada para los hijos de los socios. El valor mínimo de depósito para este tipo de cunetas es de $15,00 dólares americanos. Cuenta de ahorros apertura, mediante la plataforma virtual de la Cooperativa.

Las áreas responsables de los procesos operativos se apoyan y soportan en el Departamento de Tecnología de la Información y Comunicaciones, en base al listado de sus procesos de servicios informáticos.

3.2 Recolección de Información

Para la identificación de los riesgos con criticidad “alta” en el Departamento de “TIC”, se recolectó información a través de documentos, entrevistas personales, revisión de procesos en situ. Esto permitió determinar los factores de riesgo y controles actuales en los procesos de negocio, operaciones y tecnología de la Cooperativa “Pedro Moncayo Ltda.”

Las fuentes utilizadas para este relevamiento de información fueron:

- Documentos internos: Plan Estratégico, procedimientos del Departamento de “TIC”, Mapa de Procesos.
- Lista de productos y servicios.
- Entrevistas personales con los jefes de los departamentos que conforman el Proceso Operativo del Negocio.
- Levantamiento de actividades del departamento de “TIC” a nivel de:
  - Software de: sistemas, aplicaciones, plataformas;
  - Hardware: servidores, computadores personales;
  - Comunicaciones: ruteadores, switches, enlaces.

En cuanto a las entrevistas, las mismas se realizaron a los responsables de las áreas estratégicas para la Cooperativa: Operaciones y Negocio, y por supuesto al Departamento de Tecnología de la Información y Comunicaciones.

La Tabla 8 indica las áreas de la Cooperativa en donde se realizaron las entrevistas, a través de preguntas sobre las actividades actuales del departamento de “TIC”.

Tabla 8.

Cuadro Resumen de Entrevistas - Cooperativa “Pedro Moncayo Ltda.”

Cód. Entrevista	Actividades actuales del Departamento "TIC"	Departamentos Entrevistados de la Cooperativa			
		Tecnología	Operaciones	Negocio	Talento Humano
Ent. 01	Actividad 46 - Configuración y asignación de IP de red a nuevos usuarios	X			
Ent. 02	Actividad 47 - Configurar una nueva cámara de seguridad	X			
Ent. 03	Actividad 48 - Configuración de aplicativos de control de asistencia	X			
Ent. 04	Actividad 49 - Configuración de Pin Pad	X	X	X	
Ent. 05	Actividad 50 - Configuración de cuenta de correo electrónico a nuevo usuario	X			
Ent. 06	Actividad 03 - Mantenimiento Físico de cajeros automáticos	X	X	X	X
Ent. 07	Actividad 14 a 19 - Creación de usuarios a las aplicaciones de la Cooperativa	X	X	X	X
Ent. 08	Actividad 21 al 26 - Instalación de aplicaciones	X	X	X	X
Ent. 09	Actividad 28 al 32 - Creación de Usuarios y Reseteo de Claves	X		X	
Ent. 10	Actividad 21 al 26 - Instalación de aplicaciones	X			
Ent. 11	Actividad 51 y 53 - Respaldo de Base de Datos y Recuperación de BDD	X			

3.3 Inventario de actividades del Departamento de “TIC”

Dentro del Departamento de Tecnología de la Información y Comunicaciones se identificaron 11 actividades con 65 tareas tecnológicas, las mismas que se indican en la Tabla 9 - Listado Actual de Actividades de “TIC”

Esta tabla se encuentra dividida en 2 secciones principales con la siguiente información:

1. Actividades actuales de TI, en donde se encuentran las siguientes columnas:
   Cód. Actividad, que corresponde a un código identificador de la actividad tecnológica. La nomenclatura utilizada es: AATxx
   AAT, significa Actividad Actual Tecnológica
   xx, es un número secuencial de 2 dígitos

   Actividad, en donde se especifica el nombre de la actividad tecnológica.

   Cód. Tarea, para identificar cada una de las tareas que se ejecutan en cada actividad tecnológica. La nomenclatura utilizada es: AATxx.yy
   AAT, significa Actividad Actual Tecnológica
   xx, es un número secuencial para cada actividad tecnológica
   yy, es un número secuencial para cada tarea de la actividad.

2. Componentes, en donde se incluye información técnica requerida para la operación de las actividades tecnológicas y funcionamiento normal de la Cooperativa. Dentro de los componentes tecnológicos se identificaron los siguientes:

   Estaciones de trabajo, verificando:
   - Hardware, a nivel del modelo del procesador
   - Software, a nivel del sistema operativo

   Servidores, revisando:
   - Hardware, a nivel del modelo del procesador

- Software, a nivel del sistema operativo

Base de Datos, a nivel de motor de base de datos

Aplicaciones, en donde se validó los programas, aplicaciones, sistemas o plataformas utilizadas por la Cooperativa para los procesos del negocio.

Comunicaciones, entre los dispositivos de comunicación revisados están:

- Ruteadores,
- Switches
- Enlaces

Storage, requeridos para mantener respaldos de la información considerada como crítica para el negocio.

Cabe indicar que no todos los componentes tecnológicos son requeridos para la ejecución de las actividades TI, por lo que en la Tabla 8, pueden existir campos en blanco.

Tabla 9.

Listado Actual de Actividades de "TIC"

Actividades Actuales de TI				Componentes (1 de 7)										
				Estación de trabajo		Servidores		BDD	Aplicaciones	Comunicaciones			Storage
Cód. Actividad	Actividad	Cód. Tarea	Tarea	HW	SW	HW	SW			Ruteador	Switch	Enlace	
AAT01	MONITOREO	AAT01.1	Monitoreo de Consola de Antivirus			HD 61E Intel D	Windows Server 2008		Kaspersky Security Center 10	CISCO	DLINK	LAN	
		AAT01.2	Seguimiento y monitoreo de red							CISCO	DLINK	LAN / WAN	
		AAT01.3	Control filtrado de contenido de internet			Focus UTM			Filtrado Web	CISCO	DLINK	CNT	
		AAT01.4	Monitoreo de recursos físicos de ATM	NCR	Windows 7				Aptra	CISCO	DLINK	CONECTA	
AA T02	MANTENIMIENTO	AAT02.1	Mantenimiento preventivo de base de datos			HP Server 350	Windows Server 2012	SQL Server 2012	Financial - Core Financiero	CISCO	DLINK	LAN	HP - Disco DIMS 64
		AAT02.2	Mantenimiento preventivo de equipos de computación	Core Duo 3	Windows 7					CISCO	DLINK	LAN	
		AAT02.3	Mantenimiento del intranet institucional			HP Server 350	Windows Server 2012		Intranet Institucional	CISCO	DLINK	LAN	

Actividades Actuales de TI				Componentes (2 de 7)									
				Estación de trabajo		Servidores		BDD	Aplicaciones	Comunicaciones			Storage
Cód. Actividad	Actividad	Cód. Tarea	Tarea	HW	SW	HW	SW			Ruteador	Switch	Enlace	
AAT03	SOPORTE A USUARIOS	AAT03.1	Soporte a usuarios del CORE financiero						Financial - Core Financiero				
		AAT03.2	Soporte a usuarios servicio facilito						Facilito				
		AAT03.3	Soporte a usuarios servicio entura						Entura				
		AAT03.4	Soporte a usuarios servicio extreme						Extreme				
		AAT03.5	Soporte a usuarios consola de red						Controlador de Dominio - Directorio Activo				
		AAT03.6	Soporte a usuarios por hardware	Core Duo 3	Windows 7								
AAT04	INSTALACIÓN A USUARIOS	AAT04.1	Instalación del CORE financiero						Financial - Core Financiero				
		AAT04.2	Instalación del servicio facilito						Facilito				
		AAT04.3	Instalación del servicio entura						Entura				
		AAT04.4	Instalación del servicio extreme						Extreme				
		AAT04.5	Instalación del antivirus						Kaspersky Security Center 10				
		AAT04.6	Instalación del Intranet						Intranet Institucional				

		AAT04.7	Instalación de PINPAD						PINPAD					

Actividades Actuales de TI				Componentes (3 de 7)									
				Estación de trabajo		Servidores		BDD	Aplicaciones	Comunicaciones			Storage
Cód. Actividad	Actividad	Cód. Tarea	Tarea	HW	SW	HW	SW			Ruteador	Switch	Enlace	
AAT05	CREACIÓN USUARIOS	AAT05.1	Creación de nuevos usuarios del CORE financiero						Financial - Core Financiero				
		AAT05.2	Creación nuevos usuarios servicio facilito						Facilito				
		AAT05.3	Creación nuevos usuarios servicio entura						Entura				
		AAT05.4	Creación nuevos usuarios servicio extreme						Extreme				
		AAT05.5	Creación de nuevos usuarios de correo electrónico		Outlook	Hosting externo	Exchange		Set Pannel – Consola			Nube	
		AAT05.6	Creación de nuevo usuario de intranet						Intranet Institucional				
		AAT05.7	Creación de nuevo usuario para control de asistencia						Control de Asistencia				
		AAT05.8	Creación nuevos usuarios consola de red						Dominio - Directorio Activo				
AAT06	RESETEO DE CLAVES	AAT06.1	Reseteo de claves del CORE financiero						Financial - Core Financiero				
		AAT06.2	Reseteo de claves servicio facilito						Facilito				
		AAT06.3	Reseteo de claves servicio entura						Entura				
		AAT06.4	Reseteo de claves servicio extreme						Extreme				

		AAT06.5	Reseteo de claves consola de red						Dominio - Directorio Activo					

Actividades Actuales de TI				Componentes (4 de 7)									
				Estación de trabajo		Servidores		BDD	Aplicaciones	Comunicaciones			Storage
Cód. Actividad	Actividad	Cód. Tarea	Tarea	HW	SW	HW	SW			Ruteador	Switch	Enlace	
AAT07	INACTIVACIÓN DE USUARIO	AAT07.1	Inhabilitar usuario del CORE financiero						Financial - Core Financiero				
		AAT07.2	Inhabilitar usuario servicio facilito						Facilito				
		AAT07.3	Inhabilitar usuario servicio entura						Entura				
		AAT07.4	Inhabilitar usuario servicio extreme						Extreme				
		AAT07.5	Inhabilitar usuario consola de red						Directorio Activo				
AAT08	CONFIGURACIÓN	AAT08.1	Configuración y asignación de ip de red a nuevos usuarios							CISCO	DLINK	LAN / WAN	
		AAT08.02	Configuración de aplicativos de control de asistencia						Control de Asistencia				
		AAT08.03	Configuración de PIN PAD						PINPAD				
		AAT08.04	Configuración de estaciones de trabajo	Core Duo 3	Windows 7				Ofimática				
		AAT08.05	Configuración de seguridad para perfilamiento por cargo	Core Duo 3	Windows 7								
		AAT08.06	Configuración de un nuevo punto de red										

		AAT08.07	Configuración de cuenta de correo electrónico		Outlook		Exchange						

Actividades Actuales de TI				Componentes (5 de 7)									
				Estación de trabajo		Servidores		BDD	Aplicaciones	Comunicaciones			Storage
Cód. Actividad	Servicio	Cód. Tarea	Tarea	HW	SW	HW	SW			Ruteador	Switch	Enlace	
AAT09	SOPORTE APLICACIÓN / INFRAESTRUCTURA	AAT09.1	Cierre de Fin de Día						Financial - Core Financiero				
		AAT09.2	Acreditación mensual de intereses						Financial - Core Financiero				
		AAT09.3	Respaldo de base de datos del Core financiero					SQL Server 2012	Financial - Core Financiero				HP - Disco DIMS 64
		AAT09.4	Generación de back up de pc	Core Duo 3	Windows 7								HP - Disco DIMS 64
		AAT09.5	Baja información cámaras de seguridad						Control de Asistencias				HP - Disco DIMS 64
		AAT09.6	Baja información de control de asistencia										
		AAT09.7	Actualizaciones de parches		Windows 7		Windows 2012, Windows 2008	SQL 2012	Kaspersky				

Actividades Actuales de TI				Componentes (6 de 7)									
				Estación de trabajo		Servidores		BDD	Aplicaciones	Comunicaciones			Storage
Cód. Actividad	Servicio	Cód. Tarea	Tarea	HW	SW	HW	SW			Ruteador	Switch	Enlace	
AAT10	PROVEEDOR	AAT10.1	Instalación de nueva cámara de seguridad						Cámara de Seguridad				
		AAT10.2	Configuración de nueva cámara de seguridad						Cámara de Seguridad				
		AAT10.3	Mantenimiento preventivo de cámaras de seguridad						Cámara de Seguridad				
		AAT10.4	Mantenimiento de la página web institucional						Portal COAC				
		AAT10.5	Mantenimiento preventivo de software						Portal COAC				
		AAT10.6	Mantenimiento preventivo de cajero automático	NCR	Windows 7				Aptra				
		AAT10.7	Monitoreo consola de grabación cámaras de seguridad						Cámara de Seguridad				
		AAT10.8	Configuración de Cortafuego, filtrado web, control de aplicaciones y correo electrónico interno				Sophos UTM					CONECTA	

Actividades Actuales de TI				Componentes (7 de 7)									
				Estación de trabajo		Servidores		BDD	Aplicaciones	Comunicaciones			Storage
Cód. Actividad	Actividad	Cód. Tarea	Tarea	HW	SW	HW	SW			Ruteador	Switch	Enlace	
AAT11	REQUERIMIENTOS	AAT11.1	Nueva publicación en la página web institucional						Portal COAC				
		AAT11.2	Nuevo requerimiento del Core financiero						Financial - Core Financiero				
		AAT11.3	Generación de reportes nuevos desde la base de datos del Core financiero						Financial - Core Financiero				
		AAT11.4	Implementación de reportes nuevos en el módulo de reportes						Financial - Core Financiero				
		AAT11.5	Solicitud de video de las cámaras de seguridad						Cámara de Seguridad				

3.4 Roles y Responsabilidades

Como parte de la metodología explicada en el capítulo II, sección 2.5.4.5, a continuación, se señalan los roles y responsabilidades identificados en las actividades tecnológicos del Departamento de “TIC” y en los procesos existentes en la Cooperativa:

1. Como Consultados e Informados, se tiene a:

Dueño del proceso, son todos los funcionarios de la Cooperativa que necesita de algún servicio de tecnología y que pueden solicitar requerimientos.

Gerente de COAC “Pedro Moncayo Ltda.”, actualmente en este cargo se encuentra el Eco. Juan Carlos Mármol, es el responsable de tomar decisiones y autorizar los requerimientos en base a los objetivos estratégicos de la Cooperativa.

2. Como Aprobador y Responsable, se encuentran:

Jefe de Sistemas, actualmente ocupa este cargo el Ingeniero Christian Maldonado, quien es responsable de autorizar y tomar las decisiones en este departamento. Además, realiza actividades operativas y de gestión en base a los requerimientos del negocio.

Asistente de Sistemas, este cargo lo ejerce el Ingeniero Juan Carlos Prado, es el responsable de ejecutar las actividades y tareas operativas diarias en la Cooperativa.

En la Tabla 10, se presenta la matriz RACI correspondiente al Departamento de “TIC”, en donde se incluyen las 11 actividades tecnológicas Con los responsables de los procesos existentes de la Cooperativa.

Tabla 10.

RE2 - RACI - Roles y Recursos

ACTIVIDADES ACTUALES DE TIC	ROLES PROCESOS				CARGO	ÁREA	ROLES ACTIVIDADES	SERVICIO NEGOCIO / TI
	Dueño del Proceso Operativo COAC	Gerente de COAC	Jefe de Sistemas	Asistente de Sistemas				
Configuración		C / I	A / R	R	Jefe de Sistemas	TIC	Gestor de Configuración	Procesos Operativos
					Asistente de Sistemas	TIC	Gestor de Configuración	TIC
Creación usuarios	C / I		A / R	R	Jefe de Sistemas	TIC	Gestor de Accesos	Procesos Operativos
					Asistente de Sistemas	TIC	Gestor de Accesos	TIC
Inhabilitación usuario	C / I		A / R	R	Jefe de Sistemas	TIC	Gestor de Accesos	Procesos Operativos
					Asistente de Sistemas	TIC	Gestor de Accesos	TIC
Instalación a usuarios	C / I		A / R	R	Jefe de Sistemas	TIC	Gestor de Accesos	Procesos Operativos
					Asistente de Sistemas	TIC	Gestor de Accesos	TIC
Mantenimiento	C / I	C / I	A / R	R	Jefe de Sistemas	TIC	Gestor de Cambios	Procesos Operativos
					Asistente de Sistemas	TIC	Gestor de Cambios	TIC
Monitoreo	C / I		R	R	Jefe de Sistemas	TIC	Gestor de Monitoreo	Procesos Operativos
					Asistente de Sistemas	TIC	Gestor de Monitoreo	TIC
Proveedor	C / I	C / I	A / R	R	Jefe de Sistemas	TIC	Gestor de Proveedor	Procesos Operativos
					Asistente de Sistemas	TIC	Gestor de Proveedor	TIC
Requerimientos	C / I	C / I	A / R	R	Jefe de Sistemas	TIC	Gestor de Niveles de Servicio	Procesos Operativos
					Asistente de Sistemas	TIC	Gestor de Niveles de Servicio	TIC
Reseteo de claves	C / I		A / R	R	Jefe de Sistemas	TIC	Gestor de Accesos	Procesos Operativos
					Asistente de Sistemas	TIC	Gestor de Accesos	TIC
Soporte a usuarios	C / I		A / R	R	Jefe de Sistemas	TIC	Gestor de Incidentes y Requerimientos	Procesos Operativos
					Asistente de Sistemas	TIC	Gestor de Incidentes y Requerimientos	TIC
Soporte aplicación /	C / I	C / I	A / R	R	Jefe de Sistemas	TIC	Gestor de Incidentes y Requerimientos	Procesos Operativos

infraest ructura					Asistente de Sistemas	TIC	Gestor de Incidentes y Requerimientos	TIC

De lo observado en esta investigación, se pudo determinar que, dentro de las actividades operativas de “TIC”, también incluyen proyectos destinados a crear nuevos productos o servicios que las diferentes áreas, especialmente: Negocios, Marketing y Operaciones quieren implementar para satisfacer las necesidades de los socios o clientes.

3.5 Grado de Madurez de las actividades de “TIC”

Para conocer el grado de madurez de las actividades del Departamento de “TIC” de la Cooperativa “Pedro Moncayo Ltda.”, se utilizará el modelo de madurez planteado en RISK IT (ISACA, 2009, pág. 42), y su medición se aplicará a las actividades definidos en la Tabla 9. Listado Actual de Actividades de “TIC”, las que se citan a continuación:

- AAT01. Monitoreo
- AAT02. Mantenimiento
- AAT03. Soporte a usuarios
- AAT04. Instalación a usuarios
- AAT05. Creación de usuarios
- AAT06. Reseteo de usuarios
- AAT07. Inactivación de usuarios
- AAT08. Configuración
- AAT09. Soporte Aplicación / Infraestructura
- AAT10. Proveedores
- AAT11. Requerimientos

La matriz permitirá identificar el grado de madurez actual, también podrá visualizar el grado de madurez recomendado, al que deberían alcanzar el Departamento de “TIC”.

Para la medición del Grado de Madurez de las actividades tecnológicas, se considera los 6 atributos de medición de RISK IT explicados en el capítulo II, sección 2.5.4.3 de la presente tesis.

A continuación, se evalúa el grado de madurez de cada actividad existente en el Departamento de “TIC”:

AAT01. Monitoreo

Tabla 11.

AAT01 Monitoreo

Actividad TI	Cód. Tarea	Sistema / Aplicación / Plataforma	A1	A2	A3	A4	A5	A6
AAT01. MONITOREO	AAT01.1	Monitoreo de Consola de Antivirus	1	0	0	0	0	0
	AAT01.2	Seguimiento y monitoreo de red	1	0	0	0	0	0
	AAT01.3	Control filtrado de contenido de internet	1	0	0	0	0	0
	AAT01.4	Monitoreo de recursos físicos de cajeros automáticos	1	0	0	0	0	0

La actividad de Monitoreo en cada uno de los sistemas, aplicaciones o plataformas que realiza el Jefe y/o el Analista de Sistemas del departamento de “TIC” lo hacen por conocimiento y expertiz adquirido en el tiempo. No existe ningún procedimiento o instructivo para ejecutar esta actividad TI. Además, el monitoreo es parcial, en otras palabras, no se lo ejecuta a todos los sistemas, plataformas, aplicaciones, equipos de computación, dispositivos de comunicación, entre otros.

Resultado:

El levantamiento de información y la evaluación permitió conocer que el grado de madurez de la actividad TI de Monitoreo es:

0- Proceso Incompleto, debido a que no está implementado. Se encuentra en proceso de elaboración de la documentación y flujo de procesos involucrados.

AAT02. Mantenimiento

Tabla 12.

AAT02 Mantenimiento

Actividad TI	Cód. Tarea	Sistema / Aplicación / Plataforma	A1	A2	A3	A4	A5	A6
AAT02. MANTENIMIENTO	AAT02.1	Mantenimiento preventivo de base de datos	1	0	0	0	0	0
	AAT02.2	Mantenimiento preventivo de equipos de computación	1	0	0	0	0	0
	AAT02.3	Mantenimiento del intranet institucional	1	0	0	0	0	0

La actividad de Mantenimiento en cada uno de los sistemas, aplicaciones o plataformas que realiza el Jefe y/o el Analista de Sistemas del departamento de “TIC” es por conocimiento y por la experiencia adquirida en el tiempo. No existe ningún procedimiento o instructivo para ejecutar esta actividad TI. Además, esta actividad es puntual para ciertos sistemas o plataformas.

Resultado:

El levantamiento de información y la evaluación permitió conocer que el grado de madurez de la actividad TI de Mantenimiento es:

0- Proceso Incompleto, debido a que no está implementado. Se encuentra en proceso de elaboración de la documentación y flujo de procesos involucrados.

AAT03. Soporte a usuarios

Tabla 13.

AAT03 Soporte a Usuarios

Actividad TI	Cód. Tarea	Sistema / Aplicación / Plataforma	A1	A2	A3	A4	A5	A6
AAT03. SOPORTE A USUARIOS	AAT03.1	Soporte a usuarios del CORE financiero	1	0	0	0	0	0
	AAT03.2	Soporte a usuarios servicio facilito	1	0	0	0	0	0
	AAT03.3	Soporte a usuarios servicio entura	1	0	0	0	0	0
	AAT03.4	Soporte a usuarios servicio extreme	1	0	0	0	0	0
	AAT03.5	Soporte a usuarios consola de red	1	0	0	0	0	0
	AAT03.6	Soporte a usuarios por hardware	1	0	0	0	0	0

La actividad de Soporte a Usuarios en cada uno de los sistemas, aplicaciones o plataformas que realiza el Jefe y/o el Analista de Sistemas del departamento de "TIC" lo ejecutan en base a su conocimiento y experiencia adquirida en el tiempo. No existe ningún procedimiento o instructivo para ejecutar esta actividad TI. Como se evidenció, el soporte a usuarios no se lo hace para todos los sistemas, plataformas y aplicaciones

Resultado:

El levantamiento de información y la evaluación permitió conocer que el grado de madurez de la actividad TI de Soporte a Usuarios es:

0- Proceso Incompleto, debido a que no está implementado. Se encuentra en proceso de elaboración de la documentación y flujo de procesos involucrados.

AAT04. Instalación a usuarios

Tabla 14.

AAT04 Instalación a Usuarios

Actividad TI	Cód. Tarea	Sistema / Aplicación / Plataforma	A1	A2	A3	A4	A5	A6
AAT04. INSTALACIÓN A USUARIOS	AAT04.1	Instalación del CORE financiero	1	0	0	0	0	0
	AAT04.2	Instalación del servicio facilito	1	0	0	0	0	0
	AAT04.3	Instalación del servicio entura	1	0	0	0	0	0

	AAT04.4	Instalación del servicio extreme	1	0	0	0	0	0
	AAT04.5	Instalación del antivirus	1	0	0	0	0	0
	AAT04.6	Instalación del intranet	1	0	0	0	0	0
	AAT04.7	Instalación de PINPAD	1	0	0	0	0	0

La actividad de Instalación a Usuarios en cada uno de los sistemas, aplicaciones o plataformas que realiza el Jefe y/o el Analista de Sistemas del departamento de “TIC” se lo hace en base a su conocimiento y experiencia adquirida en el tiempo. No existe ningún procedimiento o instructivo para ejecutar esta actividad TI. Como se evidenció, las instalaciones no son en todas las aplicaciones, dado que la mayoría de estas tareas lo ejecutan empresas proveedoras.

Resultado:

El levantamiento de información y la evaluación permitió conocer que el grado de madurez de la actividad TI de Instalación a Usuarios es:

0- Proceso Incompleto, debido a que no está implementado. Se encuentra en proceso de elaboración de la documentación y flujo de procesos involucrados.

AAT05. Creación de usuarios

Tabla 15.

AAT05 Creación de Usuarios

Actividad TI	Cód. Tarea	Sistema / Aplicación / Plataforma	A1	A2	A3	A4	A5	A6
AAT05. CREACIÓN USUARIOS	AAT05.1	Creación de nuevos usuarios del CORE financiero	1	0	0	0	0	0
	AAT05.2	Creación nuevos usuarios servicio facilito	1	0	0	0	0	0
	AAT05.3	Creación nuevos usuarios servicio entura	1	0	0	0	0	0
	AAT05.4	Creación nuevos usuarios servicio extreme	1	0	0	0	0	0
	AAT05.5	Creación de nuevos usuarios de correo electrónico	1	0	0	0	0	0
	AAT05.6	Creación de nuevo usuario de intranet	1	0	0	0	0	0

	AAT05.7	Creación de nuevo usuario para control de asistencia	1	0	0	0	0	0
	AAT05.8	Creación nuevos usuarios consola de red	1	0	0	0	0	0

La actividad de Creación de Usuarios en cada uno de los sistemas, aplicaciones o plataformas que realiza el Jefe y/o el Analista de Sistemas del departamento de “TIC” lo ejecutan en base a su conocimiento y experiencia adquirida en el tiempo. No existe ningún procedimiento o instructivo para ejecutar esta actividad TI. Del levantamiento de información se pudo identificar que la creación de usuarios no se lo hace para todos los sistemas, plataformas y aplicaciones, dado que lo realizan proveedores de servicio.

Resultado:

El levantamiento de información y la evaluación permitió conocer que el grado de madurez de la actividad TI de Creación de Usuarios es:

0- Proceso Incompleto, debido a que no está implementado. Se encuentra en proceso de elaboración de la documentación y flujo de procesos involucrados.

AAT06. Reseteo de claves

Tabla 16.

AAT06 Reseteo de Claves

Actividad TI	Cód. Tarea	Sistema / Aplicación / Plataforma	A1	A2	A3	A4	A5	A6
AAT06. RESETEO DE CLAVES	AAT06.1	Reseteo de claves del CORE financiero	1	0	0	0	0	0
	AAT06.2	Reseteo de claves servicio facilito	1	0	0	0	0	0
	AAT06.3	Reseteo de claves servicio entura	1	0	0	0	0	0
	AAT06.4	Reseteo de claves servicio extreme	1	0	0	0	0	0
	AAT06.5	Reseteo de claves consola de red	1	0	0	0	0	0

La actividad de Reseteo de Claves en cada uno de los sistemas, aplicaciones o plataformas que realiza el Jefe y/o el Analista de Sistemas del departamento de “TIC” lo ejecutan sin seguir ningún procedimiento o instructivo, solamente por conocimiento empírico. Además, se pudo observar que el reseteo de claves no se lo hace para todos los sistemas, plataformas y aplicaciones, dado que esta actividad lo realiza empresas proveedoras de servicio.

Resultado:

El levantamiento de información y la evaluación permitió conocer que el grado de madurez de la actividad TI de Reseteo de Claves es:

0- Proceso Incompleto, debido a que no está implementado. Se encuentra en proceso de elaboración de la documentación y flujo de procesos involucrados.

AAT07. Inactivación de usuarios

Tabla 17.

AAT07 Inactivación de Usuarios

Actividad TI	Cód. Tarea	Sistema / Aplicación / Plataforma	A1	A2	A3	A4	A5	A6
AAT07. INACTIVACIÓN DE USUARIO	AAT07.1	Inhabilitar usuario del CORE financiero	1	0	0	0	0	0
	AAT07.2	Inhabilitar usuario servicio facilito	1	0	0	0	0	0
	AAT07.3	Inhabilitar usuario servicio entura	1	0	0	0	0	0
	AAT07.4	Inhabilitar usuario servicio extreme	1	0	0	0	0	0
	AAT07.5	Inhabilitar usuario consola de red	1	0	0	0	0	0

La actividad de Inactivación de Usuarios en cada uno de los sistemas, aplicaciones o plataformas que realiza el Jefe y/o el Analista de Sistemas del departamento de “TIC” lo ejecutan en base a su conocimiento y experiencia adquirida en el tiempo. No existe ningún procedimiento o instructivo para ejecutar esta actividad TI. Del levantamiento de información se pudo identificar que la

inactivación de usuarios no se lo hace para todos los sistemas, plataformas y aplicaciones, dado que se encuentra a cargo de empresas proveedoras este servicio.

Resultado:

El levantamiento de información y la evaluación permitió conocer que el grado de madurez de la actividad TI de Inactivación de Usuarios es:

0- Proceso Incompleto, debido a que no está implementado. Se encuentra en proceso de elaboración de la documentación y flujo de procesos involucrados.

AAT08. Configuración

Tabla 18.

AAT08 Configuración

Actividad TI	Cód. Tarea	Sistema / Aplicación / Plataforma	A1	A2	A3	A4	A5	A6
AAT08. CONFIGURACIÓN	AAT08.1	Configuración y asignación de IP de red a nuevos usuarios	1	0	0	0	0	0
	AAT08.02	Configuración de aplicativos de control de asistencia	1	0	0	0	0	0
	AAT08.03	Configuración de PIN PAD	1	0	0	0	0	0
	AAT08.04	Configuración de estaciones de trabajo	1	0	0	0	0	0
	AAT08.05	Configuración de seguridad para perfilamiento por cargo	1	0	0	0	0	0
	AAT08.06	Configuración de un nuevo punto de red	1	0	0	0	0	0
	AAT08.07	Configuración de cuenta de correo electrónico	1	0	0	0	0	0

La actividad de Configuración para cada uno de los sistemas, aplicaciones o plataformas que realiza el Jefe y/o el Analista de Sistemas del departamento de “TIC” lo ejecutan en base a su conocimiento y experiencia adquirida en el tiempo. No existe ningún procedimiento o instructivo paso a paso para hacer esta actividad TI. Son muy pocos los sistemas, plataformas y aplicaciones que

pueden ser configurados por el departamento de “TIC”, ya que esta actividad lo realizan proveedores de servicio.

Resultado:

El levantamiento de información y la evaluación permitió conocer que el grado de madurez de la actividad TI de Configuración es:

0- Proceso Incompleto, debido a que no está implementado. Se encuentra en proceso de elaboración de la documentación y flujo de procesos involucrados.

AAT09. Soporte Aplicación / Infraestructura

Tabla 19.

AAT09 Soporte Aplicación/Infraestructura

Actividad TI	Cód. Tarea	Sistema / Aplicación / Plataforma	A1	A2	A3	A4	A5	A6
AAT09. SOPORTE APLICACIÓN / INFRAESTRUCTURA	AAT09.1	Cierre de Fin de Día	1	0	0	0	0	0
	AAT09.2	Acreditación mensual de intereses	1	0	0	0	0	0
	AAT09.3	Respaldo de base de datos del Core financiero	1	0	0	0	0	0
	AAT09.4	Restaurar base de datos del Core financiero	1	0	0	0	0	0
	AAT09.5	Generación de back up de PC	1	0	0	0	0	0
	AAT09.6	Baja información cámaras de seguridad	1	0	0	0	0	0
	AAT09.7	Baja información de control de asistencia	1	0	0	0	0	0
	AAT09.8	Actualizaciones de parches	1	0	0	0	0	0

La actividad de Soporte de Aplicaciones e Infraestructura para cada uno de los sistemas, aplicaciones o plataformas que realiza el Jefe y/o el Analista de Sistemas del departamento de “TIC” lo ejecutan en base a su conocimiento y experiencia adquirida en el tiempo. No existe ningún procedimiento o instructivo,

paso a paso para hacer estas actividades TI. Son muy pocos los sistemas, plataformas y aplicaciones que están a cargo del soporte del departamento de “TIC”, ya que esta actividad lo realizan proveedores de servicio.

Resultado:

El levantamiento de información y la evaluación permitió conocer que el grado de madurez de la actividad TI de Soporte de Aplicaciones e Infraestructura es:

0- Proceso Incompleto, debido a que no está implementado. Se encuentra en proceso de elaboración de la documentación y flujo de procesos involucrados.

AAT10. Proveedores

Tabla 20.

AAT10 Proveedores

Actividad TI	Cód. Tarea	Sistema / Aplicación / Plataforma	A1	A2	A3	A4	A5	A6
AAT10. PROVEEDOR	AAT10.1	Instalación de nueva cámara de seguridad	1	0	0	0	0	0
	AAT10.2	Configuración de nueva cámara de seguridad	1	0	0	0	0	0
	AAT10.3	Mantenimiento preventivo de cámaras de seguridad	1	0	0	0	0	0
	AAT10.4	Mantenimiento de la página web institucional	1	0	0	0	0	0
	AAT10.5	Mantenimiento preventivo de software	1	0	0	0	0	0
	AAT10.6	Mantenimiento preventivo de cajero automático	1	0	0	0	0	0
	AAT10.7	Monitoreo consola de grabación cámaras de seguridad	0	0	0	0	0	0
	AAT10.8	Configuración de Cortafuego, filtrado web, control de aplicaciones y correo electrónico interno	0	0	0	0	0	0

La actividad de Proveedores, se refiere al soporte que las empresas proveedoras de servicio mantienen con COAC “Pedro Moncayo Ltda.”, para cada uno de los sistemas, aplicaciones o plataformas utilizadas por el negocio, algunas de las cuales no son gestionadas con el departamento de “TIC”, sino que los responsables o dueños del proceso operativo, lo gestionan directamente con los proveedores de servicio. No existe ningún inventario, procedimiento o instructivo que permita tener conocimiento sobre el paso a paso a seguir para solicitar soporte en caso de tener problemas de servicio.

Resultado:

El levantamiento de información y la evaluación permitió conocer que el grado de madurez de la actividad TI de Proveedores es:

0- Proceso Incompleto, debido a que no está implementado. Se encuentra en proceso de elaboración de la documentación y flujo de procesos involucrados.

AAT011. Requerimientos

Tabla 21.

AAT11 Requerimientos

Actividad TI	Cód. Tarea	Sistema / Aplicación / Plataforma	A1	A2	A3	A4	A5	A6
AAT11. REQUERIMIENTOS	AAT11.1	Nueva publicación en la página web institucional	1	0	0	0	0	0
	AAT11.2	Nuevo requerimiento del Core financiero	1	0	0	0	0	0
	AAT11.3	Generación de reportes nuevos desde la base de datos del Core financiero	1	0	0	0	0	0
	AAT11.4	Implementación de reportes nuevos en el módulo de reportes	1	0	0	0	0	0
	AAT11.5	Solicitud de video de las cámaras de seguridad	1	0	0	0	0	0

La actividad de Requerimientos que existe para cada uno de los sistemas, aplicaciones o plataformas que realiza el Jefe y/o el Analista de Sistemas del

departamento de “TIC”, no mantienen un procedimiento formal, sino más bien es verbal, ya sea por llamada telefónica, conversación o un correo electrónico sin informal.

Resultado:

El levantamiento de información y la evaluación permitió conocer que el grado de madurez de la actividad TI de Requerimientos es:

0- Proceso Incompleto, debido a que no está implementado. Se encuentra en proceso de elaboración de la documentación y flujo de procesos involucrados.

3.5.1 Consolidación del Grado de Madurez de las Actividades TI

Una vez realizado el análisis del grado de madurez de las actividades TI con cada una de las tareas ejecutadas en el Departamento de “TIC”, se determinó que el mismo se encuentra en “0-Proceso Incompleto”. Esto se debe a que ninguna actividad TI se encuentra documentada, tampoco mantiene definido el flujo de gestión del proceso a nivel de responsables, de funcionalidad, de participantes, entre otros.

A continuación, se muestra el consolidado del grado de madurez de las actividades TI en la Figura 15:

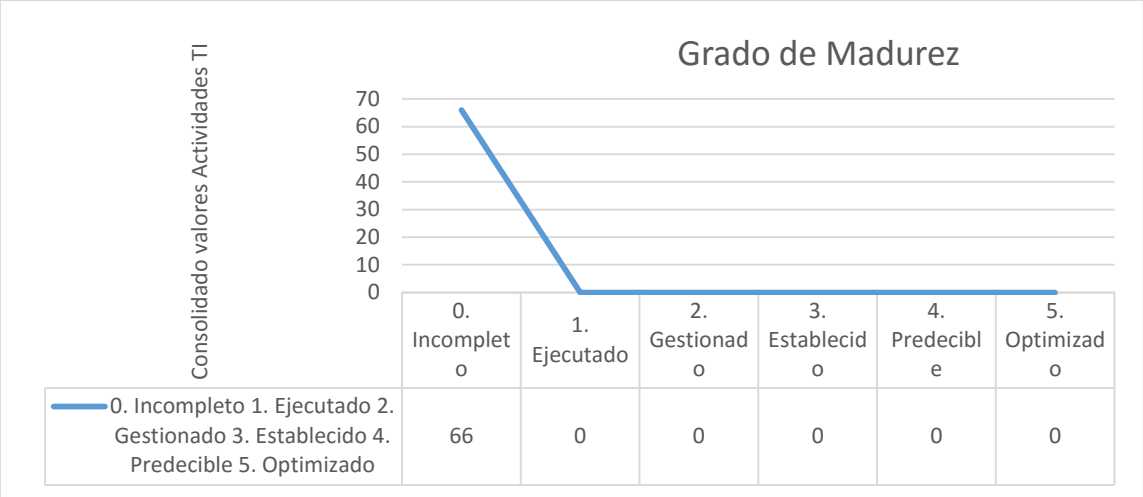


Figura 16. Consolidado de Grado de Madurez de actividades TI.

4 Capítulo IV. Evaluación de Riesgos

En este capítulo se identificará los riesgos y evaluará la criticidad de los mismos, en base a una escala y a parámetros de impacto o consecuencia y probabilidad o frecuencia; todo basado en el dominio de “RE – Evaluación de Riesgos” de la metodología de RISK IT (ISACA, 2009, pág. 23), indicada en el capítulo II.

4.1 Uso de marco de Gestión de Riesgos de TI

En este proyecto de titulación y en base a la metodología indicada en el Capítulo II se va a utilizar el dominio RE – Evaluación de Riesgos de RISK IT (ISACA, 2009, pág. 15) .

Esto ayudará a reconocer las actividades vitales del Departamento de “TIC” y detectar amenazas y vulnerabilidades existentes que podrían afectar la operatividad del negocio. Además, permitirá priorizar los riesgos, establecer el grado de madurez de estas actividades TI y determinar un plan de mejoras, para que la Cooperativa pueda tomar acciones y decisiones acorde a sus metas y objetivos planteados.

4.1.1 Parámetros de Métodos de Análisis de Riesgos

Para realizar el análisis de riesgos en este proyecto de titulación y de acuerdo a la metodología explicada en el capítulo II de RISK IT, se utilizarán dos parámetros: frecuencia o probabilidad de ocurrencia y el impacto o consecuencia para el negocio si se llegara a suceder la amenaza, de acuerdo a la guía “The Risk IT Practitioner Guide” (ISACA, 2009, pág. 32)

Además, se empleará el método de análisis cuantitativo, dado que se utilizarán “valores cuantitativos (por ejemplo, rangos) para definir valores cualitativos. La esencia de la evaluación cuantitativa del riesgo consiste en derivar la frecuencia y las consecuencias de los escenarios de riesgo, basados en métodos y datos estadísticos.” (The Risk IT Practitioner Guide, 2009, pág. 34), explicados en el capítulo II de la presente tesis.

4.2 Identificación de problemas en el Departamento de “TIC”

En el Departamento de “TIC”, se identificaron problemas en sus actividades actuales. Estos problemas representan amenazas o vulnerabilidades para el negocio tanto a nivel financiero, clientes, interno y de aprendizaje y crecimiento.

Para codificar estos problemas se ha utilizado la siguiente nomenclatura: Pxx; en donde:

P, significa Problema

xx, es un número secuencial de 2 dígitos

Los problemas encontrados en el Departamento de “TIC” son los siguientes:

1. P01. No existe documentación sobre la operación de las actividades de “TIC”.
2. P02. No existe ningún proceso de gestión de eventos y gestión de incidentes.

3. P03. No existe un proceso de custodia de información.
4. P04. No existe un proceso de restauración de base de datos.
5. P05. No existe ningún proceso de gestión de solución de problemas.
6. P06. No existe ningún proceso de gestión de niveles de servicio.
7. P07. No existe ningún proceso de gestión de proveedores.
8. P08. No existe ningún modelo de seguridad.
9. P09. No cuentan con una inducción adecuada de los procesos internos

4.2.1 Amenazas y vulnerabilidades

A continuación, se describen los problemas de cada uno de las actividades actuales del Departamento de "TIC" con sus respectivas amenazas y vulnerabilidades:

AAT01. MONITOREO. - En esta actividad se han encontrado los siguientes problemas:

P01. No existe documentación sobre la operativa de las actividades de "TIC"

No existe documentación sobre la operativa de las actividades de monitoreo ejecutados sobre el antivirus, el filtrado de contenido de internet, los recursos físicos de los cajeros automáticos y la red.

Amenaza. - La actividad de monitoreo se lo lleva de manera empírica, es decir, sin utilizar ningún manual o guía de usuario, porque la forma de ejecutar esta actividad no se encuentra escrito.

Vulnerabilidad. - El conocimiento del flujo y la operativa de esta actividad lo tiene el Jefe del área de Tecnología de la Información y Comunicaciones únicamente. Si por alguna razón este funcionario tiene que salir de la Cooperativa, existiría la posibilidad de que no se realice parcial o total el monitoreo de los sistemas, lo que podría ocasionar indisponibilidad del negocio.

P02. No existe ningún proceso de gestión de eventos y gestión de incidentes.

No existe ningún proceso de gestión de eventos y gestión de incidentes, que permita priorizar la atención inmediata sobre eventos anómalos, amenazas o vulnerabilidades en los sistemas monitoreados por el departamento de “TIC”

Amenaza. – Al no existir ningún proceso de gestión de eventos y de gestión de incidentes sobre eventos anómalos de los sistemas monitoreados, ocasionan que la Cooperativa se exponga a un riesgo inminente de disponibilidad de servicio, que podría ocasionar pérdida económica y daño de la reputación corporativa.

Vulnerabilidad. – La actividad de monitoreo no posee niveles de atención para resolución de eventos o incidentes tecnológicos internos (empleados, funcionarios de la Cooperativa) o externos (clientes). Tampoco mantiene un proceso de escalamiento para el restablecimiento de servicio con los proveedores, en base a la criticidad, frecuencia e impacto que ayude a erradicar la causa del evento o incidente.

AAT02. MANTENIMIENTO. - En esta actividad se han encontrado los siguientes problemas:

P01. No existe documentación sobre la operativa de las actividades de “TIC”

No existe documentación en donde se detallen los pasos a seguir para realizar el mantenimiento preventivo sobre las bases de datos de las aplicaciones, incluida la aplicación principal del negocio Core Financiero, Financial, y de los equipos de cómputo existentes en la Cooperativa. Tampoco se ha documentado el mantenimiento que se debe dar a la intranet institucional.

Amenaza. – El desconocer la forma de ejecutar el mantenimiento preventivo de las bases de datos de las aplicaciones y de los equipos de cómputo, existe la posibilidad de perder información vital y primordial para el negocio, que puede desembocar en pérdida económica y de imagen corporativa. Además, al no saber cómo realizar un mantenimiento del intranet institucional, puede provocar que los visitantes a este sitio tengan información desactualizada referente a beneficios, productos y servicios ofertados por COAC.

Vulnerabilidad. - El conocimiento del flujo y la operativa de esta actividad lo tiene de forma empírica solamente los actuales funcionarios del Departamento de Tecnología de la Información y Comunicaciones. Si por alguna razón estos colaboradores salen de la Cooperativa, existe una probabilidad alta de que esta actividad no se lo ejecute y provoque pérdidas de clientes, económicas e incluso multas por retraso de pago de impuestos, entre otros para la Cooperativa.

P03. No existe un proceso de custodia de información.

Una de las actividades a realizar dentro del mantenimiento preventivo de las bases de datos, de los equipos de cómputo y de la intranet institucional, es obtener respaldos de la información, sin embargo, el lugar de almacenamiento de estos respaldos es en los cajones de los escritorios ubicados en el departamento de “TIC”.

Vulnerabilidad. – Los activos de información que se obtienen principalmente de la base de datos, son primordiales para el negocio. Al no contar con un proceso de custodia adecuado, existe la posibilidad de que se pierdan los repositorios o que se dañen, y al momento que se requiera no van a estar disponibles, lo que puede ocasionar problemas legales con los entes de control, así como con los socios o clientes de la COAC; además, de pérdidas económicas y de reputación.

P04. No existe un proceso de restauración de base de datos.

A pesar de que existe la actividad para respaldar la base de datos del Core Financiero “Financial”, no existe ningún proceso formal para restaurar ésta y las otras bases de datos de las aplicaciones existentes en la Cooperativa.

Amenaza. – Si los activos de información obtenidos de los respaldos de las bases de datos, no son válidos, pueden ocasionar pérdida de información de clientes o socios, así como de la transaccionalidad de la Cooperativa.

Vulnerabilidad. – Al no tener un proceso formal de restauración de la información que se extrajo de las bases de datos, existe la posibilidad de que los datos no guarden la integridad requerida y esto ocasione problemas legales con los entes de control, con los socios o clientes, con los proveedores, entre otros de la Cooperativa.

AAT03. SOPORTE A USUARIOS. - En esta actividad se han encontrado los siguientes problemas:

P01. No existe documentación sobre la operativa de las actividades de “TIC”.

No existe ninguna documentación sobre la funcionalidad de las aplicaciones a las que tienen acceso los empleados de la Cooperativa, como son: Financial, Facilito, Extreme, sobre el soporte requerido para el acceso a la red y a los computadores de escritorio.

Amenaza. – El desconocer la forma de dar soporte sobre las aplicaciones que utilizan los usuarios, afecta a la calidad de servicio que se da a los socios o clientes, debido a que los empleados no pueden acceder a las aplicaciones requeridas y, por ende, existe retraso en la atención al público, consiguiendo malestar e incluso un mal entendido si el tiempo de indisponibilidad del sistema es excesivo.

Vulnerabilidad. - El conocimiento del flujo y la operativa de esta actividad solamente poseen los actuales funcionarios del Departamento de Tecnología de la Información y Comunicaciones de forma empírica. Si por alguna razón estos colaboradores salen de la institución, existe una probabilidad alta de que fallen las aplicaciones, especialmente la del Core Financiero, provocando demora en la atención a los clientes o socios, desmejorando la calidad de servicio e incluso causando especulación y malos entendidos respecto a las finanzas de la Cooperativa.

P02. No existe ningún proceso de gestión de eventos y gestión de incidentes.

No existe ningún proceso de gestión de eventos y gestión de incidentes, que permita priorizar la atención inmediata sobre eventos anómalos, amenazas o vulnerabilidades en los sistemas y aplicaciones utilizados por los empleados de COAC “Pedro Moncayo Ltda.”

Amenaza. – Al no existir ningún proceso de gestión de eventos y de incidentes sobre fallas o eventos anómalos de las aplicaciones utilizadas por los empleados, la Cooperativa está expuesta a un riesgo inminente de pérdida de confiabilidad por la demora en la atención a los clientes o socios causado mal estar y especulaciones, que podría ocasionar pérdida de la reputación corporativa.

Vulnerabilidad. – La actividad de soporte no posee niveles de atención para resolución de eventos o incidentes operativos y tecnológicos internos (empleados, funcionarios de la Cooperativa) o externos (clientes). Tampoco mantiene un proceso de escalamiento para el restablecimiento de servicio con los proveedores, en base a la criticidad, frecuencia e impacto que ayude a erradicar la causa del evento o incidente.

P05. No existe ningún proceso de gestión de solución de problemas.

Cuando los empleados de la Cooperativa tienen problemas con las aplicaciones o sistemas que requieren para realizar su trabajo diario, no conocen cuál es el soporte que les puede dar el departamento de “TIC” y cómo deben solicitarlo.

Amenaza. – La ausencia de un proceso de gestión de solución de problemas perjudica con la eficacia y eficiencia de los empleados de la Cooperativa, dado que no saben el procedimiento a seguir para solucionar los inconvenientes o problemas que se les presenta en las aplicaciones o sistemas a los que tienen acceso por sus actividades y tareas diarias.

Vulnerabilidad. – La inexistencia de un proceso de gestión de solución de problemas puede convertirse en una vulnerabilidad crítica que atenta contra la calidad de servicio que la Cooperativa quiere dar a sus clientes o socios, al desmejorar los tiempos de atención por tener problemas de soporte de las aplicaciones o sistemas utilizados por los empleados.

P06. No existe ningún proceso de gestión de niveles de servicio.

Tanto el soporte dado por parte del Departamento de Tecnología de la Información y Comunicaciones como el soporte dado por los proveedores de los sistemas y aplicaciones que utilizan los usuarios de la Cooperativa no mantienen un esquema de niveles de acuerdos de servicio que permita tener conocimiento del tiempo de respuesta que se tiene por cada requerimiento realizado, o los niveles de escalamiento necesarios en base a la criticidad del problema, o por la calidad de servicio brindado al requerimiento.

Amenaza. – Al no contar con un proceso de gestión de niveles de servicio los empleados y el departamento de “TIC”, no pueden realizar ningún reclamo al proveedor de servicio, ya sea por atención del requerimiento fuera de tiempo o por la calidad de servicio brindado.

Vulnerabilidad. – Al no tener un proceso de gestión de niveles de servicio tanto el departamento de “TIC” como los empleados tienen una alta probabilidad de pérdida de tiempo para la resolución de requerimientos, que para el negocio pueden ser vitales y que no son atendidos con la prioridad del caso. Esto puede ocasionar pérdidas económicas para la Cooperativa por no contar con un acuerdo escrito de niveles de servicio con los diferentes proveedores con los que trabaja.

P07. No existe ningún proceso de gestión de proveedores.

El soporte de la mayoría de aplicaciones y sistemas que utiliza COAC “Pedro Moncayo Ltda.”, lo realizan proveedores servicio; sin embargo, no existe ningún proceso de gestión de proveedores, complicándose más porque no todos los sistemas están bajo responsabilidad de “TIC”.

Amenaza. – Cuando los empleados solicitan soporte sobre una aplicación o sistema en particular por problemas de acceso, desconocen el procedimiento que deben seguir para gestionar su requerimiento con los proveedores de servicio, lo que provoca ineficiencia e ineficacia en su trabajo, especialmente de atención al público.

Otra amenaza inminente es la divulgación de información considerada como confidencial a la que las empresas proveedoras tienen acceso, especialmente a las credenciales de usuarios con máximos privilegios de los sistemas y aplicaciones que administran como parte del servicio.

Vulnerabilidad. – Al no existir un proceso de gestión de proveedores, la Cooperativa puede estar expuesta a robo, destrucción, uso inadecuado de información confidencial y crítica para el negocio, no se tiene actas de responsabilidad, ni acuerdos de confidencialidad de entrega, manejo y manipulación de información, específicamente de credenciales de usuarios para

acceder a las aplicaciones y a los sistemas administrados por los proveedores de servicio.

P08. No existe ningún modelo de seguridad

El Departamento de Tecnología de la Información y Comunicaciones no tiene ningún modelo de seguridad para proteger la información calificada como crítica para la Cooperativa.

Amenaza. – Los empleados de la Cooperativa no tienen una cultura de seguridad respecto al uso de cuentas de usuario, aplicaciones a las que tienen acceso e información crítica manejada y manipulada, de acuerdo a las funciones y actividades que realizan, por lo que la Cooperativa está expuesta a un riesgo inminente de fuga de información, robos o fraudes.

Vulnerabilidad. - A pesar que el Departamento de Tecnología de la Información y Comunicaciones lleva controles respecto a inducción de uso de contraseñas, personaliza credenciales de usuarios para el acceso de aplicaciones y sistemas, no posee ningún modelo de seguridad que le garantice confidencialidad, integridad y disponibilidad de la información categorizada como crítica.

P09. No cuentan con una inducción adecuada de los procesos internos

La inducción que reciben los colaboradores de COAC “Pedro Moncayo Ltda.”, relacionado a los accesos a sistemas o aplicaciones no incluye al proceso de soporte a usuarios.

Amenaza. – Existe desconocimiento de las actividades de soporte a usuarios por parte de los empleados de la Cooperativa, lo que provoca problemas de gestión de requerimientos para acceso a las aplicaciones y sistemas, debido a una inducción inadecuada por parte del área de Talento Humano, lo que podría provocar ineficiencia e ineficacia en la calidad de servicio a los socios o clientes.

AAT04. INSTALACIÓN A USUARIOS. - En esta actividad se han encontrado los siguientes problemas:

P01. No existe documentación sobre la operativa de las actividades de "TIC".

No existe ninguna documentación sobre la instalación de los sistemas y aplicaciones a las que tienen acceso los empleados de la Cooperativa, como son: Financial, Facilito, Entura, Extreme, Pin Pad y el antivirus requerido para que los empleados realicen sus actividades diarias.

Amenaza. – El desconocer la forma de instalar las aplicaciones y sistemas, afecta a la calidad de servicio que los empleados y socios o clientes esperan del departamento de "TIC", que incluso puede provocar demoras en la atención al público.

Vulnerabilidad. - El conocimiento del flujo y la operativa de esta actividad solamente poseen los actuales funcionarios del Departamento de Tecnología de la Información y Comunicaciones de forma empírica. Si por alguna razón estos colaboradores salen de la institución, existe una alta probabilidad de que nadie pueda instalar las aplicaciones y sistemas, especialmente la del Core Financiero, lo que provocaría que la atención a los clientes o socios se vea impactada.

P02. No existe ningún proceso de gestión de eventos y gestión de incidentes.

No existe ningún proceso de gestión de eventos y gestión de incidentes, que permita priorizar la atención inmediata sobre eventos anómalos, amenazas o vulnerabilidades en la instalación de los sistemas y aplicaciones utilizados por los empleados de COAC "Pedro Moncayo Ltda."

Amenaza. – Al no existir ningún proceso de gestión de eventos y de incidentes sobre fallas o eventos anómalos durante la instalación de las aplicaciones utilizadas por los empleados, la Cooperativa está expuesta a un riesgo inminente

de pérdida de confiabilidad por la demora en la atención a los clientes o socios causando mal estar y especulaciones, que podría ocasionar pérdida de la reputación corporativa.

Vulnerabilidad. – La actividad de instalación a usuarios no posee niveles de atención para resolución de eventos o incidentes operativos y tecnológicos internos (empleados, funcionarios de la Cooperativa).

P06. No existe ningún proceso de gestión de niveles de servicio.

La actividad de instalación de aplicaciones y sistemas a los usuarios por parte del Departamento de Tecnología de la Información y Comunicaciones, no mantiene un esquema de niveles de acuerdos de servicio, especialmente sobre el tiempo de respuesta que se necesita para cada requerimiento, o los niveles de escalamiento necesarios en base a la criticidad del problema.

Amenaza. – Al no contar con un proceso de gestión de niveles de servicio los empleados no pueden realizar ningún reclamo al departamento de “TIC”, ya sea por atención del requerimiento fuera de tiempo o por la calidad de servicio brindado.

Vulnerabilidad. – Tanto el departamento de “TIC” como los empleados tienen una alta probabilidad de pérdida de tiempo para la resolución de requerimientos, debido a la falta de un proceso de gestión de niveles de servicio, que les permita dar prioridad a la instalación de aplicaciones y sistemas de acuerdo a la criticidad que éstas representan dentro del negocio.

P09. No cuentan con una inducción adecuada de los procesos internos

La inducción que reciben los colaboradores de COAC “Pedro Moncayo Ltda.”, relacionado a los accesos a sistemas o aplicaciones no incluye al proceso de instalación de aplicaciones y sistemas a usuarios finales.

Amenaza. – Existe desconocimiento de las actividades de instalación de aplicaciones y sistemas a usuarios por parte de los empleados de la Cooperativa, lo que provoca inconvenientes para gestionar requerimientos y esto es debido a una inducción inadecuada por parte del área de Talento Humano.

AAT05. CREACIÓN DE USUARIOS. - En esta actividad se han encontrado los siguientes problemas:

P01. No existe documentación sobre la operativa de las actividades de "TIC".

No existe ninguna documentación de la funcionalidad sobre la creación de usuarios en las aplicaciones y sistemas a las que tienen que acceso los empleados de la Cooperativa, como son: Financial, Facilito, Extreme, Entura, correo electrónico, Portal Corporativo (Intranet), control de asistencia y acceso a la red.

Amenaza. – El desconocer la forma de crear usuarios en las aplicaciones y sistemas, afecta la eficacia y eficiencia de los usuarios, dado que los empleados no pueden acceder a las aplicaciones que necesitan para ejecutar su trabajo diario, eso puede conllevar a desmejorar a atención a los clientes o socios.

Vulnerabilidad. - La operativa de esta actividad es conocido de forma empírica por los actuales funcionarios del Departamento de Tecnología de la Información y Comunicaciones. Si por alguna razón estos colaboradores salen de la institución, nadie más dentro de la Cooperativa podría realizar esta actividad y, por ende, provocar demora en la atención a los clientes o socios, desmejorando la calidad de servicio e incluso causando especulación y malos entendidos respecto a las finanzas de la Cooperativa.

P02. No existe ningún proceso de gestión de eventos y gestión de incidentes.

No existe ningún proceso de gestión de eventos y gestión de incidentes, que permita priorizar la atención inmediata sobre eventos anómalos, amenazas o vulnerabilidades en los sistemas y aplicaciones que se han realizado creación de usuarios para los empleados de COAC “Pedro Moncayo Ltda.”

Amenaza. – Al no existir ningún proceso de gestión de eventos y de incidentes sobre eventos anómalos en la creación de cuentas de usuarios para las aplicaciones y sistemas utilizados por los empleados, la Cooperativa está expuesta a un riesgo inminente de confidencialidad e integridad de la información crítica utilizada por el negocio.

Vulnerabilidad. – La actividad de soporte no posee niveles de atención para resolución de eventos o incidentes operativos y tecnológicos internos (empleados, funcionarios de la Cooperativa) o externos (socios). Tampoco mantiene un proceso de escalamiento para el restablecimiento de servicio con los proveedores, en base a la criticidad, frecuencia e impacto que ayude a erradicar la causa del evento o incidente.

P05. No existe ningún proceso de gestión de solución de problemas.

Cuando los empleados de la Cooperativa tienen problemas con los usuarios creados en las aplicaciones o sistemas a los que acceden para realizar su trabajo diario, no conocen cuál es el soporte que les puede dar el departamento de “TIC” y cómo deben solicitarlo.

Amenaza. – La ausencia de un proceso de gestión de solución de problemas perjudica con la eficacia y eficiencia de los empleados de la Cooperativa, dado que no saben el procedimiento a seguir para solucionar los inconvenientes o problemas que se les presenta con las nuevas credenciales de usuario para las aplicaciones o sistemas a los que requieren acceder por sus actividades y tareas diarias.

Vulnerabilidad. – La inexistencia de un proceso de gestión de solución de problemas puede convertirse en una vulnerabilidad crítica que atenta contra la calidad de servicio que la Cooperativa quiere dar a sus clientes o socios, al desmejorar los tiempos de atención por tener problemas con los usuarios creados en las aplicaciones o sistemas utilizados por los empleados.

P06. No existe ningún proceso de gestión de niveles de servicio.

Tanto el soporte dado por parte del Departamento de Tecnología de la Información y Comunicaciones como el soporte dado por los proveedores de los sistemas y aplicaciones que utilizan los usuarios de la Cooperativa no mantienen un esquema de niveles de acuerdos de servicio que permita tener conocimiento del tiempo de respuesta que se tiene por cada requerimiento realizado de la creación de usuarios, o los niveles de escalamiento necesarios en base a la criticidad del acceso solicitado, o por la calidad de servicio brindado al requerimiento.

Amenaza. – Al no contar con un proceso de gestión de niveles de servicio los empleados y el departamento de “TIC”, no pueden realizar ningún reclamo al proveedor de servicio, ya sea por atención del requerimiento fuera de tiempo o por la calidad de servicio brindado sobre la creación de usuarios en las aplicaciones y sistemas.

Vulnerabilidad. – Al no tener un proceso de gestión de niveles de servicio tanto el departamento de “TIC” como los empleados tienen una alta probabilidad de pérdida de tiempo para la resolución de requerimientos de creación de usuarios, que para el negocio pueden ser vitales y que no son atendidos con la prioridad del caso.

P07. No existe ningún proceso de gestión de proveedores.

La creación de cuentas de usuario para acceso a red y correo electrónico que utiliza COAC “Pedro Moncayo Ltda.”, lo realizan a través de los sistemas administrados por proveedores de servicio, debido a lo cual, se complica al no existir ningún proceso de gestión de proveedores.

Amenaza. – La amenaza inminente es la divulgación de información confidencial a la que las empresas proveedoras tienen acceso cuando realizan la creación de usuarios en los sistemas y aplicaciones que administran como parte del servicio.

Vulnerabilidad. – Al no existir un proceso de gestión de proveedores, la Cooperativa puede estar expuesta a robo, destrucción, uso inadecuado de información confidencial y crítica como son cuentas de usuarios. No se tiene actas de responsabilidad, ni acuerdos de confidencialidad de entrega, manejo y manipulación de información, específicamente de credenciales de usuarios para acceder a las aplicaciones y a los sistemas administrados por los proveedores de servicio.

P08. No existe ningún modelo de seguridad

El Departamento de Tecnología de la Información y Comunicaciones no tiene ningún modelo de seguridad para proteger la información calificada como crítica para la Cooperativa.

Amenaza. – Los empleados de la Cooperativa no tienen una cultura de seguridad respecto al uso de cuentas de usuario, aplicaciones a las que tienen acceso e información crítica manejada y manipulada, de acuerdo a las funciones y actividades que realizan, por lo que la Cooperativa está expuesta a un riesgo inminente de fuga de información, robos o fraudes.

Vulnerabilidad. - A pesar que el Departamento de Tecnología de la Información y Comunicaciones lleva controles respecto a inducción de uso de contraseñas, personaliza credenciales de usuarios para el acceso de aplicaciones y sistemas,

no posee ningún modelo de seguridad que le garantice confidencialidad, integridad y disponibilidad de la información categorizada como crítica.

AAT06. RESETEO DE USUARIOS. - En esta actividad se han encontrado los siguientes problemas:

P01. No existe documentación sobre la operativa de las actividades de "TIC".

No existe ninguna documentación de la funcionalidad sobre el reseteo de cuentas de usuario en las aplicaciones y sistemas a las que tienen que acceso los empleados de la Cooperativa, como son: Financial, Facilito, Extreme, Entura, y acceso a la red.

Amenaza. – El desconocer la forma de resetear usuarios en las aplicaciones y sistemas, afecta a la eficacia y eficiencia de los usuarios, dado que los empleados no pueden acceder a las aplicaciones que necesitan para ejecutar su trabajo diario, eso puede conllevar a desmejorar la atención a los clientes o socios.

Vulnerabilidad. - La operativa de esta actividad es conocido de forma empírica únicamente por los actuales funcionarios del Departamento de Tecnología de la Información y Comunicaciones. Si por alguna razón estos colaboradores salen de la institución, nadie más dentro de la Cooperativa podría realizar esta actividad y, por ende, provocar demora en la atención a los clientes o socios, desmejorando la calidad de servicio.

P02. No existe ningún proceso de gestión de eventos y gestión de incidentes.

No existe ningún proceso de gestión de eventos y gestión de incidentes, que permita priorizar la atención inmediata sobre eventos anómalos, amenazas o vulnerabilidades en los sistemas y aplicaciones en los que han realizado reseteo de claves de usuario sin haber sido solicitadas por los empleados de COAC.

Amenaza. – Al no existir ningún proceso de gestión de eventos y de incidentes sobre eventos anómalos en el reseteo de usuarios de las aplicaciones y sistemas utilizados por los empleados, la Cooperativa está expuesta a un riesgo inminente de confidencialidad e integridad de la información crítica utilizada por el negocio.

Vulnerabilidad. – La actividad de reseteo de contraseñas de usuarios no posee niveles de atención para resolución de eventos o incidentes operativos y tecnológicos internos (empleados, funcionarios de la Cooperativa) o externos (socios). Tampoco mantiene un proceso de escalamiento para el restablecimiento de servicio con los proveedores, en base a la criticidad, frecuencia e impacto que ayude a erradicar la causa del evento o incidente.

P05. No existe ningún proceso de gestión de solución de problemas.

Cuando los empleados de la Cooperativa tienen problemas con las contraseñas de los usuarios con los que acceden a las aplicaciones o sistemas que no son administrados por el área de Tecnología de la Información y Comunicaciones, desconocen la actividad para activar nuevamente sus credenciales.

Amenaza. – La ausencia de un proceso de gestión de solución de problemas perjudica con la eficacia y eficiencia de los empleados de la Cooperativa, dado que no saben el procedimiento a seguir para solucionar los inconvenientes o problemas que se les presenta con las claves de las credenciales de usuario requeridas para acceder a las aplicaciones o sistemas utilizadas para ejecutar sus actividades y tareas diarias.

Vulnerabilidad. – La inexistencia de un proceso de gestión de solución de problemas puede convertirse en una vulnerabilidad crítica que atenta contra la calidad de servicio que la Cooperativa quiere dar a sus clientes o socios, al desmejorar los tiempos de atención por tener problemas con las claves de los usuarios utilizados para acceder a las aplicaciones o sistemas.

P06. No existe ningún proceso de gestión de niveles de servicio.

Tanto el soporte dado por parte del Departamento de Tecnología de la Información y Comunicaciones como el soporte de los proveedores de los sistemas y aplicaciones que utilizan los usuarios de la Cooperativa no mantienen un esquema de niveles de acuerdos de servicio que permita tener conocimiento del tiempo de respuesta que se tiene por cada requerimiento realizado de reseteo de usuarios, o los niveles de escalamiento necesarios en base a la criticidad del acceso solicitado, o por la calidad de servicio brindado al requerimiento.

Amenaza. – Al no contar con un proceso de gestión de niveles de servicio los empleados y el departamento de “TIC”, no pueden realizar ningún reclamo al proveedor de servicio, ya sea por atención del requerimiento fuera de tiempo o por la calidad de servicio brindado sobre el reseteo de usuarios en las aplicaciones y sistemas.

Vulnerabilidad. – Al no tener un proceso de gestión de niveles de servicio tanto el departamento de “TIC” como los empleados tienen una alta probabilidad de pérdida de tiempo para la resolución de requerimientos de reseteo de usuarios, que para el negocio pueden ser vitales y que no son atendidos con la prioridad del caso.

P07. No existe ningún proceso de gestión de proveedores.

El reseteo de usuario para acceso a red y correo electrónico que utiliza COAC “Pedro Moncayo Ltda.”, lo realizan a través de los sistemas administrados por proveedores de servicio, por este motivo, existe un inconveniente al no existir ningún proceso de gestión de proveedores.

Amenaza. – La amenaza inminente es la divulgación de información confidencial a la que las empresas proveedoras tienen acceso cuando realizan el reseteo de usuarios en los sistemas y aplicaciones que administran como parte del servicio.

Vulnerabilidad. – Al no existir un proceso de gestión de proveedores, la Cooperativa puede estar expuesta a robo, destrucción, uso inadecuado de información confidencial y crítica como son cuentas de usuarios. No se tiene actas de responsabilidad, ni acuerdos de confidencialidad de entrega, manejo y manipulación de información, específicamente de credenciales de usuarios para acceder a las aplicaciones y a los sistemas administrados por los proveedores de servicio.

P08. No existe ningún modelo de seguridad

El Departamento de Tecnología de la Información y Comunicaciones no tiene ningún modelo de seguridad para proteger la información calificada como crítica para la Cooperativa.

Amenaza. – Los empleados de la Cooperativa no tienen una cultura de seguridad respecto al uso de cuentas de usuario, aplicaciones a las que tienen acceso e información crítica manejada y manipulada, de acuerdo a las funciones y actividades que realizan, por lo que la Cooperativa está expuesta a un riesgo inminente de fuga de información, robos o fraudes.

Vulnerabilidad. - A pesar que el Departamento de Tecnología de la Información y Comunicaciones lleva controles respecto a inducción de uso de contraseñas, personaliza credenciales de usuarios para el acceso de aplicaciones y sistemas, no posee ningún modelo de seguridad que le garantice confidencialidad, integridad y disponibilidad de la información categorizada como crítica.

P09. No cuentan con una inducción adecuada de los procesos internos

La inducción que reciben los colaboradores de COAC “Pedro Moncayo Ltda.”, relacionado a los accesos a sistemas o aplicaciones no incluye al proceso de resteo de usuarios de las distintas aplicaciones y sistemas existentes en la Cooperativa.

Amenaza. – Existe desconocimiento de las actividades de reseteo de usuarios para acceder a aplicaciones y sistemas existentes en la Cooperativa, lo que provoca inconvenientes para gestionar requerimientos y esto es debido a una inducción inadecuada o incompleta por parte del área de Talento Humano.

AAT07. INACTIVACIÓN DE USUARIOS. - En esta actividad se han encontrado los siguientes problemas:

P01. No existe documentación sobre la operativa de las actividades de “TIC”.

No existe ninguna documentación de la funcionalidad sobre la inactivación de las cuentas de usuario en las aplicaciones y sistemas utilizados por los empleados de la Cooperativa, como son: Financial, Facilito, Extreme, Entura, y acceso a la red.

Amenaza. – El desconocer la forma de inactivar los usuarios en las aplicaciones y sistemas es una amenaza latente que afecta a la seguridad y al cumplimiento de normativas emitidas por los entes de control, dado que las credenciales de usuarios de las aplicaciones y sistemas de empleados que temporalmente no son utilizados o que ya no laboran en la Cooperativa deben ser inactivados y si es el caso eliminados.

Vulnerabilidad. - La operativa de esta actividad es conocido de forma empírica únicamente por los actuales funcionarios del Departamento de Tecnología de la Información y Comunicaciones. Si por alguna razón estos colaboradores salen de la institución, nadie más dentro de la Cooperativa podría realizar esta actividad y, por ende, provocar usos inadecuados con credenciales de usuarios

que temporal o definitivamente no las utilizan y por consecuencia existir fuga de información confidencial, incluso, robos o fraudes económicos.

P02. No existe ningún proceso de gestión de eventos y gestión de incidentes.

No existe ningún proceso de gestión de eventos y gestión de incidentes, que permita priorizar la atención inmediata sobre eventos anómalos, amenazas o vulnerabilidades en los sistemas y aplicaciones en los que han utilizados credenciales de usuarios que deberían estar inactivos por salida temporal o permanente del empleado de COAC.

Amenaza. – Al no existir ningún proceso de gestión de eventos y de incidentes sobre eventos anómalos de usuarios de las aplicaciones y sistemas que deberían estar inactivos y que fueron utilizados por otros funcionarios, la Cooperativa está expuesta a un riesgo inminente a robos, fraudes y fuga de información de confidencial o alteración de la integridad de los datos.

Vulnerabilidad. – La actividad de inactivación de usuarios no posee niveles de atención para resolución de eventos o incidentes operativos y tecnológicos internos (empleados, funcionarios de la Cooperativa) o externos (socios). Tampoco mantiene un proceso de escalamiento con los proveedores de servicio, en base a la criticidad, frecuencia e impacto que ayude a erradicar la causa del evento o incidente.

P05. No existe ningún proceso de gestión de solución de problemas.

Cuando los empleados de la Cooperativa tienen problemas con las contraseñas de los usuarios con los que acceden a las aplicaciones o sistemas que no son administrados por el área de Tecnología de la Información y Comunicaciones, desconocen la actividad para activar nuevamente sus credenciales.

Amenaza. – La ausencia de un proceso de gestión de solución de problemas perjudica con la eficacia y eficiencia de los empleados de la Cooperativa, dado que no saben el procedimiento a seguir para solucionar los inconvenientes o problemas que se les presenta con las claves de las credenciales de usuario requeridas para acceder a las aplicaciones o sistemas utilizadas para ejecutar sus actividades y tareas diarias.

Vulnerabilidad. – La inexistencia de un proceso de gestión de solución de problemas puede convertirse en una vulnerabilidad crítica que atenta contra la calidad de servicio que la Cooperativa quiere dar a sus clientes o socios, al desmejorar los tiempos de atención por tener problemas con las claves de los usuarios utilizados para acceder a las aplicaciones o sistemas.

P06. No existe ningún proceso de gestión de niveles de servicio.

Tanto el soporte dado por parte del Departamento de Tecnología de la Información y Comunicaciones como el soporte dado por los proveedores de los sistemas y aplicaciones que utilizan los usuarios de la Cooperativa no mantienen un esquema de niveles de acuerdos de servicio que permita tener conocimiento del tiempo de respuesta que se tiene por cada requerimiento realizado de reseteo de usuarios, o los niveles de escalamiento necesarios en base a la criticidad del acceso solicitado, o por la calidad de servicio brindado al requerimiento.

Amenaza. – Al no contar con un proceso de gestión de niveles de servicio los empleados y el departamento de “TIC”, no pueden realizar ningún reclamo al proveedor de servicio, ya sea por atención del requerimiento fuera de tiempo o por la calidad de servicio brindado sobre el reseteo de usuarios en las aplicaciones y sistemas.

Vulnerabilidad. – Al no tener un proceso de gestión de niveles de servicio tanto el departamento de “TIC” como los empleados tienen una alta probabilidad de

pérdida de tiempo para la resolución de requerimientos de reseteo de usuarios, que para el negocio pueden ser vitales y que no son atendidos con la prioridad del caso.

P07. No existe ningún proceso de gestión de proveedores.

El reseteo de usuario para acceso a red y correo electrónico que utiliza COAC “Pedro Moncayo Ltda.”, lo realizan a través de los sistemas administrados por proveedores de servicio, por este motivo, existe un inconveniente al no existir ningún proceso de gestión de proveedores.

Amenaza. – La amenaza inminente es la divulgación de información confidencial a la que las empresas proveedoras tienen acceso cuando realizan el reseteo de usuarios en los sistemas y aplicaciones que administran como parte del servicio.

Vulnerabilidad. – Al no existir un proceso de gestión de proveedores, la Cooperativa puede estar expuesta a robo, destrucción, uso inadecuado de información confidencial y crítica como son cuentas de usuarios. No se tiene actas de responsabilidad, ni acuerdos de confidencialidad de entrega, manejo y manipulación de información, específicamente de credenciales de usuarios para acceder a las aplicaciones y a los sistemas administrados por los proveedores de servicio.

P08. No existe ningún modelo de seguridad

El Departamento de Tecnología de la Información y Comunicaciones no tiene ningún modelo de seguridad para proteger la información calificada como crítica para la Cooperativa.

Amenaza. – Los empleados de la Cooperativa no tienen una cultura de seguridad respecto al uso de cuentas de usuario, aplicaciones a las que tienen acceso e información crítica manejada y manipulada, de acuerdo a las funciones y

actividades que realizan, por lo que la Cooperativa está expuesta a un riesgo inminente de fuga de información, robos o fraudes.

Vulnerabilidad. - A pesar que el Departamento de Tecnología de la Información y Comunicaciones lleva controles respecto a inducción de uso de contraseñas, personaliza credenciales de usuarios para el acceso de aplicaciones y sistemas, no posee ningún modelo de seguridad que le garantice confidencialidad, integridad y disponibilidad de la información categorizada como crítica.

P09. No cuentan con una inducción adecuada de los procesos internos

La inducción que reciben los colaboradores de COAC “Pedro Moncayo Ltda.”, relacionado a los accesos a sistemas o aplicaciones no incluye al proceso de resteo de usuarios de las distintas aplicaciones y sistemas existentes en la Cooperativa.

Amenaza. – Existe desconocimiento de las actividades de reseteo de usuarios para acceder a aplicaciones y sistemas existentes en la Cooperativa, lo que provoca inconvenientes para gestionar requerimientos y esto es debido a una inducción inadecuada o incompleta por parte del área de Talento Humano.

AAT08. CONFIGURACIÓN. - En esta actividad se han encontrado los siguientes problemas:

P01. No existe documentación sobre la operativa de las actividades de “TIC”.

No existe ninguna documentación sobre la configuración de: puntos de red y asignación de direcciones lógicas (direcciones IPs), accesos a la red, sistemas como: control de asistencia, pin pad, equipos computacionales, cuentas de correo electrónico y perfilamiento de usuarios por cargo.

Amenaza. – El desconocer la forma de configurar los computadores, servidores, dispositivos de comunicación, creación de puntos de red, asignación de direcciones lógicas y sistemas de control, afecta a la calidad de servicio que los empleados y socios o clientes esperan del departamento de “TIC”, que incluso puede provocar demoras en la atención al público.

Vulnerabilidad. - El conocimiento del flujo y la operativa de esta actividad solamente poseen los actuales funcionarios del Departamento de Tecnología de la Información y Comunicaciones de forma empírica. Si por alguna razón estos colaboradores salen de la institución, existe una alta probabilidad de que nadie pueda realizar las diferentes configuraciones en computadores, servidores, puntos de red y sistemas de control y acceso, lo que provocaría que la atención a los clientes o socios se vea impactada.

P02. No existe ningún proceso de gestión de eventos y gestión de incidentes.

No existe ningún proceso de gestión de eventos y gestión de incidentes, que permita priorizar la atención inmediata sobre eventos anómalos, amenazas o vulnerabilidades en la configuración de los sistemas de control y acceso, así de creación de nuevos puntos de red, o computadores y servidores utilizados por los empleados de COAC “Pedro Moncayo Ltda.”

Amenaza. – Al no existir ningún proceso de gestión de eventos y de incidentes sobre fallas o eventos anómalos durante la configuración de computadores, servidores y sistemas de control y accesos utilizados por los empleados, la Cooperativa está expuesta a un riesgo inminente de pérdida de confiabilidad por la demora en la atención a los clientes o socios causando mal estar y especulaciones, que podría ocasionar pérdida de la reputación corporativa.

Vulnerabilidad. – La actividad de configuración no posee niveles de atención para resolución de eventos o incidentes operativos y tecnológicos internos (empleados, funcionarios de la Cooperativa).

P05. No existe ningún proceso de gestión de solución de problemas.

Cuando los empleados de la Cooperativa tienen problemas con los computadores, sistemas de control y acceso respecto a las configuraciones, que no son administrados por el área de Tecnología de la Información y Comunicaciones, desconocen la actividad para solventar los problemas.

Amenaza. – La ausencia de un proceso de gestión de solución de problemas perjudica con la eficacia y eficiencia de los empleados de la Cooperativa, dado que no saben el procedimiento a seguir para solucionar los inconvenientes o problemas que se les presenta con las configuraciones de sus computadores o sistemas de control y accesos necesarios para ejecutar sus actividades y tareas diarias.

Vulnerabilidad. – La inexistencia de un proceso de gestión de solución de problemas puede convertirse en una vulnerabilidad crítica que atenta contra la calidad de servicio que la Cooperativa quiere dar a sus clientes o socios, al desmejorar los tiempos de atención por tener problemas con los computadores, puntos de red, asignación de direcciones lógicas, correo electrónico, sistema pin pad requeridos para acceder a las aplicaciones.

P06. No existe ningún proceso de gestión de niveles de servicio.

La actividad de configuración de computadores, servidores y sistemas de control y acceso por parte del Departamento de Tecnología de la Información y Comunicaciones, no mantiene un esquema de niveles de acuerdos de servicio, especialmente sobre el tiempo de respuesta que se necesita para cada requerimiento, o los niveles de escalamiento necesarios en base a la criticidad del problema.

Amenaza. – Al no contar con un proceso de gestión de niveles de servicio los empleados no pueden realizar ningún reclamo al departamento de “TIC”, ya sea

por atención del requerimiento fuera de tiempo o por la calidad de servicio brindado.

Vulnerabilidad. – Tanto el departamento de “TIC” como los empleados tienen una alta probabilidad de pérdida de tiempo para la resolución de requerimientos, debido a la falta de un proceso de gestión de niveles de servicio, que les permita dar prioridad a la configuración de computadores, servidores y sistemas de control y accesos de acuerdo a la criticidad que éstas representan dentro del negocio.

P07. No existe ningún proceso de gestión de proveedores.

El correo electrónico que utiliza COAC “Pedro Moncayo Ltda.”, lo realiza a través de los sistemas administrados por proveedores de servicio, por este motivo, existe un inconveniente al no existir ningún proceso de gestión de proveedores.

Amenaza. – La amenaza inminente es la divulgación de información confidencial a la que las empresas proveedoras tienen acceso cuando realizan configuraciones de sistemas, dispositivos de comunicación, entre otros, que administran como parte del servicio.

Vulnerabilidad. – Al no existir un proceso de gestión de proveedores, la Cooperativa puede estar expuesta a robo, destrucción, uso inadecuado de información confidencial y crítica como son cuentas de usuarios con máximos privilegios y especialmente acceso a toda la infraestructura de red. No se tiene actas de responsabilidad, ni acuerdos de confidencialidad de entrega, manejo y manipulación de información, específicamente de credenciales de usuarios administradores para acceder a las aplicaciones y a los sistemas.

P08. No existe modelo de seguridad

El Departamento de Tecnología de la Información y Comunicaciones no tiene ningún modelo de seguridad para proteger la información calificada como crítica para la Cooperativa.

Amenaza. – La confidencialidad, integridad y disponibilidad de los activos de la información de COAC “Pedro Moncayo Ltda.” se encuentran amenazados, cuando se realizan configuraciones incorrectas, lo que supone un riesgo inminente de fuga de información, robos o fraudes.

Vulnerabilidad. - A pesar que el Departamento de Tecnología de la Información y Comunicaciones lleva controles respecto a inducción de uso de contraseñas, personaliza credenciales de usuarios para el acceso de aplicaciones y sistemas, no posee ningún modelo de seguridad que le garantice confidencialidad, integridad y disponibilidad de los sistemas y de la información categorizada como crítica.

AAT09. SOPORTE APLICACIÒN / INFRAESTRUCTURA. - En esta actividad se han encontrado los siguientes problemas:

P01. No existe documentación sobre la operativa de las actividades de “TIC”.

No existe ninguna documentación sobre los pasos a seguir para respaldar la base de datos del Core Financiero, cierre de fin de día, acreditación mensual de intereses, respaldos de los computadores, respaldos de la información de los sistemas de cámaras de seguridad y de control de asistencia y actualización de parches.

Amenaza. – El desconocer la forma de realizar las tareas para dar soporte a las aplicaciones e infraestructura, afecta a la calidad de servicio que los empleados y socios o clientes esperan del departamento de “TIC”, que incluso puede provocar indisponibilidad de los servicios.

Vulnerabilidad. - El conocimiento del flujo y la operativa de esta actividad solamente poseen los actuales funcionarios del Departamento de Tecnología de la Información y Comunicaciones de forma empírica. Si por alguna razón estos colaboradores salen de la institución, existe una alta probabilidad de que nadie pueda realizar las diferentes actividades requeridas para dar soporte a las aplicaciones e infraestructura, lo que provocaría indisponibilidad de los sistemas e incluso alteración de la información crítica para el negocio.

P02. No existe ningún proceso de gestión de eventos y gestión de incidentes.

No existe ningún proceso de gestión de eventos y gestión de incidentes, que permita priorizar la atención inmediata sobre eventos anómalos, amenazas o vulnerabilidades en las actividades de funcionalidad requeridas por las aplicaciones e infraestructura de la red utilizados por los empleados de COAC “Pedro Moncayo Ltda.”

Amenaza. – Al no existir ningún proceso de gestión de eventos y de incidentes sobre fallas o eventos anómalos durante el soporte de aplicaciones e infraestructura de red utilizados por los empleados, la Cooperativa está expuesta a un riesgo inminente de pérdida de disponibilidad e integridad, a más de cumplimiento de las leyes y normativas de LOEPS, causando mal estar y especulaciones, que podría ocasionar pérdida de la reputación corporativa.

Vulnerabilidad. – La actividad de soporte de aplicaciones e infraestructura no posee niveles de atención para resolución de eventos o incidentes operativos y tecnológicos internos (empleados, funcionarios de la Cooperativa).

P03. No existe un proceso de custodia de información.

Una de las actividades a realizar dentro del soporte de aplicaciones e infraestructura, es obtener respaldos de la información de la base de datos, aplicaciones y computadores, sin embargo, el lugar de almacenamiento de estos

respaldos es en los cajones de los escritorios ubicados en el departamento de “TIC”.

Vulnerabilidad. – Los activos de información que se obtienen principalmente de la base de datos del core financiero, sistemas y computadores personales son primordiales para el negocio. Al no contar con un proceso de custodia adecuado, existe la posibilidad de que se pierdan los repositorios o que se dañen, y al momento que se requiera no van a estar disponibles, lo que puede ocasionar problemas legales con los entes de control, así como con los socios o clientes de la COAC; además, de pérdidas económicas y de reputación.

P04. No existe un proceso de restauración de base de datos.

A pesar de que existe la actividad para respaldar la base de datos del Core Financiero “Financial” y sistemas no existe ningún proceso formal para restaurar ésta y las otras bases de datos de las aplicaciones existentes en la Cooperativa.

Amenaza. – Si los activos de información obtenidos de los respaldos de las bases de datos y sistemas, no son válidos, pueden ocasionar pérdida de información de clientes o socios, así como de la transaccionalidad de la Cooperativa.

Vulnerabilidad. – Al no tener un proceso formal de restauración de la información que se extrajo de las bases de datos y sistemas, existe la posibilidad de que los datos no guarden la integridad requerida y esto ocasione problemas legales con los entes de control, con los socios o clientes, con los proveedores, entre otros de la Cooperativa.

P05. No existe ningún proceso de gestión de solución de problemas.

Cuando los empleados de la Cooperativa tienen problemas con los computadores, respaldos de bases de datos o sistemas de control y acceso, que

no son administrados por el área de Tecnología de la Información y Comunicaciones, no pueden solventar los problemas.

Amenaza. – La ausencia de un proceso de gestión de solución de problemas perjudica a la disponibilidad de los sistemas y a la integridad de los activos de información de la aplicación principal de la Cooperativa, dado que no saben el procedimiento a seguir para solucionar los inconvenientes o problemas que se les presenta en estas actividades.

Vulnerabilidad. – La inexistencia de un proceso de gestión de solución de problemas puede convertirse en una vulnerabilidad crítica sobre la disponibilidad de los sistemas utilizados en la Cooperativa.

P06. No existe ningún proceso de gestión de niveles de servicio.

La actividad de soporte de aplicaciones e infraestructura, no mantiene un esquema de niveles de acuerdos de servicio, especialmente sobre el tiempo de respuesta que se necesita para cada requerimiento, o los niveles de escalamiento necesarios en base a la criticidad del problema.
Amenaza. – Al no contar con un proceso de gestión de niveles de servicio los empleados no pueden realizar ningún reclamo al departamento de “TIC”, ya sea por atención del requerimiento fuera de tiempo o por la calidad de servicio brindado.

Vulnerabilidad. – Tanto el departamento de “TIC” como los empleados tienen una alta probabilidad de pérdida de tiempo para la resolución de requerimientos, debido a la falta de un proceso de gestión de niveles de servicio, que les permita dar prioridad a las actividades necesarias para el soporte a aplicaciones e infraestructura de acuerdo a la criticidad que éstas representan dentro del negocio.

P07. No existe ningún proceso de gestión de proveedores.

Las aplicaciones y sistemas que utiliza COAC “Pedro Moncayo Ltda.”, lo realiza a través de los sistemas administrados por proveedores de servicio, por este motivo, existe un inconveniente al no existir ningún proceso de gestión de proveedores.

Amenaza. – La amenaza inminente es la divulgación de información confidencial a la que las empresas proveedoras tienen acceso a las aplicaciones y sistemas, que administran como parte del servicio.

Vulnerabilidad. – Al no existir un proceso de gestión de proveedores, la Cooperativa puede estar expuesta a indisponibilidad de los sistemas, además de uso inadecuado de información confidencial y crítica como son cuentas de usuarios con máximos privilegios y especialmente acceso a toda la infraestructura de red. No se tiene actas de responsabilidad, ni acuerdos de confidencialidad de entrega, manejo y manipulación de información, específicamente de credenciales de usuarios administradores para acceder a las aplicaciones y a los sistemas.

P08. No existe ningún modelo de seguridad

El Departamento de Tecnología de la Información y Comunicaciones no tiene ningún modelo de seguridad para proteger la disponibilidad de los sistemas considerados como críticos para la Cooperativa.

Amenaza. – La integridad y disponibilidad de los sistemas de COAC “Pedro Moncayo Ltda.” se encuentran amenazados, cuando no se cuenta con los procesos adecuados para asegurad los activos de la información.

Vulnerabilidad. - El Departamento de Tecnología de la Información y Comunicaciones, no posee ningún modelo de seguridad que le garantice la

integridad de la información crítica para el negocio y la disponibilidad de los sistemas.

AAT10. PROVEEDORES. - En esta actividad se han encontrado los siguientes problemas:

P02. No existe ningún proceso de gestión de eventos y gestión de incidentes.

No existe ningún proceso de gestión de eventos y gestión de incidentes, que permita priorizar la atención inmediata sobre eventos anómalos, amenazas o vulnerabilidades en las aplicaciones y sistemas administradas por los proveedores de servicios utilizados por los empleados de COAC “Pedro Moncayo Ltda.”

Amenaza. – Al no existir ningún proceso de gestión de eventos y de incidentes sobre fallas o eventos anómalos de las aplicaciones y sistemas administrados por los proveedores de servicio utilizados por los empleados, la Cooperativa está expuesta a un riesgo inminente de confidencialidad, disponibilidad de los sistemas e integridad, a más de cumplimiento de las leyes y normativas de LOEPS, causando mal estar y especulaciones, que podría ocasionar pérdida de la reputación corporativa.

Vulnerabilidad. – La actividad de proveedores no posee niveles de atención para resolución de eventos o incidentes operativos y tecnológicos externos.

P06. No existe ningún proceso de gestión de niveles de servicio.

La actividad de proveedores, no mantiene un esquema de niveles de acuerdos de servicio, especialmente sobre el tiempo de respuesta que se necesita para cada requerimiento, o los niveles de escalamiento necesarios en base a la criticidad del problema.

Amenaza. – Al no contar con un proceso de gestión de niveles de servicio los empleados no pueden realizar ningún reclamo al departamento de “TIC”, ya sea por atención del requerimiento fuera de tiempo o por la calidad de servicio brindado.

Vulnerabilidad. – Tanto el departamento de “TIC” como los empleados tienen una alta probabilidad de pérdida de tiempo para la resolución de requerimientos, debido a la falta de un proceso de gestión de niveles de servicio, que les permita dar prioridad a las aplicaciones y sistemas administrados por los proveedores de servicio de acuerdo a la criticidad que éstas representan dentro del negocio.

P07. No existe ningún proceso de gestión de proveedores.

Las aplicaciones y sistemas que utiliza COAC “Pedro Moncayo Ltda.”, lo realiza a través de los sistemas administrados por proveedores de servicio, por este motivo, existe un inconveniente al no existir ningún proceso de gestión de proveedores.

Amenaza. – La amenaza inminente es la divulgación de información confidencial y la indisponibilidad de los sistemas a lo que las empresas proveedoras tienen acceso porque administran como parte del servicio.

Vulnerabilidad. – Al no existir un proceso de gestión de proveedores, la Cooperativa puede estar expuesta a indisponibilidad de los sistemas. Además, de uso inadecuado de información confidencial y crítica como son cuentas de usuarios con máximos privilegios y especialmente acceso a toda la infraestructura de red. No se tiene actas de responsabilidad, ni acuerdos de confidencialidad de entrega, manejo y manipulación de información, específicamente de credenciales de usuarios administradores para acceder a las aplicaciones y a los sistemas.

P08. No existe ningún modelo de seguridad

El Departamento de Tecnología de la Información y Comunicaciones no tiene ningún modelo de seguridad para proteger la disponibilidad de los sistemas, la integridad y confidencialidad de los activos de información considerados como críticos para la Cooperativa.

Amenaza. – La confidencialidad, integridad y disponibilidad de los sistemas de COAC "Pedro Moncayo Ltda." se encuentran amenazados, cuando no se cuenta con los controles adecuados sobre los activos de la información.

Vulnerabilidad. - El Departamento de Tecnología de la Información y Comunicaciones, no posee ningún modelo de seguridad que le garantice la confidencialidad, integridad de la información crítica para el negocio y la disponibilidad de los sistemas.

AAT11. REQUERIMIENTOS. - En esta actividad se han encontrado los siguientes problemas:

P06. No existe ningún proceso de gestión de niveles de servicio.

La actividad de soporte de aplicaciones e infraestructura, no mantiene un esquema de niveles de acuerdos de servicio, especialmente sobre el tiempo de respuesta que se necesita para cada requerimiento, o los niveles de escalamiento necesarios en base a la criticidad del problema.

Amenaza. – Al no contar con un proceso de gestión de niveles de servicio las áreas solicitantes de la Cooperativa no pueden realizar ningún reclamo al departamento de "TIC", ya sea por atención del requerimiento fuera de tiempo o por la calidad de servicio brindado.

Vulnerabilidad. – Tanto el departamento de "TIC" como las áreas del negocio solicitantes tienen una alta probabilidad de pérdida de tiempo para la resolución

de requerimientos, debido a la falta de un proceso de gestión de niveles de servicio, que les permita dar prioridad a las actividades necesarias para el soporte a aplicaciones e infraestructura de acuerdo a la criticidad que éstas representan para la Cooperativa.

P07. No existe ningún proceso de gestión de proveedores.

Los requerimientos para crear nuevas páginas del intranet institucional, nuevas funcionalidades y reportes dentro de la aplicación Financial, se los realiza a través de proveedores de servicio, por este motivo, existe un inconveniente al no haber ningún proceso de gestión de proveedores.

Amenaza. – La amenaza inminente es la divulgación de información confidencial a la que las empresas proveedoras tienen acceso a las aplicaciones y sistemas, que administran como parte del servicio.

Vulnerabilidad. – En la actividad de proveedores, el departamento de “TIC” no exige actas de responsabilidad, ni acuerdos de confidencialidad de entrega, manejo y manipulación de información, específicamente de credenciales de usuarios administradores para acceder a las aplicaciones y a los sistemas.

P08. No existe ningún modelo de seguridad

El Departamento de Tecnología de la Información y Comunicaciones no tiene ningún modelo de seguridad para proteger la disponibilidad de los sistemas y que se ajusten a las normativas o leyes emitidos por los entes de control, en caso de requerir modificaciones en los sistemas o aplicaciones.

Amenaza. – La confidencialidad e integridad de la información crítica de COAC “Pedro Moncayo Ltda.” se podrían ver amenazados, por fuga, divulgación o uso indebido de información crítica para el negocio.

Vulnerabilidad. - El Departamento de Tecnología de la Información y Comunicaciones, no posee ningún modelo de seguridad que le garantice la confidencialidad e integridad de la información crítica para el negocio con los proveedores de servicio.

4.2.2 Descripción del impacto o consecuencia

Para la descripción del impacto de riesgos, se utilizará la técnica “Metas del Negocio en COBIT y Balanced Scorecard, BSC”, (The Risk IT Practitioner Guide, 2009), dado que es el mismo que está empleado dentro del Plan Estratégico de la Cooperativa de Ahorro y Crédito “Pedro Moncayo Ltda.”. El “BSC”, será aplicado, específicamente dentro de las actividades actuales del área de Tecnología de la Información y Comunicaciones, tomando en cuenta los problemas identificados y en base a las “perspectivas clásicas del Cuadro de Mando Integral (BSC), que a continuación se indican: financiera, clientes, interna y aprendizaje y crecimiento”. (pág. 36)

4.2.2.1 Perspectiva Financiera

- “Mejorar el desempeño financiero de la Cooperativa” (02 Plan estratégico PM 2015 2017, 2016)

Impacto del Negocio. – Se han identificado varias vulnerabilidades y amenazas de los problemas encontrados en el departamento de “TIC” que impedirían cumplir con este objetivo estratégico, como es:

Pérdida económica por indisponibilidad del servicio provocada por falla en los sistemas tecnológicos causado porque:

- P02. No existe ningún proceso de gestión de eventos y gestión de incidentes, que ayude a identificar eventos anómalos o fallas tecnológicas u operativas en los sistemas o aplicaciones críticas para el negocio.

- P05. No existe ningún proceso de gestión de solución de problemas, que resuelva los problemas técnicos y operativos antes de que se conviertan en incidentes tecnológicos.
- P06. No existe ningún proceso de gestión de niveles de servicio, que ayude a priorizar los requerimientos críticos para que sean atendidos de inmediato.
- P07. No existe ningún proceso de gestión de proveedores, que ayude a proteger a la Cooperativa de uso inadecuado de información considera como crítica para el negocio.
- P08. No existe ningún modelo de seguridad, que ayude a proteger la confidencialidad, integridad y disponibilidad de los activos de la información de COAC “Pedro Moncayo Ltda.”

4.2.2.2 Perspectiva Clientes

- “Mejorar el nivel de satisfacción de socios y clientes” (02 Plan estratégico PM 2015 2017, 2016)

Impacto del Negocio. – Dentro de la visión y misión de la Cooperativa se encuentra este objetivo estratégico, sin embargo, las vulnerabilidades y amenazas encontradas en las actividades actuales del departamento de “TIC”, pueden provocar:

Pérdida de confiabilidad en los clientes o socios debido a lentitud en la atención y desmejoramiento de la calidad de servicio causado porque:

- P02. No existe ningún proceso de gestión de eventos y gestión de incidentes, que ayude a dar soporte a eventos anómalos o fallas técnicas y operativas de usuarios, sistemas y aplicaciones.
- P05. No existe ningún proceso de gestión de solución de problemas, que ayude a resolver de inmediato problemas en los accesos de las aplicaciones o sistemas requeridos por los empleados de la Cooperativa.

- P06. No existe ningún proceso de gestión de niveles de servicio, que ayude a atender los requerimientos realizados por los empleados tanto al departamento de “TIC” como a los proveedores de servicio.
- P07. No existe ningún proceso de gestión de proveedores, que permita garantizar que los sistemas y aplicaciones administrados por ellos, estén disponibles, libres de intermitencias o interrupciones.
- P08. No existe ningún modelo de seguridad, que garantice a los clientes o socios que su información está manejada con confidencialidad e itegridad.

4.2.2.3 Perspectiva Interna

- “Lograr el cumplimiento de los proyectos de fortalecimiento organizacional” (02 Plan estratégico PM 2015 2017, 2016)

Impacto del Negocio. – Las vulnerabilidades y amenazas encontrados en las actividades actuales del departamento de “TIC”, pueden provocar que esta meta estratégica no sea cumplida por:

Pérdida de eficiencia y eficacia de los empleados de la Cooperativa y por incumplimiento a las normativas emitidas por los entes de control debido a desconocimiento de actividades tecnológicas y presencia de eventos anómalos en los sistemas o aplicaciones, causado porque:

- P01. No existe documentación sobre la operativa de las actividades de “TIC”, y en caso de que los actuales funcionarios del Departamento de Tecnología de la Información y Comunicaciones salgan de la Cooperativa, ningún otro empleado tiene el conocimiento de estos procesos.
- P02. No existe ningún proceso de gestión de eventos y gestión de incidentes, que ayude a dar soporte a eventos anómalos o fallas técnicas y operativas de usuarios, sistemas y aplicaciones.

- P03. No existe un proceso de custodia de información, que son respaldos de información de los clientes o socios, que de acuerdo a la normativa se deben conservar en base a lo indicado en el LOEPS.
- P04. No existe un proceso de restauración de base de datos, que se necesita en caso de que haya pérdida de información crítica.
- P05. No existe ningún proceso de gestión de solución de problemas, que ayude a resolver de inmediato problemas en los accesos de las aplicaciones o sistemas requeridos por los empleados de la Cooperativa.
- P06. No existe ningún proceso de gestión de niveles de servicio, que ayude a atender los requerimientos realizados por los empleados tanto al departamento de "TIC" como a los proveedores de servicio.
- P07. No existe ningún proceso de gestión de proveedores, que permita garantizar que los sistemas y aplicaciones administrados por ellos, estén disponibles, libres de intermitencias o interrupciones.
- P08. No existe ningún modelo de seguridad, que garantice a los clientes o socios que su información está manejada con confidencialidad e integridad.

4.2.2.4 Perspectiva Aprendizaje y Crecimiento

- "Mejorar el desempeño del talento humano" (02 Plan estratégico PM 2015 2017, 2016)

Impacto del Negocio. – Los empleados de la Cooperativa tienen inconvenientes sobre las actividades tecnológicas que tienen que realizar para solicitar, utilizar y acceder a los sistemas o aplicaciones que requieren para realizar su trabajo diario. Esto es provocado por:

Falta de programas de capacitación o inducción de procesos de gestión de accesos y usuarios de sistemas y aplicaciones. La causa es porque:

- P09. No cuentan con una inducción adecuada de los procesos internos

➢ “Fortalecer la gestión de Tecnología de la Información y Comunicaciones” (02 Plan estratégico PM 2015 2017, 2016)

Impacto del Negocio. – Las actividades actuales que ejecuta el departamento de “TIC”, no se encuentran establecidos como servicios, lo que dificulta cumplir con la meta estratégica planteada. Esto es provocado porque:

No se encuentran implementados servicios tecnológicos que permitan robustecer el departamento de “TIC”, causado porque:

- P01. No existe documentación sobre la operación de las actividades de “TIC”.
- P02. No existe ningún proceso de gestión de eventos y gestión de ncidentes.
- P03. No existe un proceso de custodia de información.
- P04. No existe un proceso de restauración de base de datos.
- P05. No existe ningún proceso de gestión de solución de problemas.
- P06. No existe ningún proceso de gestión de niveles de servicio.
- P07. No existe ningún proceso de gestión de proveedores.
- P08. No existe ningún modelo de seguridad

En base a las perspectivas del “BSC” aplicadas a las metas estratégicas de la Cooperativa se ha podido establecer que las consecuencias o impactos del negocio son:

- Pérdida económica por indisponibilidad del servicio provocada por falla en los sistemas tecnológicos, los criterios de información de COBIT que se ajustan son: la eficacia, eficiencia y disponibilidad.

- Pérdida de confiabilidad en los clientes o socios debido a lentitud en la atención y desmejoramiento de la calidad de servicio, se ajustan todos los

criterios de información COBIT y son: eficacia, eficiencia, confiabilidad, integridad, disponibilidad, cumplimiento, confiabilidad

- Pérdida de eficiencia y eficacia de los empleados de la Cooperativa y por incumplimiento a las normativas emitidas por los entes de control debido a desconocimiento de actividades tecnológicas y presencia de eventos anómalos en los sistemas o aplicaciones. Los criterios de información COBIT, también son todos: eficacia, eficiencia, confiabilidad, integridad, disponibilidad, cumplimiento, confiabilidad.

- Falta de programas de capacitación o inducción de procesos de gestión de accesos y usuarios de sistemas y aplicaciones. Los criterios que se ajustan son: eficacia y eficiencia

- No se encuentran implementados servicios tecnológicos que permitan robustecer el departamento de “TIC”, los criterios son: eficacia, eficiencia, confiabilidad, integridad, disponibilidad, cumplimiento, confiabilidad.

En la siguiente tabla, se resumen las metas estratégicas o metas del negocio planteadas por la Cooperativa indicadas en el Plan Estratégico (Cooperativa de Ahorro y Crédito Pedro Moncayo Ltda., 2016) con cada uno de los impactos identificados en base a los problemas encontrados en el Departamento de “TIC”, siguiendo la metodología indicada en “The Risk IT Practitioner Guide” (ISACA, 2009, pág. 44)

Tabla 22.

Metas Estratégicas vs. Impactos del Negocio

Metas Estratégicas e Impacto del Negocio	
Metas del Negocio	**Impacto del Negocio**
Perspectiva Financiera	
Mejorar el desempeño financiero de la Cooperativa.	Pérdida económica por indisponibilidad del servicio provocada por falla en los sistemas tecnológicos
Perspectiva de los Clientes	
Mejorar el nivel de satisfacción de socios y clientes.	Pérdida de confiabilidad en los clientes o socios debido a lentitud en la atención y desmejoramiento de la calidad de servicio
Perspectiva Interna	
Lograr el cumplimiento de los proyectos de fortalecimiento organizacional.	Pérdida de eficiencia y eficacia de los empleados de la Cooperativa y por incumplimiento a las normativas emitidas por los entes de control debido a desconocimiento de actividades tecnológicas y presencia de eventos anómalos en los sistemas o aplicaciones
Perspectiva de Aprendizaje y Crecimiento	
Mejorar el desempeño del talento humano.	Falta de programas de capacitación o inducción de procesos de gestión de accesos y usuarios de sistemas y aplicaciones

Fortalecer la gestión de Tecnología de la Información y Comunicaciones.	No se encuentran implementados servicios tecnológicos que permitan robustecer el departamento de “TIC”

Adaptado de The Risk IT Practitioner Guide (ISACA, 2009, pág. 44)

4.2.3 Criterios para evaluar el impacto o consecuencia

Luego de esta evaluación del impacto o consecuencia de las metas del negocio, se utilizará los criterios de información de COBIT correspondientes a la técnica de Balanced Scorecard, para identificar el riesgo asociado a las metas estratégicas de la Cooperativa.

En la Tabla 23 – Metas / Impactos del Negocio y Criterios de Información COBIT, en la columna “Impacto del Negocio”, se encuentran los riesgos identificados en cada una de las perspectivas: financiera, clientes, interna y de aprendizaje.

Estos impactos del negocio, están marcados con una letra “P”, cuya nomenclatura significa principal, en cada uno de los criterios a los que afecte el riesgo, caso contrario, se deja en blanco.

Tabla 23.

Metas / Impactos del Negocio y Criterios de Información COBIT

Metas / Impactos del Negocio y Criterios de Información COBIT							
Impacto del Negocio	Criterios de Información COBIT						
	Eficacia	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
Perspectiva Financiera							
Pérdida económica por indisponibilidad del servicio provocada por falla en los sistemas tecnológicos	P	P			P		
Perspectiva Clientes							
Pérdida de confiabilidad en los clientes o socios debido a lentitud en la atención y desmejoramiento de la calidad de servicio	P	P	P	P	P	P	P
Perspectiva Interna							

Pérdida de eficiencia y eficacia de los empleados de la Cooperativa y por incumplimiento a las normativas emitidas por los entes de control debido a desconocimiento de actividades tecnológicas y presencia de eventos anómalos en los sistemas o aplicaciones	P	P	P	P	P	P	P
Perspectiva de Aprendizaje y Crecimiento							
Falta de programas de capacitación o inducción de procesos de gestión de accesos y usuarios de sistemas y aplicaciones	P	P					
No se encuentran implementados servicios tecnológicos que permitan robustecer el departamento de "TIC"	P	P	P	P	P	P	P

Adaptado de The Risk IT Practitioner Guide (ISACA, 2009, pág. 45)

4.3 Escenarios de Riesgos

De acuerdo a la metodología explicada en el capítulo II de la presente tesis, se ha efectuado este levantamiento de información, los funcionarios responsables de cada una de las áreas que son parte de los procesos de operación del negocio, en la cadena de valor, están conscientes del riesgo inherente que implica el tener el conocimiento directo de los procesos del negocio de forma empírica, no documentada.

A continuación, se describe las principales causas por las cuales, los riesgos identificados pueden tener un gran impacto a la operación del negocio:

- No existe un área que proporcione y defina los lineamientos y estándares de los procesos de operación, negocio y tecnología que cada departamento debe cumplir.

- A pesar de que el departamento de “TIC”, es imprescindible para cada área de la Cooperativa, especialmente las áreas de Operaciones y Negocio, que dependen siempre de este departamento para el lanzamiento de nuevos productos y servicios, no está dentro de la cadena de valor como proceso de operación, sino más bien como proceso de apoyo y soporta, lo que impide que muchos de sus requerimientos sean suspendidos por no ser prioritarios.

En cuanto al departamento de “TIC”, se identificaron amenazas, vulnerabilidades y problemas en las actividades actuales, especialmente la vulnerabilidad más crítica consiste también, en que el conocimiento directo de las actividades TI lo tiene únicamente el Jefe de Sistemas y de forma práctica; en otras palabras, no existe ninguna documentación procedimental y de instrucciones paso a paso de la operación de este departamento.

Para realizar el análisis de riesgos identificados, se ha tomado como base los 9 problemas evidenciados en el Departamento de “TIC” que afectan directamente

a la operación de COAC “Pedro Moncayo Ltda.”, y que a continuación, se indican en la siguiente tabla:

Tabla 24.

Riesgos Identificados por Problemas TI

CÓD. RIESGO	RIESGO	PROBLEMA TI
R1	Pérdida económica por indisponibilidad del servicio provocada por falla en los sistemas tecnológicos	P01. No existe documentación sobre la operación de las actividades de “TIC”. P02. No existe ninguna actividad de gestión de eventos y gestión de incidentes. P03. No existe ninguna actividad de custodia de información. P04. No existe ninguna actividad de restauración de base de datos. P05. No existe ninguna actividad de gestión de solución de problemas. P06. No existe ninguna actividad de gestión de niveles de servicio. P07. No existe ninguna actividad de gestión de proveedores. P08. No existe ninguna actividad de gestión de seguridad P09. No cuentan con una inducción adecuada de las actividades internas
R2	Pérdida de confiabilidad en los clientes o socios debido a lentitud en la atención y desmejoramiento de la calidad de servicio	P02. No existe ninguna actividad de gestión de eventos y gestión de incidentes. P03. No existe ninguna actividad de custodia de información. P05. No existe ninguna actividad de gestión de solución de problemas. P06. No existe ninguna actividad de gestión de niveles de servicio. P08. No existe ninguna actividad de gestión de seguridad

CÓD. RIESGO	RIESGO	PROBLEMA TI
R3	Pérdida de eficiencia y eficacia de los empleados de la Cooperativa y por incumplimiento a las normativas emitidas por los entes de control debido a desconocimiento de actividades tecnológicos y presencia de eventos anómalos en los sistemas o aplicaciones	P01. No existe documentación sobre la operación de las actividades de “TIC”. P03. No existe ninguna actividad de custodia de información. P04. No existe ninguna actividad de restauración de base de datos. P05. No existe ninguna actividad de gestión de solución de problemas. P06. No existe ninguna actividad de gestión de niveles de servicio. P07. No existe ninguna actividad de gestión de proveedores. P08. No existe ninguna actividad de gestión de seguridad P09. No cuentan con una inducción adecuada de las actividades internas
R4	Falta de programas de capacitación o inducción de actividades de gestión de accesos y usuarios de sistemas y aplicaciones	P01. No existe documentación sobre la operación de las actividades de “TIC”. P08. No existe ninguna actividad de gestión de seguridad P09. No cuentan con una inducción adecuada de las actividades internas
R5	No se encuentran implementados servicios tecnológicos que permitan robustecer el departamento de “TIC”	P01. No existe documentación sobre la operación de las actividades de “TIC”. P02. No existe ninguna actividad de gestión de eventos y gestión de incidentes. P05. No existe ninguna actividad de gestión de solución de problemas. P06. No existe ninguna actividad de gestión de niveles de servicio. P07. No existe ninguna actividad de gestión de proveedores. P08. No existe ninguna actividad de gestión de seguridad

4.4 Mapa de Riesgo

En esta sección se efectuará el mapa de procesos considerando las definiciones de capítulo II sección 2.6.

Los riesgos que se consideran para la medición son:

- R1- Pérdida económica por indisponibilidad del servicio provocada por falla en los sistemas tecnológicos

- R2- Pérdida de confiabilidad en los clientes o socios debido a lentitud en la atención y desmejoramiento de la calidad de servicio

- R3- Pérdida de eficiencia y eficacia de los empleados de la Cooperativa y por incumplimiento a las normativas emitidas por los entes de control debido a desconocimiento de actividades tecnológicos y presencia de eventos anómalos en los sistemas o aplicaciones

- R4- Falta de programas de capacitación o inducción de actividades de gestión de accesos y usuarios de sistemas y aplicaciones

- R5- No se encuentran implementados servicios tecnológicos que permitan robustecer el departamento de “TIC”,

En base a las tablas descritas en el capítulo 2 sección 2.6 se estable el peso para evaluar los riesgos.

Las consideraciones estas dadas por el impacto y probabilidad a las actividades que ejecuta el Jefe y Analista del departamento de “TIC”.

A continuación, el resultado de esta evaluación de riesgos, se encuentran en la siguiente Tabla 25:

Tabla 25.

Matriz de Mapeo de Riesgos

CÓD. RIESGO	RIESGO	PROBLEMA IDENTIFICADO	CRITICIDAD	PROBABILIDAD	IMPACTO
R1	Pérdida económica por indisponibilidad del servicio provocada por falla en los sistemas tecnológicos	P01. No existe documentación sobre la operación de las actividades de “TIC”. P02. No existe ninguna actividad de gestión de eventos y gestión de incidentes. P03. No existe ninguna actividad de custodia de información. P04. No existe ninguna actividad de restauración de base de datos. P05. No existe ninguna actividad de gestión de solución de problemas. P06. No existe ninguna actividad de gestión de niveles de servicio. P07. No existe ninguna actividad de gestión de proveedores. P08. No existe ninguna actividad de gestión de seguridad P09. No cuentan con una inducción adecuada de las actividades internas	Alto	5,0	4,0
R2	Pérdida de confiabilidad en los clientes o socios debido a lentitud en la atención y desmejoramiento de la calidad de servicio	P02. No existe ninguna actividad de gestión de eventos y gestión de incidentes. P03. No existe ninguna actividad de custodia de información. P05. No existe ninguna actividad de gestión de solución de problemas. P06. No existe ninguna actividad de gestión de niveles de servicio. P08. No existe ninguna actividad de gestión de seguridad	Alto	4,7	4,0
R3	Pérdida de eficiencia y eficacia de los empleados de la Cooperativa y por incumplimiento a las normativas emitidas por los entes de control debido a desconocimiento de actividades tecnológicos y presencia de eventos anómalos en los sistemas o aplicaciones	P01. No existe documentación sobre la operación de las actividades de “TIC”. P03. No existe ninguna actividad de custodia de información. P04. No existe ninguna actividad de restauración de base de datos. P05. No existe ninguna actividad de gestión de solución de problemas. P06. No existe ninguna actividad de gestión de niveles de servicio. P07. No existe ninguna actividad de gestión de proveedores. P08. No existe ninguna actividad de gestión de seguridad P09. No cuentan con una inducción adecuada de las actividades internas	Medio	3,3	3,3
R4	Falta de programas de capacitación o inducción de actividades de gestión de accesos y usuarios de sistemas y aplicaciones	P01. No existe documentación sobre la operación de las actividades de “TIC”. P08. No existe ninguna actividad de gestión de seguridad P09. No cuentan con una inducción adecuada de las actividades internas	Bajo	2,0	2,0

R5	No se encuentran implementados servicios tecnológicos que permitan robustecer el departamento de “TIC”	P01. No existe documentación sobre la operación de las actividades de “TIC”. P02. No existe ninguna actividad de gestión de eventos y gestión de incidentes. P05. No existe ninguna actividad de gestión de solución de problemas. P06. No existe ninguna actividad de gestión de niveles de servicio. P07. No existe ninguna actividad de gestión de proveedores. P08. No existe ninguna actividad de gestión de seguridad	Alto	4,3	3,7

La evaluación de riesgos categorizó de acuerdo al impacto y a la probabilidad, la misma se tiene:

- 3 riesgos con criticidad ALTA.
- 2 riesgo con criticidad MEDIA
- 1 riesgo con criticidad BAJA.

La representación gráfica de la Matriz de Mapeo de Riesgos se presenta en la Figura 17, en donde se visualizan las zonas de impacto y de probabilidad *Alta*. Sobre estos riesgos se deberá tomar acciones de mitigación de riesgos basados en el plan de Mejora que se propondrá en el capítulo V.

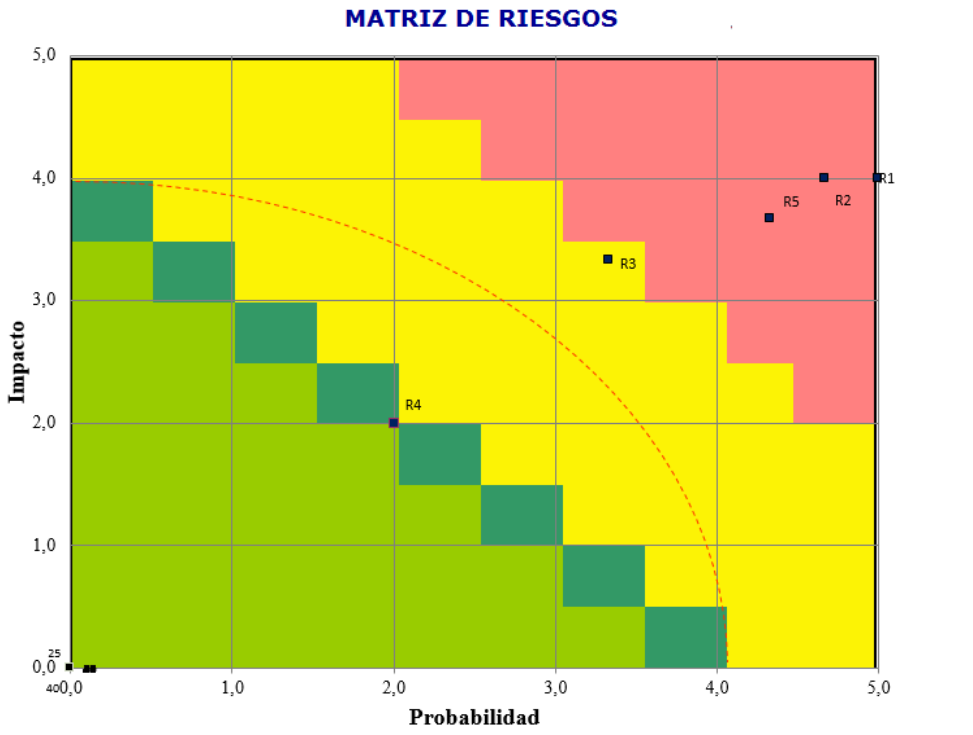


Figura 17. Plano Cartesiano de Riesgos – COAC “Pedro Moncayo Ltda.”

Los riesgos con criticidad *Alta,* ubicados en la zona roja del Plano Cartesiano de la Figura 17 son:

- R1- Pérdida económica por indisponibilidad del servicio provocada por falla en los sistemas tecnológicos.

- R2- Pérdida de confiabilidad en los clientes o socios debido a lentitud en la atención y desmejoramiento de la calidad de servicio.

- R5- No se encuentran implementados servicios tecnológicos que permitan robustecer el departamento de “TIC”.

La Figura 17, se efectuará un detalle de la matriz de riesgo para visualización de los 3 riesgos de impacto.

De estos 3 riesgos evaluados con criticidad *Alta,* se puede concluir que el riesgo R1 – Pérdida económica (Peso = 4.5), tiene una alta probabilidad (Peso = 5.0) de ocurrencia y un alto impacto (Peso = 4.0) que puede afectar directamente a la operación de COAC “Pedro Moncayo Ltda.”. Por tal motivo, es primordial que al momento de tomar acciones sobre este riesgo le den la prioridad del caso.

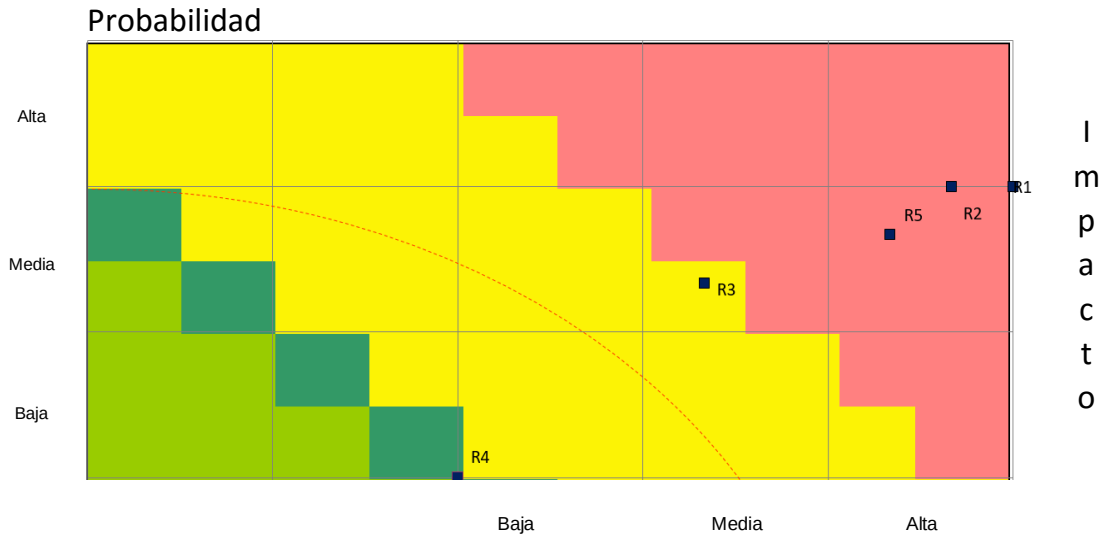


Figura 18. Ubicación de Riesgos en la zona de impacto y probabilidad.

5 Capítulo V. Desarrollo del Plan de Mejora de las actividades tecnológicas.

En este capítulo se indican los planes de acción a ejecutar para eliminar, mitigar o minimizar los riesgos identificados con criticidad “Alta”

5.1 Antecedentes del Plan de Mejora

Para determinar la situación actual del Departamento de “TIC” de la Información respecto a los servicios que brinda a la Cooperativa de Ahorro y Crédito “Pedro Moncayo Ltda.”, se realizó una evaluación de riesgos y del grado de madurez de las actividades tecnológicas, en base a la metodología RISK IT (ISACA, 2009)

En el análisis de riesgos se identificaron 3 riesgos con criticidad “Alta”, los mismos que están tomados en cuenta en el plan de mejoras.

Además, en este plan se considera las acciones a realizar para mejorar el grado de madurez actual de las actividades ejecutadas en el Departamento de “TIC”.

5.2 Objetivos del Plan de Mejoras

Establecer un plan de mejoras que contenga las acciones mínimas que permitan mitigar los riesgos evaluados con criticidad alta y elevar el grado de madurez actual de las actividades ejecutadas en el Departamento de Tecnología de la Información y Comunicaciones y de esta manera proteger la operación del negocio de amenazas y vulnerabilidades.

Dentro del mismo existen los siguientes objetivos específicos:

- Determinar los planes de acción que permitirán mitigar los riesgos identificados con criticidad alta.

- Especificar las acciones a realizar para incrementar el grado de madurez actual de las actividades existentes en el Departamento de “TIC”.

5.3 Alcance del Plan de Mejoras

El informe presenta los planes de acción para los riesgos calificados con criticidad “ALTA”, obtenidos del análisis de los mismos realizado en el capítulo IV.

Los riesgos evaluados como “ALTOS” con los problemas asociados se encuentran en la siguiente tabla:

Tabla 26.

Riesgos con criticidad "ALTA" con Problemas Asociados

CÓD. RIESGO	RIESGOS	PROBLEMAS ASOCIADOS
R1	Pérdida económica por indisponibilidad del servicio provocada por falla en los sistemas tecnológicos	P01. No existe documentación sobre la operación de las actividades de "TIC". P02. No existe ningún proceso de gestión de eventos y gestión de incidentes. P03. No existe un proceso de custodia de información. P04. No existe un proceso de restauración de base de datos. P05. No existe ningún proceso de gestión de solución de problemas. P06. No existe ningún proceso de gestión de niveles de servicio. P07. No existe ningún proceso de gestión de proveedores. P08. No existe ningún modelo de seguridad P09. No cuentan con una inducción adecuada de los procesos internos
R2	Pérdida de confiabilidad en los clientes o socios debido a lentitud en la atención y desmejoramiento de la calidad de servicio	P02. No existe ningún proceso de gestión de eventos y gestión de incidentes. P03. No existe un proceso de custodia de información. P05. No existe ningún proceso de gestión de solución de problemas. P06. No existe ningún proceso de gestión de niveles de servicio. P08. No existe ningún modelo de seguridad
R5	No se encuentran implementados servicios tecnológicos que permitan robustecer el departamento de "TIC"	P01. No existe documentación sobre la operación de las actividades de "TIC". P02. No existe ningún proceso de gestión de eventos y gestión de incidentes. P05. No existe ningún proceso de gestión de solución de problemas. P06. No existe ningún proceso de gestión de niveles de servicio. P07. No existe ningún proceso de gestión de proveedores. P08. No existe ningún modelo de seguridad

También se incluye dentro de este plan las acciones para elevar del grado de madurez "0 - Proceso Incompleto" las actividades tecnológicas del Departamento de "TIC" al grado de madurez recomendado, que puede ser:

1 - Proceso Ejecutado
2 - Proceso Gestionado
3 - Proceso Establecido

5.4 Estructura del Plan de Mejoras

Se encuentra definido de la siguiente manera:

a) Los riesgos calificados con criticidad "ALTA", en base a la probabilidad e impacto al negocio y de acuerdo a las actividades actuales de "TIC".

b) Planes de acción con tareas puntuales a ejecutar con el grado de madurez objetivo para cada actividad tecnológica.

5.5 Procedimientos Aplicados para establecer el Plan de Mejoras

El proceso utilizado para establecer el plan de mejoras se detalla a continuación:

- Evaluación del grado de madurez de las actividades actuales del Departamento de “TIC”, realizado en el capítulo III de este proyecto de titulación.
- Identificación de riesgos utilizando las perspectivas indicadas en la metodología de “RISK IT”, Balance Scorecard, en base a los problemas, amenazas y vulnerabilidad evidenciados, desarrollado en el capítulo IV del presente trabajo de titulación.

- Mapeo del nivel de criticidad de riesgos basados en la probabilidad y el impacto, con calificación “ALTO”, realizado en el capítulo IV del presente trabajo de titulación.

- Definición de las acciones que la Cooperativa “Pedro Moncayo Ltda.” debe efectuar para mitigar los riesgos existentes y alcanzar una mejora continua en sus procesos, con priorización y tiempos estimados de ejecución de las actividades y tareas recomendadas, por desarrollar en este capítulo.

5.6 Plan de Mejoras

5.6.1 Grado de Madurez de las Actividades TI

En la Tabla 27 y en la Figura18, se indica el grado de madurez actual que tienen las actividades TI, del Departamento de Tecnología de la Información y Comunicaciones.

Tabla 27.

Grado de Madurez de las Actividades TI - Riesgos

GRADO DE MADUREZ										
Cod. Actividad	**Actividad**	**0. Proceso Incompleto**	**1. Proceso Ejecutado**	**2. Proceso Gestionado**	**3. Proceso Establecido**	**4. Proceso Predecible**	**5. Proceso Optimizado**	**Nivel Actual**	**Nivel Básico Requerido**	**Nivel Optimo**
AAT01	MONITOREO	1	0	0	0	0	0	0	1	2
AAT02	MANTENIMIENTO	1	0	0	0	0	0	0	1	2
AAT03	SOPORTE A USUARIOS	1	0	0	0	0	0	0	1	2
AAT04	INSTALACIÓN A	1	0	0	0	0	0	0	1	2
AAT05	CREACIÓN USUARIOS	1	0	0	0	0	0	0	1	2
AAT06	RESETEO DE CLAVES	1	0	0	0	0	0	0	1	2
AAT07	INACTIVACIÓN DE USUARIO	1	0	0	0	0	0	0	1	2
AAT08	CONFIFURACION	1		0	0	0	0	0	1	2
AAT09	SOPORTE APLICACIÓN / INFRAESTRUCTURA	1	0	0	0	0	0	0	1	2
AAT10	PROVEEDOR	1	0	0	0	0	0	0	1	2
AAT11	REQUERIMIENTOS	1	0	0	0	0	0	0	1	2

Como se puede observar, las Actividades TI actualmente están en un grado de madurez “0 – Procesos Incompletos”, y tal cual se indicó anteriormente, lo recomendado es cambiar el grado de madurez de estas actividades, para ello es necesario realizar los planes de acción indicados a continuación.

5.6.2 Planes de Acción

En el Plan de Mejoras se explican las tareas y proyectos requeridos que deben ser ejecutados para mitigar los riesgos con criticidad “Alta”, los mismos se indican a continuación:

- Planes de acción – Tareas, en donde se indican las actividades a realizar para solucionar los problemas de documentación y dar el marco de gobierno al departamento de “TIC”.

- Planes de acción – Proyectos, se detallan los proyectos requeridos para lograr que el departamento de “TIC”, se alinee a los objetivos estratégicos del negocio y pueda incluirse dentro del proceso de operación del mapa de procesos de COAC.

5.6.2.1 Planes de Acción - Tareas

Dentro de los planes de acción de esta sección, se tienen los siguientes:

1. Establecer y difundir las principales políticas respecto a los activos de la información primordiales para la continuidad del negocio. Las principales políticas que se deben establecer y difundir son:

1.1. Política de Gestión de Servicios TI, las tareas a realizar son las siguientes:

1.1.1. Elaborar Política de Gestión de Servicios TI

Tiempo Estimado: se necesita un tiempo estimado de 80 horas hombre.

Recursos y áreas: para esta tarea se necesitan 5 recursos de las siguientes áreas o departamentos:

- Tecnología de la Información y Comunicaciones
- Planificación y Procesos
- Riesgos
- Talento Humano
- Asesoría Legal

1.1.2. Revisar Política de Gestión de Servicios TI

Tiempo Estimado: se necesita un tiempo estimado de 40 horas hombre.

Recursos y áreas: para esta tarea se necesita que 1 recurso de la Gerencia General.

1.1.3. Aprobar Política de Gestión de Servicios TI

Tiempo Estimado: se necesita un tiempo estimado de 24 horas hombre.

Recursos y áreas: la aprobación de esta Política se la realizará en la Asamblea General de Socios que debe ser convocada por el Gerente General.

1.1.4. Publicar Política de Gestión de Servicios TI

Tiempo Estimado: se necesita un tiempo estimado de 16 horas hombre.
Recursos y áreas: la publicación de la Política es realizado por el área de Planificación y Procesos

Prioridad: Esta Política tiene una prioridad 1, por ser la más importante el establecimiento del gobierno del Departamento de “TIC”.

Total Tarea: El total de horas hombre requerido para la realización de esta Política es de 160.

1.2. Política de Gestión de Seguridad, dentro de esta Política se tiene que realizar las siguientes tareas:

1.2.1. Elaborar Política de Gestión de Seguridad

Tiempo Estimado: se necesita un tiempo estimado de 80 horas hombre.

Recursos y áreas: para esta tarea se necesitan 5 recursos de las siguientes áreas o departamentos:

- Tecnología de la Información y Comunicaciones
- Planificación y Procesos
- Riesgos
- Talento Humano
- Asesoría Legal

1.2.2. Revisar Política de Gestión de Seguridad

Tiempo Estimado: se necesita un tiempo estimado de 40 horas hombre.

Recursos y áreas: para esta tarea se necesita que 1 recurso de la Gerencia General.

1.2.3. Aprobar Política de Gestión de Seguridad

Tiempo Estimado: se necesita un tiempo estimado de 24 horas hombre.
Recursos y áreas: la aprobación de esta Política se la realizará en la Asamblea General de Socios que debe ser convocada por el Gerente General.

1.2.4. Publicar Política de Gestión de Seguridad

Tiempo Estimado: se necesita un tiempo estimado de 16 horas hombre.
Recursos y áreas: la publicación de la Política es realizado por el área de Planificación y Procesos

Prioridad: Esta Política tiene una prioridad 2, dado que se va a establecer la gestión de seguridad dentro del mapa de procesos de la Cooperativa.

Total Tarea: El total de horas hombre requerido para la realización de esta Política es de 160.

1.3. Política de Gestión de Riesgos y Continuidad

1.3.1. Elaborar Política de Gestión de Riesgos y Continuidad

Tiempo Estimado: se necesita un tiempo estimado de 80 horas hombre.

Recursos y áreas: para esta tarea se necesitan 5 recursos de las siguientes áreas o departamentos:

- Tecnología de la Información y Comunicaciones
- Planificación y Procesos
- Riesgos
- Talento Humano
- Asesoría Legal

1.3.2. Revisar Política de Gestión de Riesgos y Continuidad

Tiempo Estimado: se necesita un tiempo estimado de 40 horas hombre.

Recursos y áreas: para esta tarea se necesita que 1 recurso de la Gerencia General.

1.3.3. Aprobar Política de Gestión de Riesgos y Continuidad

Tiempo Estimado: se necesita un tiempo estimado de 24 horas hombre.

Recursos y áreas: la aprobación de esta Política se la realizará en la Asamblea General de Socios que debe ser convocada por el Gerente General.

1.3.4. Publicar Política de Gestión de Riesgos y Continuidad

Tiempo Estimado: se necesita un tiempo estimado de 16 horas hombre.
Recursos y áreas: la publicación de la Política es realizado por el área de Planificación y Procesos

Prioridad: Esta Política tiene una prioridad 3, con la misma se quiere establecer la gestión de riesgos y continuidad del negocio.

Total de tiempo estimado. - El total de horas-hombre requerido para la realización del Plan de Acción 1 es de 160.

1. Documentar las actividades actuales del Departamento de “TIC”.

Las actividades TI que deben ser documentadas son las siguientes:

1. Soporte a usuarios, tiene prioridad 4
2. Creación de Usuarios, tiene prioridad 5
3. Reseteo de Usuarios, tiene prioridad 6
4. Inactivación de Usuarios, tiene prioridad 7
5. Monitoreo de aplicaciones y sistemas, prioridad 8
6. Instalación de sistemas y aplicaciones, tiene prioridad 9
7. Soporte de aplicaciones e infraestructura, tiene prioridad 10
8. Configuración de aplicaciones y sistemas, tiene prioridad 11
9. Mantenimiento de aplicaciones e infraestructura, tiene prioridad 12
10. Requerimientos de usuarios, tiene prioridad 13

Tareas a ejecutar. - Las tareas a ejecutar en cada una de estas actividades TI son:

a) Elaborar procedimientos.

Tiempo Estimado: se necesita un tiempo estimado de 40 horas hombre.

Recursos y áreas: para esta tarea se necesitan 2 recursos de las siguientes áreas o departamentos:

- Tecnología de la Información y Comunicaciones
- Planificación y Procesos

b) Revisar procedimientos

Tiempo Estimado: se necesita un tiempo estimado de 24 horas hombre.

Recursos y áreas: para esta tarea se necesita 1 recurso del departamento de Tecnología de la Información y Comunicaciones

c) Aprobar procedimientos

Tiempo Estimado: se necesita un tiempo estimado de 16 horas hombre.

Recursos y áreas: para esta tarea se necesita 1 recurso del departamento de Tecnología de la Información y Comunicaciones

d) Difundir procedimientos

Tiempo Estimado: se necesita un tiempo estimado de 8 horas hombre.

Recursos y áreas: para esta tarea se necesita 1 recurso del departamento de Planificación y Procesos.

e) Elaborar instructivos

Tiempo Estimado: se necesita un tiempo estimado de 24 horas hombre.

Recursos y áreas: para esta tarea se necesita 1 recurso del departamento de Tecnología de la Información y Comunicaciones

f) Revisar instructivos

Tiempo Estimado: se necesita un tiempo estimado de 8 horas hombre.

Recursos y áreas: para esta tarea se necesita 1 recurso del departamento de Tecnología de la Información y Comunicaciones

Total de tiempo estimado. – El total de tiempo estimado para el Plan de Acción 2 es 1200 horas hombre.

Problemas Solucionados. - El problema que se solventan al ejecutar estos planes de acción es el siguiente:

P01. No existe documentación sobre la operación de los procesos de “TIC”.

Riesgos Mitigados. – Los riesgos que se mitigan al realizar estos planes de acción son:

- R01. Pérdida económica por indisponibilidad del servicio provocada por falla en los sistemas tecnológicos.

- R05. No se encuentran implementados servicios tecnológicos que permitan robustecer el departamento de “TIC”.

A continuación, se presenta la Tabla 28 con los Planes de Acción – Tareas:

Tabla 28.

Planes de Acción – Tareas

PLAN DE MEJORAS PARA EL DEPARTAMENTO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES

Plan de Acción	Actividades de "TIC"	Tareas	Tiempo Estimado (horas hombre)	Recursos	Áreas de COAC	Prioridad	Problema Resuelto	Riesgos Mitigados
1. Establecer y difundir las principales políticas respecto a los activos de la información primordiales para la continuidad del negocio	1.1. Gestión de servicios TI	1.1.1. Elaborar Política de Gestión de Servicios TI	80	R1, R2, R3, R4, R5	TIC, Planificación y Procesos, Riesgos, Talento Humano, Asesoría Jurídica	1	P01. No existe documentación sobre la operación de las actividades de "TIC".	R01. Pérdida económica por indisponibilidad del servicio provocada por falla en los sistemas tecnológicos R05. No se encuentran implementados servicios tecnológicos que permitan robustecer el departamento de "TIC"
		1.1.2. Revisar Política de Gestión de Servicios TI	40	R6	Gerencia General			
		1.1.3. Aprobar Política de Gestión de Servicios TI	24	R7	Asamblea General			
		1.1.4. Publicar Política de Gestión de Servicios TI	16	R2	Planificación y Procesos			
	1.2. Gestión de Seguridad	1.2.1. Elaborar Política de Gestión de Seguridad	80	R1, R2, R3, R4, R5	TIC, Planificación y Procesos, Riesgos, Talento Humano, Asesoría Jurídica	2		
		1.2.2. Revisar Política de Gestión de Seguridad	40	R6	Gerencia General			
		1.2.3. Aprobar Política de Gestión de Seguridad	24	R7	Asamblea General			
		1.2.4. Publicar Política de Gestión de Seguridad	16	R2	Planificación y Procesos			
	1.3. Gestión de Riesgos y Continuidad	1.3.1. Elaborar Política de Gestión de Riesgos y Continuidad	80	R1, R2, R3, R4, R5	TIC, Planificación y Procesos, Riesgos, Talento Humano, Asesoría Jurídica	3		
		1.3.2. Revisar Política de Gestión de Riesgos y Continuidad	40	R6	Gerencia General			
		1.3.3. Aprobar Política de Gestión de Riesgos y Continuidad	24	R7	Asamblea General			
		1.3.4. Publicar Política de Gestión de Riesgos y Continuidad	16	R2	Planificación y Procesos			

Pedro Moncayo Ltda.
COOPERATIVA DE AHORRO Y CRÉDITO
Apoyando al Desarrollo de la Comunidad

PLAN DE MEJORAS PARA EL DEPARTAMENTO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES

Plan de Acción	Actividades de "TIC"	Tareas	Tiempo Estimado (horas hombre)	Recursos	Áreas de COAC	Prioridad	Problema Resuelto	Riesgos Mitigados
2. Documentar las actividades actuales del Departamento de "TIC". … ¼	2.1. Soporte a usuarios	2.1.1. Elaborar procedimiento	40	R1, R2	TIC, Planificación y Procesos	4	P01. No existe documentación sobre la operación de las actividades de "TIC".	R01. Pérdida económica por indisponibilidad del servicio provocada por falla en los sistemas tecnológicos. R05. No se encuentran implementados servicios tecnológicos que permitan robustecer el departamento de "TIC"
		2.1.2. Revisar procedimiento	24	R1	TIC			
		2.1.3. Aprobar procedimiento	16	R1	TIC			
		2.1.4. Difundir procedimiento	8	R2	Planificación y Procesos			
		2.1.5. Elaborar instructivo	24	R1	TIC			
		2.1.6. Revisar instructivo	8	R2	TIC			
	2.2. Creación de usuarios	2.2.1. Elaborar procedimiento	40	R1	TIC, Planificación y Procesos	5		
		2.2.2. Revisar procedimiento	24	R2	TIC			
		2.2.3. Aprobar procedimiento	16	R3	TIC			
		2.2.4. Difundir procedimiento	8	R4	Planificación y Procesos			
		2.2.5. Elaborar instructivo	24	R1	TIC			
		2.2.6. Revisar instructivo	8	R2	TIC			
	2.3. Reseteo de usuarios	2.3.1. Elaborar procedimiento	40	R1	TIC, Planificación y Procesos	6		
		2.3.2. Revisar procedimiento	24	R2	TIC			
		2.3.3. Aprobar procedimiento	16	R3	TIC			
		2.3.4. Difundir procedimiento	8	R4	Planificación y Procesos			
		2.3.5. Elaborar instructivo	24	R1	TIC			
		2.3.6. Revisar instructivo	8	R2	TIC			

Pedro Moncayo Ltda.
COOPERATIVA DE AHORRO Y CRÉDITO
Apoyando al Desarrollo de la Comunidad

PLAN DE MEJORAS PARA EL DEPARTAMENTO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES

Plan de Acción	Actividades de "TIC"	Tareas	Tiempo Estimado (horas hombre)	Recursos	Áreas de COAC	Prioridad	Problema Resuelto	Riesgos Mitigados
2. Documentar las actividades actuales del Departamento de "TIC". …2/4	2.4. Inactivación de usuarios	2.4.1. Elaborar procedimiento	40	R1	TIC, Planificación y Procesos	7	P01. No existe documentación sobre la operación de las actividades de "TIC".	R01. Pérdida económica por indisponibilidad del servicio provocada por falla en los sistemas tecnológicos. R05. No se encuentran implementados servicios tecnológicos que permitan robustecer el departamento de "TIC"
		2.4.2. Revisar procedimiento	24	R2	TIC			
		2.4.3. Aprobar procedimiento	16	R3	TIC			
		2.4.4. Difundir procedimiento	8	R4	Planificación y Procesos			
		2.4.5. Elaborar instructivo	24	R1	TIC			
		2.4.6. Revisar instructivo	8	R2	TIC			
	2.5. Monitoreo de aplicaciones y sistemas	2.5.1. Elaborar procedimiento	40	R1	TIC, Planificación y Procesos	8		
		2.5.2. Revisar procedimiento	24	R2	TIC			
		2.5.3. Aprobar procedimiento	16	R3	TIC			
		2.5.4. Difundir procedimiento	8	R4	Planificación y Procesos			
		2.5.5. Elaborar instructivo	24	R1	TIC			
		2.5.6. Revisar instructivo	8	R2	TIC			
	2.6. Instalación de sistemas y aplicaciones	2.6.1. Elaborar procedimiento	40	R1	TIC, Planificación y Procesos	9		
		2.6.2. Revisar procedimiento	24	R2	TIC			
		2.6.3. Aprobar procedimiento	16	R3	TIC			
		2.6.4. Difundir procedimiento	8	R4	Planificación y Procesos			
		2.6.5. Elaborar instructivo	24	R1	TIC			
		2.6.6. Revisar instructivo	8	R2	TIC			

Pedro Moncayo Ltda.
COOPERATIVA DE AHORRO Y CRÉDITO
Apoyando al Desarrollo de la Comunidad

PLAN DE MEJORAS PARA EL DEPARTAMENTO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES

Plan de Acción	Actividades de "TIC"	Tareas	Tiempo Estimado (horas hombre)	Recursos	Áreas de COAC	Prioridad	Problema Resuelto	Riesgos Mitigados
2. Documentar las actividades actuales del Departamento de "TIC". ...3/4	2.7. Soporte de aplicaciones e infraestructura	2.7.1. Elaborar procedimiento	40	R1	TIC, Planificación y Procesos	10	P01. No existe documentación sobre la operación de las actividades de "TIC".	R01. Pérdida económica por indisponibilidad del servicio provocada por falla en los sistemas tecnológicos. R05. No se encuentran implementados servicios tecnológicos que permitan robustecer el departamento de "TIC".
		2.7.2. Revisar procedimiento	24	R2	TIC			
		2.7.3. Aprobar procedimiento	16	R3	TIC			
		2.7.4. Difundir procedimiento	8	R4	Planificación y Procesos			
		2.7.5. Elaborar instructivo	24	R1	TIC			
		2.7.6. Revisar instructivo	8	R2	TIC			
	2.8. Configuración de aplicaciones y sistemas	2.8.1. Elaborar procedimiento	40	R1	TIC, Planificación y Procesos	11		
		2.8.2. Revisar procedimiento	24	R2	TIC			
		2.8.3. Aprobar procedimiento	16	R3	TIC			
		2.8.4. Difundir procedimiento	8	R4	Planificación y Procesos			
		2.8.5. Elaborar instructivo	24	R1	TIC			
		2.8.6. Revisar instructivo	8	R2	TIC			
	2.9. Mantenimiento de aplicaciones e infraestructura	2.9.1. Elaborar procedimiento	40	R1	TIC, Planificación y Procesos	12		
		2.9.2. Revisar procedimiento	24	R2	TIC			
		2.9.3. Aprobar procedimiento	16	R3	TIC			
		2.9.4. Difundir procedimiento	8	R4	Planificación y Procesos			
		2.9.5. Elaborar instructivo	24	R1	TIC			
		2.9.6. Revisar instructivo	8	R2	TIC			

Pedro Moncayo Ltda.
COOPERATIVA DE AHORRO Y CRÉDITO
Apoyando al Desarrollo de la Comunidad

PLAN DE MEJORAS PARA EL DEPARTAMENTO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES

Plan de Acción	Actividades de "TIC"	Tareas	Tiempo Estimado (horas hombre)	Recursos	Áreas de COAC	Prioridad	Problema Resuelto	Riesgos Mitigados
2. Documentar las actividades actuales del Departamento de "TIC". …4/4	2.10. Requerimientos de usuarios	2.10.1. Elaborar procedimiento	40	R1	TIC, Planificación y Procesos	13	P01. No existe documentación sobre la operación de las actividades de "TIC".	R01. Pérdida económica por indisponibilidad del servicio provocada por falla en los sistemas tecnológicos. R05. No se encuentran implementados servicios tecnológicos que permitan robustecer el departamento de "TIC"
		2.10.2. Revisar procedimiento	24	R2	TIC			
		2.10.3. Aprobar procedimiento	16	R3	TIC			
		2.10.4. Difundir procedimiento	8	R4	Planificación y Procesos			
		2.10.5. Elaborar instructivo	24	R1	TIC			
		2.10.6. Revisar instructivo	8	R2	TIC			

5.6.2.2 Planes de Acción – Proyectos

Dentro del Plan de Mejoras, se han identificado un proyecto que se requieren sea implementados para que permitan al Departamento de “TIC” alinearse a metas estratégicas de la Cooperativa. El proyecto requerido es:

3. Implementación del Portafolio y Catálogo de Servicios TI.

El Catálogo de Servicios TI que deben ser implementados son los siguientes:

Gestión de Proveedores. – Se da una Prioridad 1 a este servicio TI

Tiempo Estimado: se necesita un tiempo estimado de 4 meses.

Recursos y áreas: para este proyecto se necesitan 5 recursos de las siguientes áreas o departamentos:

- Tecnología de la Información y Comunicaciones
- Planificación y Procesos
- Riesgos
- Talento Humano
- Asesoría Legal

Gestión Técnica. – Se da una Prioridad 3a este servicio TI

Tiempo Estimado: se necesita un tiempo estimado de 2 meses.

Recursos y áreas: para este proyecto se necesitan 2 recursos de las siguientes áreas o departamentos:

- Tecnología de la Información y Comunicaciones
- Planificación y Procesos

Gestión de Operación TI. – Se da una Prioridad 1 a este servicio TI
Tiempo Estimado: se necesita un tiempo estimado de 2 meses.

Recursos y áreas: para este proyecto se necesitan 2 recursos de las siguientes áreas o departamentos:

- Tecnología de la Información y Comunicaciones
- Planificación y Procesos

Gestión de Aplicaciones. – Se da una Prioridad 2 a este servicio TI

Tiempo Estimado: se necesita un tiempo estimado de 4 meses.

Recursos y áreas: para este proyecto se necesitan 2 recursos de las siguientes áreas o departamentos:

- Tecnología de la Información y Comunicaciones
- Planificación y Procesos

Gestión de Configuraciones. – Se da una Prioridad 3 a este servicio TI.

Tiempo Estimado: se necesita un tiempo estimado de 4 meses.

Recursos y áreas: para este proyecto se necesitan 2 recursos de las siguientes áreas o departamentos:

- Tecnología de la Información y Comunicaciones
- Planificación y Procesos

Gestión de Mesa de Ayuda. – Se da una Prioridad 1 a este servicio TI

Tiempo Estimado: se necesita un tiempo estimado de 2 meses.

Recursos y áreas: para este proyecto se necesitan 2 recursos de las siguientes áreas o departamentos:

- Tecnología de la Información y Comunicaciones
- Planificación y Procesos

Gestión de Niveles de Servicio. – Se da una Prioridad 1 a este servicio TI.

Tiempo Estimado: se necesita un tiempo estimado de 2 meses.

Recursos y áreas: para este proyecto se necesitan 4 recursos de las siguientes áreas o departamentos:

- Tecnología de la Información y Comunicaciones
- Planificación y Procesos
- Negocios
- Asesoría Legal

Gestión de Requerimientos. – Se da una Prioridad 3 a este servicio TI.

Tiempo Estimado: se necesita un tiempo estimado de 2 meses.

Recursos y áreas: para este proyecto se necesitan 2 recursos de las siguientes áreas o departamentos:

- Tecnología de la Información y Comunicaciones
- Planificación y Procesos

Gestión de Problemas. – Se da una Prioridad 2 a este servicio TI.

Tiempo Estimado: se necesita un tiempo estimado de 3 meses.

Recursos y áreas: para este proyecto se necesitan 3 recursos de las siguientes áreas o departamentos:

- Tecnología de la Información y Comunicaciones
- Planificación y Procesos

- Riesgos

Gestión de Eventos. – Se da una Prioridad 2 a este servicio TI.

Tiempo Estimado: se necesita un tiempo estimado de 3 meses.

Recursos y áreas: para este proyecto se necesitan 3 recursos de las siguientes áreas o departamentos:

- Tecnología de la Información y Comunicaciones
- Planificación y Procesos
- Riesgos

Gestión de Incidentes. – Se da una Prioridad 2 a este servicio TI.

Tiempo Estimado: se necesita un tiempo estimado de 4 meses.

Recursos y áreas: para este proyecto se necesitan 5 recursos de las siguientes áreas o departamentos:

- Tecnología de la Información y Comunicaciones
- Planificación y Procesos
- Riesgos
- Negocios
- Talento Humano
- Asesoría Legal

Gestión de Cambios. – Se da una Prioridad 3 a este servicio TI.

Tiempo Estimado: se necesita un tiempo estimado de 4 meses.

Recursos y áreas: para este proyecto se necesitan 4 recursos de las siguientes áreas o departamentos:

- Tecnología de la Información y Comunicaciones
- Planificación y Procesos
- Riesgos
- Negocios

Gestión de Conocimiento. – Se da una Prioridad 3 a este servicio TI.

Tiempo Estimado: se necesita un tiempo estimado de 3 meses.

Recursos y áreas: para este proyecto se necesitan 3 recursos de las siguientes áreas o departamentos:

- Tecnología de la Información y Comunicaciones
- Planificación y Procesos
- Talento Humano

Problemas Solucionados. – Con este proyecto se solucionan todos los problemas identificados en el capítulo IV, y que son los siguientes:

- P01. No existe documentación sobre la operación de los procesos de “TIC”.

- P02. No existe ningún proceso de gestión de eventos y gestión de incidentes.

- P03. No existe un proceso de custodia de información.

- P04. No existe un proceso de restauración de base de datos.

- P05. No existe ningún proceso de gestión de solución de problemas.

- P06. No existe ningún proceso de gestión de niveles de servicio.

- P07. No existe ningún proceso de gestión de proveedores.

- P08. No existe ningún modelo de seguridad

- P09. No cuentan con una inducción adecuada de los procesos internos

Riesgos Mitigados. – Los riesgos que se mitigan al implementar este proyecto son:

- R01. Pérdida económica por indisponibilidad del servicio provocada por falla en los sistemas tecnológicos.

- R03. Pérdida de confiabilidad en los clientes o socios debido a lentitud en la atención y desmejoramiento de la calidad de servicio

- R05. No se encuentran implementados servicios tecnológicos que permitan robustecer el departamento de “TIC”.

A continuación, se presenta la Tabla 29 con los Planes de Acción – Proyectos:

Tabla 29.

Planes de Acción – Proyectos

PLAN DE MEJORAS PARA EL DEPARTAMENTO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES

Plan de Acción	Actividades de "TIC"	Proyecto	Tiempo Estimado (meses)	Recursos	Áreas de COAC	Prioridad	Problema Resuelto	Riesgos Mitigados
3. Implementar el portafolio y el catálogo de servicios TI en el Departamento de "TIC", que se ajuste a las necesidades del negocio y permita alinearse a las metas estratégicas de la Cooperativa. …1/3	3.1. Gestión de Proveedores	Implementar el servicio de Gestión de Proveedores	4	R1, R2, R3, R4, R5	TIC, Planificación y Procesos, Riesgos, Negocios, Asesoría Jurídica	1	P01. No existe documentación sobre la operación de las actividades de "TIC".	R01. Pérdida económica por indisponibilidad del servicio provocada por falla en los sistemas tecnológicos
	3.2. Gestión Técnica	Implementar el servicio de Gestión Técnica	2	R1, R2	TIC, Planificación y Procesos	3	P03. No existe un proceso de custodia de información.	R03. Pérdida de confiabilidad en los clientes o socios debido a lentitud en la atención y desmejoramiento de la calidad de servicio
	3.3. Gestión de Operación TI	Implementar el servicio de Gestión de Operación TI	2	R1, R2	TIC, Planificación y Procesos	2	P04. No existe un proceso de restauración de base de datos.	
	3.4. Gestión de Aplicaciones	Implementar el servicio de Gestión de Aplicaciones	4	R1, R2	TIC, Planificación y Procesos	2	P06. No existe ningún proceso de gestión de niveles de servicio.	
	3.5. Gestión de Configuraciones	Implementar el servicio de Gestión de Configuraciones	4	R1, R2	TIC, Planificación y Procesos	2	P07. No existe ningún proceso de gestión de proveedores.	R05. No se encuentran implementados servicios tecnológicos que permitan robustecer el departamento de "TIC"
	3.6. Gestión de Mesa de Ayuda	Implementar el servicio de Gestión de Mesa de Ayuda	2	R1, R2	TIC, Planificación y Procesos	1	P09. No cuentan con una inducción adecuada de los procesos internos	

Pedro Moncayo Ltda.
COOPERATIVA DE AHORRO Y CRÉDITO
Apoyando al Desarrollo de la Comunidad

PLAN DE MEJORAS PARA EL DEPARTAMENTO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES

Plan de Acción	Actividades de "TIC"	Proyecto	Tiempo Estimado (meses)	Recursos	Áreas de COAC	Prioridad	Problema Resuelto	Riesgos Mitigados
3. Implementar el portafolio y el catálogo de servicios TI en el Departamento de "TIC", que se ajuste a las necesidades del negocio y permita alinearse a las metas estratégicas de la Cooperativa. ...2/3	3.7. Gestión de Niveles de Servicio	Implementar el servicio de Gestión de Niveles de Servicio	2	R1, R2, R3, R4	TIC, Planificación y Procesos, Negocios, Asesoría Jurídica	1	P01. No existe documentación sobre la operación de las actividades de "TIC". P02. No existe ningún proceso de gestión de eventos y gestión de incidentes. P05. No existe ningún proceso de gestión de solución de problemas. P06. No existe ningún proceso de gestión de niveles de servicio. P08. No existe ningún modelo de seguridad	R01. Pérdida económica por indisponibilidad del servicio provocada por falla en los sistemas tecnológicos R03. Pérdida de confiabilidad en los clientes o socios debido a lentitud en la atención y desmejoramiento de la calidad de servicio R05. No se encuentran implementados servicios tecnológicos que permitan robustecer el departamento de "TIC"
	3.8. Gestión de Requerimientos	Implementar el servicio de Gestión de Requerimientos	2	R1, R2	TIC, Planificación y Procesos	3		
	3.9. Gestión de Problemas	Implementar el servicio de Gestión de Problemas	3	R1, R2, R3	TIC, Planificación y Procesos, Riesgos	2		
	3.10. Gestión de Eventos	Implementar el servicio de Gestión de Eventos	3	R1, R2, R3	TIC, Planificación y Procesos, Riesgos	2		
	3.10. Gestión de Incidentes	Implementar el servicio de Gestión de Incidentes	4	R1, R2, R3, R4, R5	TIC, Planificación y Procesos, Riesgos, Negocios, Talento Humano	2		

Pedro Moncayo Ltda.
COOPERATIVA DE AHORRO Y CRÉDITO
Apoyando al Desarrollo de la Comunidad

PLAN DE MEJORAS PARA EL DEPARTAMENTO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIONES

Plan de Acción	Actividades de "TIC"	Proyecto	Tiempo Estimado (meses)	Recursos	Áreas / Departamentos	Prioridad	Problema Resuelto	Riesgos Mitigados
3. Implementar el portafolio y el catálogo de servicios TI en el Departamento de "TIC", que se ajuste a las necesidades del negocio y permita alinearse a las metas estratégicas de la Cooperativa. …3/3	3.11. Gestión de Cambios	Implementar el servicio de Gestión de Cambios	4	R1, R2, R3, R4	TIC, Planificación y Procesos, Riesgos, Negocios	3	P01. No existe documentación sobre la operación de las actividades de "TIC". P08. No existe ningún modelo de seguridad P09. No cuentan con una inducción adecuada de los procesos internos	R01. Pérdida económica por indisponibilidad del servicio provocada por falla en los sistemas tecnológicos R03. Pérdida de confiabilidad en los clientes o socios debido a lentitud en la atención y desmejoramiento de la calidad de servicio R05. No se encuentran implementados servicios tecnológicos que permitan robustecer el departamento de "TIC"
	3.12. Gestión de Conocimiento	Implementar el servicio de Gestión de Conocimiento	3	R1, R2, R3	TIC, Planificación y Procesos, Talento Humano	3		

5.6.3 Resumen de recursos del Plan de Mejoras

A continuación, se presentan los recursos necesarios para los planes de acción, recursos y priorización para las tareas y los proyectos indicados en la sección 5.6.2.

5.6.3.1 Resumen de recursos del Plan de Mejoras - Tareas

En la Tabla 30, se detalla el tiempo total estimado que tomará efectuar las tareas a implementarse para el establecimiento de políticas y la documentación de procedimientos, las mismas contienen las siguientes columnas:

1. Plan de Acción: Define la documentación de las políticas y las actividades a ejecutarse.

2. Actividades “TIC”: Describe las actividades TI de la Cooperativa sobre los cuales se aplica el plan de acción.

3. Tiempo Estimado (horas): Corresponde al esfuerzo requerido en horas para efectuar la documentación.

4. Nro. Recursos: Es el número de recursos estimado para la ejecución de la documentación.

5. Áreas: Se describe el área al que se está efectuando el cambio.

6. Prioridad: Es la categoría asignada para ejecutar la actividad, es decir, el orden en el que se sugiere la implementación de políticas y documentación requerida.

A continuación, se presenta la Tabla 30:

Tabla 30.

Tiempos requeridos para la ejecución Plan de acción de Tareas

RESUMEN DE RECURSOS Y TIEMPO ESTIMADO PARA PLAN DE ACCIONES – TAREAS					
Plan de Acción	**Actividades de "TIC"**	**Tiempo Estimado (horas hombre)**	**Nro. Recursos**	**Áreas / Departamentos**	**Prioridad**
1. Establecer y difundir las principales políticas respecto a los activos de la información primordiales para la continuidad del negocio	1.1. Gestión de servicios TI	160	7	TIC, Planificación y Procesos, Riesgos, Talento Humano, Asesoría Jurídica, Gerencia General, Asamblea General	1
	1.2. Gestión de Seguridad	160	7	TIC, Planificación y Procesos, Riesgos, Talento Humano, Asesoría Jurídica, Gerencia General, Asamblea General	2
	1.3. Gestión de Riesgos y Continuidad	160	7	TIC, Planificación y Procesos, Riesgos, Talento Humano, Asesoría Jurídica, Gerencia General, Asamblea General	3
2. Documentar las actividades actuales del Departamento de "TIC".	2.1. Soporte a usuarios	120	2	TIC, Planificación y Procesos	4
	2.2. Gestión de Seguridad	120	4	TIC, Planificación y Procesos	5
	2.3. Reseteo de usuarios	120	4	TIC, Planificación y Procesos	6
	2.4. Inactivación de usuarios	120	2	TIC, Planificación y Procesos	7
	2.5. Monitoreo de aplicaciones y sistemas	120	4	TIC, Planificación y Procesos	8
	2.6. Gestión de Riesgos y Continuidad	120	4	TIC, Planificación y Procesos	9
	2.7. Soporte de aplicaciones e infraestructura	120	4	TIC, Planificación y Procesos	10
	2.8. Configuración de aplicaciones y sistemas	120	4	TIC, Planificación y Procesos	11
	2.9. Mantenimiento de aplicaciones e infraestructura	120	4	TIC, Planificación y Procesos	12
	2.10. Requerimientos de usuarios	120	4	TIC, Planificación y Procesos	13
	TOTAL HORAS	**1.680**			

Como se puede observar en esta tabla, el tiempo requerido para la ejecución de estos planes de acción es de ±10 meses (1.680 horas hombre) con 7 recursos de los departamentos de: "TIC", Planificación y Procesos, Riesgos, Talento

Humano, Asesoría Jurídica, Gerencia General, Asamblea General, trabajando 8 horas diarias.

En el caso de los procedimientos e instructivos, el tiempo de ejecución puede reducirse si las actividades o tareas se realizan en paralelo. En otras palabras, se elaboran, se revisan, se aprueban y se difunden al mismo tiempo, los procedimientos o instructivos indicados en la Tabla 28.

Si este fuera el caso, se requerirá la contratación de 2 recursos más para el Departamento de “TIC”, ya sean de forma temporal o fija; con esto, se reduciría el tiempo de ejecución de la documentación de esta tarea a ± 3 meses; y los Planes de Acción – Tareas, pasarían de 10 a 6 meses aproximadamente, con 9 recursos y un trabajo de 8 horas diarias.

Se recomienda considerar esta alternativa, el contratar 2 recursos más al Departamento de “TIC”, tomando en cuenta que el principal problema identificado en este trabajo de titulación, es la falta de documentación de las actividades TI actuales.

5.6.3.2 Resumen de recursos del Plan de Mejoras - Proyectos

La Tabla 31 detalla el tiempo que tomará la implementación del Portafolio y Catálogo de servicios TI, mediante la ejecución de proyectos. Los componentes indicados en esta tabla son:

1. Plan de Acción: Detalla sobre que se implementará el proyecto

2. Actividades de “TIC”: Se implementará en las 13 actividades de “TIC2

3. Proyecto: Describe el proyecto que se aplicará en las actividades de “TIC”.

4. Tiempo Estimado (meses): Corresponde al esfuerzo requerido en horas para efectuar la documentación.

5. Nro. Recursos: Es el número de recursos estimado para la ejecución de la documentación

6. Áreas: Se describe el área al que se está efectuando el cambio.

7. Prioridad: Es la categoría asignada para ejecutar la actividad, es decir, el orden en el que se sugiere la implementación de política y documentaciones que se requiere registrar.

   A continuación, se presenta la Tabla 31:

Tabla 31.

Tiempos requeridos para la ejecución del Plan de acción - Proyecto

Pedro Moncayo Ltda.
COOPERATIVA DE AHORRO Y CRÉDITO
Apoyando al Desarrollo de la Comunidad

RESUMEN DE RECURSOS Y TIEMPOS ESTIMADOS PARA PLAN DE ACCIÓN – PROYECTOS

Plan de Acción	Actividades de "TIC"	Proyecto	Nro. Recursos	Áreas / Departamentos	Prioridad	Tiempo Estimado (meses)	Tiempo Estimado por Prioridad (meses)
3. Implementar el portafolio y el catálogo de servicios TI en el Departamento de "TIC", que se ajuste a las necesidades del negocio y permita alinearse a las metas estratégicas de la Cooperativa.	3.1. Gestión de Proveedores	Implementar el servicio de Gestión de Proveedores	5	TIC, Planificación y Procesos, Riesgos, Negocios, Asesoría Jurídica	1	3	4
	3.2. Gestión de Mesa de Ayuda	Implementar el servicio de Gestión de Mesa de Ayuda	2	TIC, Planificación y Procesos	1	2	
	3.3. Gestión de Niveles de Servicio	Implementar el servicio de Gestión de Niveles de Servicio	4	TIC, Planificación y Procesos, Negocios, Asesoría Jurídica	1	2	
	3.4. Gestión de Operación TI	Implementar el servicio de Gestión de Operación TI	2	TIC, Planificación y Procesos	1	2	
	3.5. Gestión de Aplicaciones	Implementar el servicio de Gestión de Aplicaciones	2	TIC, Planificación y Procesos	2	4	4
	3.6. Gestión de Eventos	Implementar el servicio de Gestión de Eventos	3	TIC, Planificación y Procesos, Riesgos	2	3	
	3.7. Gestión de Incidentes	Implementar el servicio de Gestión de Incidentes	5	TIC, Planificación y Procesos, Riesgos, Negocios, Talento Humano	2	4	
	3.8. 3.8. Gestión de Problemas	Implementar el servicio de Gestión de Problemas	3	TIC, Planificación y Procesos, Riesgos	2	3	
	3.9. Gestión de Cambios	Implementar el servicio de Gestión de Cambios	4	TIC, Planificación y Procesos, Riesgos, Negocios	3	4	4
	3.10. Gestión de Configuraciones	Implementar el servicio de Gestión de Configuraciones	2	TIC, Planificación y Procesos	3	4	
	3.11. Gestión de Conocimiento	Implementar el servicio de Gestión de Conocimiento	3	TIC, Planificación y Procesos, Talento Humano	3	3	
	3.12. Gestión de Requerimientos	Implementar el servicio de Gestión de Requerimientos	2	TIC, Planificación y Procesos	3	2	

	3.13. Gestión Técnica	Implementar el servicio de Gestión Técnica	2	TIC, Planificación y Procesos	3	2	
						TOTAL MESES:	**12**

Como se muestra en la Tabla 31, el total de meses que tomará efectuar el Plan de Acción – Proyecto, con 11 recursos, trabajando 8 horas diarias es ± 10 meses, siempre y cuando se puedan ejecutar los proyectos propuestos de manera paralela. Para que sea viable esta propuesta, se definió 3 prioridades, las mismas se explican a continuación:

Prioridad 1:

Los proyectos que se proponen efectuar en parálelo con prioridad 1 son:

3.1. Gestión de Proveedores
3.3. Gestión de Operación TI
3.6. Gestión de Mesa de Ayuda
3.7. Gestión de Nivel de Servicios

En esta propuesta se estima un tiempo aproximado de 4 meses con 6 recursos de los departamentos: Tecnología de la Información y Comunicaciones, 2 recursos; Planificación y Procesos, 1 recursos; Riesgos, 1 recurso; Negocios, 1 recurso y Asesoría Jurídica, 1 recurso.

Se debe tomar en cuenta que los recursos de los departamentos de Riesgos, Negocios y Asesoría Jurídica tienen el rol de usuarios consultores. En el caso del recurso de Planificación y Procesos, intervendrá en el relevamiento y documentación de cada actividad IT. En cambio, los recursos del departamento de “TIC”, son quienes implementarán cada proyecto.

Prioridad 2:

Los proyectos que se proponen efectuar en parálelo con prioridad 2 son:

3.4. Gestión de Aplicaciones
3.9. Gestión de Problemas
3.10. Gestión de Eventos
3.11. Gestión de Incidentes

En esta propuesta también se estima un tiempo aproximado de 4 meses con 6 recursos de los departamentos: Tecnología de la Información y Comunicaciones, 2 recursos; Planificación y Procesos, 1 recursos; Riesgos, 1 recurso; Negocios, 1 recurso y Talento Humano, 1 recurso.

En esta prioridad también se debe considerar que los recursos de los departamentos de Riesgos, Negocios y Talento Humano tienen el rol de usuarios consultores. En el caso del recurso de Planificación y Procesos, intervendrá en el relevamiento y documentación de cada actividad IT. En cambio, los recursos del departamento de “TIC”, son quienes implementarán cada proyecto.

Prioridad 3:

Los proyectos que deben efectuar con prioridad 3 son:

3.2. Gestión Técnica
3.5. Gestión de Configuraciones
3.8. Gestión de Requerimientos
3.12. Gestión de Cambios
3.13. Gestión de Conocimiento

En esta propuesta también se estima un tiempo aproximado de 4 meses con 7 recursos de los departamentos: Tecnología de la Información y Comunicaciones, 3 recursos; Planificación y Procesos, 1 recursos; Riesgos, 1 recurso; Negocios, 1 recurso y Talento Humano, 1 recurso.

En la implementación de los proyectos 3.2, 3.5, 3.8 y 3.12, los recursos de los departamentos de Riesgos y Negocios tienen el rol de usuarios consultores. El recurso de Planificación y Procesos, intervendrá en el relevamiento y documentación de cada actividad IT y los recursos de “TIC”, ejecutarán los mismos.

Para el Proyecto de Gestión de Conocimiento, Talento Humano y Planificación y Procesos, deberán implementarlo y el departamento de “TIC” tendrá que apoyar como usuario experto. Por tal motivo, para la ejecución de este proyecto, se necesita 1 recurso TI adicional, ya sea de forma temporal o fija.

La ejecución del Plan de Acción - Proyecto en su totalidad, considerando las 3 prioridades, tiene un tiempo estimado de implementación de ± 12 meses con 8 recursos, la jornada de trabajo será de 8 horas diarias sin considerar los días no laborables (feriados y fines de semana).

6 Conclusiones y Recomendaciones

En este capítulo se detallará conclusiones y recomendaciones que se han obtenido de este trabajo de titulación.

6.1 Conclusiones

Las conclusiones a las que se llegó son:

De acuerdo a la investigación efectuada en el presente proyecto de titulación, la mayoría de los productos y servicios ofrecidos a los clientes de la Cooperativa, son a través del uso de la tecnología, generando un valor al negocio; por lo que, en el Mapa de Procesos, el Departamento de Tecnología de la Información y Comunicaciones no puede estar considerado como un área de apoyo, tal cual está actualmente, sino más bien como un Proceso Operativo, enfocado a la funcionalidad del negocio y su operación, al ser un pilar fundamental para el logro de los Objetivos Estratégico de la Cooperativa.

La revisión de las diferentes metodologías, tales como: Framework COBIT 5, COBIT 5 para Riesgos, Risk IT y Guía Práctica del Profesional, permitió conocer: los escenarios de riesgos, el grado de madurez de las actividades TI actuales, el listado de activos de información, entre otros del Departamento de Tecnología de la Información y Comunicaciones; de esta manera, utilizando el Plan de Mejoras presentado en este estudio de investigación, se puede mitigar los riesgos para evitar pérdidas económicas por indisponibilidad del servicio.

El grado de madurez de las actividades actuales del Departamento de “TIC” de la Cooperativa “Pedro Moncayo Ltda.”, es 0 - Procesos Incompletos. Esto se debe a que ninguna actividad TI se encuentra documentada, tampoco mantiene definido el flujo de gestión de los procesos a nivel de responsables, de funcionalidad y de participantes; con estos antecedentes, la Gerencia puede

focalizar las actividades que requieren mayor atención y aplicar acciones de correctivas oportunas, en base al Plan de Acciones presentado en el capítulo anterior de este trabajo de investigación.

La metodología utilizada en este proyecto permitió priorizar y clasificar los 3 riesgos existentes con criticidad “Alta”, inherentes a las Metas del Negocio de la Cooperativa. Dentro de esta priorización, se ha podido determinar que el riesgo R1 – Pérdida económica, es el que mantiene una alta probabilidad de ocurrencia y un alto impacto que puede afectar directamente a la operación, productividad e imagen o reputación corporativa de COAC “Pedro Moncayo Ltda.”, por reclamos de clientes o socios y por la falta de los servicios de terceros.

Es indispensable el apoyo de la Gerencia General de COAC “Pedro Moncayo Ltda.” para la ejecución del Plan de Mejoras desarrollado en este trabajo de investigación, lo que permitirá eliminar los problemas identificados en el Departamento de “TIC” y mitigar los riesgos con criticidad “Alta” que pueden afectar a la operación del negocio, tomando en cuenta las actividades o tareas a implementar de acuerdo a las metas estratégicas planteadas.

Dentro del Portafolio de Servicios TI, indicado en el Plan de Mejoras, es indispensable que el Departamento de “TIC” cuente con un servicio de Service Desk o Mesa de Ayuda que le permita tener centralizado la atención de requerimientos, soportes, problemas o incidentes, estableciendo por lo menos 3 niveles de servicio:

Alto, cuya prioridad es “0”. La atención debe ser inmediata, cuando se trate de una afectación directa a la operación de la Cooperativa y no existe continuidad del negocio.

Medio, cuya prioridad es “1”. Hay indisponibilidad del servicio, pero depende del nivel de impacto al negocio y la afectación a la atención de los clientes, ya sea

por inconvenientes en los sistemas, plataformas o aplicaciones considerados como críticos para la operación de la Cooperativa.

Bajo, cuya prioridad es “2. Existe indisponibilidad de un servicio puntual ya sea de un sistema, plataforma o aplicación; sin embargo, la operación normal del negocio no es afectada.

El Plan de Mejoras presentado en este proyecto de titulación, se ha dividido en Planes de Acción para actividades o tareas TI y en Planes de Acción para proyectos TI, en los que se han establecido los recursos, tiempos estimados y prioridades para la implementación de las acciones requeridas para minimizar los riesgos identificados en COAC “Pedro Moncayo Ltda.”

La ejecución de los Planes de Acción de las tareas se ha estimado durante un tiempo de ± 6 meses, donde las tareas TI se realizarán de forma secuencial, con 7 recursos y un esfuerzo diario de 8 horas laborables. El plan propuesto establece la contratación temporal o fija de 2 recursos adicionales para el departamento de Tecnología de Información y Comunicaciones.

Para la implementación del Plan de Acción de los Proyectos, se ha considerado el priorizar los proyectos para que puedan ser ejecutados de forma paralela y de esta manera reducir el tiempo a ± 12 meses con 8 recursos, la jornada de trabajo será de 8 horas diarias sin considerar los días no laborables (feriados y fines de semana). Dentro de esta estimación está considerado la contratación temporal o fija de 1 recurso adicional para el Departamento de “TIC”.

Dado que, en esta investigación, no fueron tomados en cuenta los 2 riesgos con criticidad “Meda” y “Baja”, es necesario considerarlos dentro de otro proyecto de titulación, para garantizar que exista una mitigación completa de los riesgos identificados en la Cooperativa de Ahorro y Crédito “Pedro Moncayo Ltda.”

6.2 Recomendaciones

En base a los resultados obtenidos en este estudio investigativo se recomienda:

Colocar al Departamento de “TIC”, dentro de los Procesos Operativos del Mapa de Procesos; dado que, la tecnología es usada en todas las fases de gestación de los productos y servicios ofrecidos a los clientes, convirtiéndole a este departamento en un pilar fundamental para la operación del negocio.

Utilizar ITIL como un marco de trabajo en el Departamento de Tecnología de la Información y Comunicaciones para que le permita contar con un Portafolio y Catálogo de servicios TI, muy necesarios dentro de las actividades y procesos propios de COAC “Pedro Moncayo Ltda.

Iniciar la ejecución de las acciones indicadas en el Plan de Mejoras desarrollado en este proyecto de investigación para disminuir los riesgos que pueden provocar:

Pérdida económica.
Pérdida de confiabilidad.
Falta de implementación de servicios tecnológicos.

Constituir el Comité de Riesgos, que permita gestionar, controlar y tomar decisiones sobre las acciones a realizar para disminuir o mitigar los riesgos existentes de la Cooperativa. Este Comité deberá estar integrado por los siguientes departamentos:

Gerencia General
Riesgos
Cumplimiento
Negocios
Operaciones

Tecnología de la Información y Comunicaciones
Auditoría Interna

Establecer los niveles de servicio de forma interna con los departamentos de la Cooperativa y de forma externa con las empresas proveedoras de servicio, para garantizar una atención oportuna, en base a una priorización de los requerimientos dada por su criticidad en la operación del negocio.

Realizar un seguimiento Semanal del avance de la implementación del Plan de Mejoras por parte del Comité de Administración de la Cooperativa de Ahorro y Crédito “Pedro Moncayo Ltda.”, que les permita tomar decisiones a tiempo, en caso de existir problemas o inconvenientes en la ejecución de este plan.
Establecer un plan de mejoras para los 2 riesgos categorizados con criticidad “Medio” y “Bajo”, como parte de una segunda fase, que permita mitigar los riesgos identificados en este proyecto de titulación.

REFERENCIAS

Ciifen. (2011). *Definición del Riesgo*. Recuperado el 9 de Julio de 2016 de http://www.ciifen.org/index.php?option=com_content&view=category&id=84&layout=blog&Itemid=111&lang=es

COAC "Pedro Moncayo" Ltda. (2016). *COAC Pedro Moncayo Ltda - Transparencia*. Recuperado el 23 Marzo de 2016 de https://www.copedromoncayo.fin.ec/images/Balances/IndicadoresFinancieros.pdf

COAC. (2016). 20150319 Organigrama Propuesto P Moncayo 04 (Final).pdf

Cooperativa de Ahorro y Crédito Pedro Moncayo Ltda. (2016). *02 Plan estratégico PM 2015 2017.*

Dávila R., F. (2014). *PLAN ESTRATÉGICO 2015 - 2017.*

Gutierrez Amaya, H. C. (s.f.). *MAGERIT: metodología práctica para gestionar riesgos*. Recuperado el 11 de Julio de 2016 de http://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2010). *Metodología de la investigación.* México: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

Huerta, A. (2012). Introducción al Análisis de Riesgos. Recuperado el 20 de Julio de 2016 de *https://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/*.

Huerta, A. (2012). *Introducción al análisis de riesgos – Metodologías*. Recuperado el 20 de Julio de 2016 de

http://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/

Internic. (2015). *CRAMM (Análisis de Riesgo de la ACTC y método de gestión)*. Recuperado el 25 de Julio 2016 de https://managementmania.com/en/cramm-ccta-risk-analysis-and-management-method

ISACA . (2009). *Marco de Riesgos de TI.* ISACA.

ISACA. (2009). Risk-IT-Overview. *Risk-IT*.

ISACA. (2009). *The Risk IT Practitioner Guide.* ISACA.

ISACA. (2012). *COBIT 5 AN ISACA FRAMEWORK.*

ISACA. (2012). *COBIT 5 Framework Spanish.* Madrid: Capítulo de Madrid de ISACA.

ISACA. (2013). *COBIT 5 para Riesgos.* ISACA.

MIES. (2012). LEY ORGÁNICA DE LA ECONOMÍA POPULAR Y SOLIDARIA . *LEY ORGÁNICA DE LA ECONOMÍA POPULAR Y SOLIDARIA* . Quito, Ecuador.

Miguel Angel Mendoza. (2015). *Weblivesecurity*. Recuperado 02 de Agosto de 2016 de http://www.welivesecurity.com/la-es/2015/02/11/desafios-planes-seguridad-para-pymes/

OGC. (2010). *ITIL®: Service Strategy.* TSO.

PAe. (s.f). *MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Recuperado el 10 de Agosto de 2016 de http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.V-X5zSjhA2w

Project Management Institute. (2014). *Guìa de Fundamentos para la Direcciòn de Proyectos 5ta. Edición.* Project Management Institute Inc.

SANS Institute. (2007). *A Qualitative Risk Analysis and Management Tool - CRAMM.* Recuperado 25 de Agosto de 2016 de https://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83

SEPS. (2011). Recupeado el 25 de Agosto de 2016 de http://www.seps.gob.ec/noticia?que-es-la-economia-popular-y-solidaria-eps

WordPress, B. d. (2012). Recuperado el 28 de Agosto de 2016 de *https://francoitgrc.wordpress.com/2014/11/26/15/*.

Zuñiga, A., & M. S. (2016). *in@SlideShare*. Recuperado el 28 de Agosto de 2016 de http://es.slideshare.net/LeoGomez3/riesgo-de-ti: http://es.slideshare.net/LeoGomez3/riesgo-de-ti

ANEXOS

Anexo 1. Entrevistas

Se adjunta resumen de las entrevistas efectuada al Jefe de Sistema y al Analista del Departamento de “TIC”

Entrevista N1 - Proceso 46 - Configuración y asignación de ip de red a nuevos usuarios.

Interpretación: No se tiene procedimientos documentados para efectuar Configuración y asignación de direcciones lógicas IPs.

La ejecución se efectúa por pedido de la Gerencia dado que no existe un proceso definidos de solicitud, gestión de los requerimientos; tampoco tienen establecidos tiempos para la atención.

Análisis: En base a las respuestas dadas, las actividades se realizan por conocimiento y expertiz del Jefe o Analista del departamento de “TIC”.

Entrevista N1	**Proceso 46 - Configuración y asignación de ip de red a nuevos usuarios**	
Realizado por:	**Fany Cacuango y Erika Mora**	
	SI	**NO**
Existe procesos definidos para la asignación de ips a los usuarios?		X
Existe procesos para gestionar requerimientos para la asignación del nuevo ip?		X
Existe política de comunicación para distribuir las ips por departamentos?		X
Existe procesos de verificación para la instalación/mantenimiento/reconfirmación de punto de red?		X
Existe diagrama de estructura de la red?		X
Tiene poyecto para levantar los procesos del departamento de tecnología?	X	

Observación:
-El Gerente notifica directamente que se instale el nuevo puesto y punto de red.
- No se tienen documenta de standares para procesos
- Se está armando los procesos del departamento de tecnología

Entrevista N2 - Proceso 47 - Configurar una nueva cámara de seguridad

Interpretación: No se tiene procedimientos documentados para efectuar la instalación de la aplicación para el control de asistencia.

Análisis: En base a las respuestas dadas, la aplicación no es centralizada, para la instalación deben trasladarse físicamente a cada agencia.

No monitorean eventos inusuales o anómalos registrados dentro o fuera de las instalaciones Cooperativa. El uso que le dan a esta actividad, es para control de reclamos de clientes por un tiempo máximo de 3 meses.

Entrevista N2	**Proceso 47 - Configurar una nueva cámara de seguridad**	
Realizado por:	**Fany Cacuango y Erika Mora**	
	SI	**NO**
Existe procesos establecidos para cambios de cámara de seguridad?		X
Actualmente el departamento de TIC administran el sistema de la cámara de	X	
Tiene procesos establecidos para custodia de los videos?	X	
Tiene procesos de custodia de los videos?		X
Existe procesos definidos de mantenimiento de cámada?		X
Está asignado a un grupo de la cooperativa para el monitoreo de las pantallas?		X

Observación:
-El Gerente aprueba toda compra - Disponen 10 cámaras, admistran el sistema: configura, reemplaza la camara - El proceso lo utiliza para soporte de entrega de información

Entrevista N3 - Proceso 47 - Configurar de aplicativos de control de asistencias

Interpretación: No se tiene procedimientos documentados para efectuar la instalación de la aplicación de control de ingreso y salida.

Análisis: En base a las respuestas dadas, se deben trasladar físicamente a las agencias. La información de control de registros de ingreso/salidas no está centralizado lo que ocasiona retrasos en el cuadre para el pago de horas extras.

Entrevista N3	Proceso 48 - Configuración de aplicativos de control de asistencia
Realizado por:	Fany Cacuango y Erika Mora

	SI	NO
Existe procesos establecidos para crear, eliminar usuarios del sisntea de control de asiste		X
Realizan procesos de inducción del uso de la aplicación?	X	
Tiene procesos establecidos para custodia de los videos?	X	
Generan reportes de control de asistencia para otras Areas?		
La aplicación de control de asistencias está centralizada?		X

Observación:
- Se aplica en cada agencia
- No tiene procesos centralizado
- El control se realiza tardíamente

Entrevista N4 - Proceso 49 - Configurar de Pin Pad

Interpretación: Para brindar servicios adicionales a los clientes instalan Pin Pad en la máquina del Jefe de Departamento de Operaciones.

Análisis: No existen controles para la implementación ni procesos que le hayan enviado a el Departamento de “TIC”.

Se ve riesgos la instalación en un solo equipo, no existen respaldos ni de equipo y tampoco de personas para que pueda continuar con el servicio de tener el caso de ausentismo.

Entrevista N4	Proceso 49 - Configuración de Pin Pad
Realizado por:	Fany Cacuango y Erika Mora

	SI	NO
Existe procesos establecidos installar Pin Pad?		X
Se instala a todos las áreas operativas de la Cooperativa?		X
Existe procesos de despliegue para la instalación del Pin Pad?		X
Es administrada por el departamento de TIC?		X
La aplicación de control de asistencias está centralizada?		X

Observación:
Por normativa las tarjetas deben tener chip por lo que requiere el servicio se canaliza con CONECTA

Entrevista N5 - Proceso 49 – Configuración de cuentas de correo electrónico.

Interpretación: No existe cuentas de correo electrónico para cada persona, la asignación de correo electrónico es para cada departamento.

Análisis: Se debe revisar las políticas internas de asignación de correo para que se personalicen y que existe control de filtrados de información.

Se debe implementar procesos y políticas nuevas para poder inclusive sancionar a los usuarios que no hagan uso adecuado de la información.

Entrevista N5	Proceso 50 - Configuración de cuenta de correo electrónico a nuevo usuario
Realizado por:	Fany Cacuango y Erika Mora

	SI	NO
Existe procesos establecidos para asignar las cuentas de correo electrónico?		X
Se asignan cuentas a cada usuario?		X
Existen procesos de backups de los correos?		X
Tienen asignado responsables de cuentas por area?		x

Observación:
No tienen polítcas o reglamentos para la asignación de los correos

Entrevista N6 - Proceso 03 – Mantenimiento Físico de ATMs (Cajero Automático)

Interpretación: El mantenimiento al cajero automático se ejecuta el chequeo del sistema operativo por medio de instrucciones y esperar que el sistema se reestablezca.

Análisis: No tienen ningún proceso establecido para informar de las actividades realizadas ni registro de la ejecución trimestral que se efectúa.

Según lo que nos informan los entrevistados (Jefe y Analista de Sistemas) de presentar cualquier novedad proceden a informar al proveedor. Revisando la documentación de procesos para escalamientos no existe y tampoco forma de medir tiempos de respuesta de parte de los proveedores.

Entrevista N6	Proceso 03 - Mantenimiento Físico de Atms
Realizado por:	Fany Cacuango y Erika Mora

	SI	NO
Existe procesos establecidos para ejecutar el chequeo preventivo al cajero físico?		X
Actualmente el departamento de TIC informa el estado de revisiones ejecutado a los cajeros físicos?	X	
Tiene procesos establecidos la operatividad del cajero físico?		X
Tiene procesos escalar daños físicos que presente el cajero?		X
Existe procesos definidos de mantenimiento de cámada?		X
Está asignado a un grupo de la cooperativa para el monitoreo de las pantallas?		X

Observación:
- Chequeo Trimestral
- Reportan daños a proveedor

Entrevista N7 - Proceso 14 al 19 – Procesos de creación de usuarios a la aplicación.

Interpretación: La ejecución de creación de usuarios, reseteo, inhabilitación de usuarios en el sistema se lo efectúa en base a notificaciones verbales y en pocas ocasiones por e-mail.

Análisis: Es requerido que existe procesos y políticas para gestionar la atención de creación/resteo/inhabilitación de usuarios con el objetivo que puedan continuar con sus actividades diarias sin que se interrumpa la atención de la operación de la Cooperativa.

Entrevista N7	Proceso 14 a 19 - Procesos de creación de usuarios a las aplicaciones de la cooperativa		
Realizado por:	Fany Cacuango y Erika Mora		

	SI	NO
Existe procesos establecidos para creación de usuarios a las diversas aplicaciones?		X
Tienen roles definidos para la asignación de los perfiles?	X	
Tienen tiempos establecidos para la creación y notificación de los usuarios?		X
Los requerimientos son solicitados por medios de mails o forma verbal?	X	
El comunicado de asignación de roles lo efectúa el departamente de Talento Humano?	X	

Observación:
- El comunicado de ingreso y areas a la que los recursos ingresa lo hacen de forma verbal, no tienen comunicados por mail o requerimientos.
- Los requerimientos son por teléfono

Entrevista N8 - Proceso 21 al 26 – Instalación de Aplicaciones.

Interpretación: No tienen proceso documentados para la ejecución de implementación de aplicaciones, el expertiz lo han adquirido en base al trabajo diario que realizan.

Análisis: No tienen ningún proceso establecido para la implementación o actualización de cambios de versiones que se realizan en Core Financial, esto podría ocasionar que tengan una indisponibilidad en los servicios afectando a los clientes.

Entrevista N8	Proceso 21 al 26 - Intalación de aplicaciones
Realizado por:	Fany Cacuango y Erika Mora

	SI	NO
Existe procesos establecidos para implementación de aplicaciones a empleados?		X
Tienen roles definidos para la asignación de los perfiles?	X	
Tienen tiempos establecidos para la creación y notificación de los usuarios?		X
Los requerimientos son solicitados por medios de mails o forma verbal?	X	
El comunicado de asignación de roles lo efectúa el departamente de Talento Humano?	X	
Existes procesos establecidos para comunicar a los usuarios que pueden ingresar a la		X
Requiere soporte de proveedores para la intalación de las aplicaciones de terceros?		X
Tienen procesos de SLA defininos para gestión de requerimientos?		X
Existen procesos de solicitud de atención a incidentes o nuevos requerimientos?		X
Gestionan los contratos de proveedor para conocer niveles de serivicio?		X

Observación:
- Las instalaciones es en base a conocimiento emperíco
- Tiempos de atención de requerimientos no existen, gestión y soporte se efectúan de forma telefónca

Entrevista N9 - Proceso 21 al 26 – Creación de Usuarios y Reseteo de Claves

Interpretación: La ejecución de creación de usuarios, reseteo, inhabilitación de usuarios en el sistema se lo efectúa en base a notificaciones verbales y en pocas ocasiones por e-mail.

Análisis: Es requerido que existe procesos y políticas para gestionar la atención de creación/resteo/inhabilitación de usuarios con el objetivo que puedan continuar con sus actividades diarias sin que se interrumpa la atención de la operación de la Cooperativa.

Entrevista N9	Proceso 21 al 26 - Creación de Usuarios y Reseteo de Claves
Realizado por:	Fany Cacuango y Erika Mora

	SI	NO
Existe procesos establecidos para implementación de creación de usuarios y reseteo de claves?		X
Tiene tiempos definidos para la ejecución del proceso?		X
Tiene procesos definidos para efectuar la notificación de finalización del proceso?		X
Tiene algorimos establecidos para la generación de claves?	X	
Los usuarios son presonalizadas en cada aplicación?		
Requieren soportes para la asignación de usuarios de aplicaciones de terceros?	X	
Tienen contratos de niveles de servicios con proveedores?		X

Observación:
-

Entrevista N10 - Proceso 21 al 26 – Instalación de aplicaciones

Interpretación: No tienen documentado la actividad de instalación de aplicaciones, pero se instala en base al expertiz técnico considerando datos generales como: Asignación de puesto de trabajo (rol), perfil, aplicación que utilizarán, software base, software utilitario.

Análisis:

De presentarse cualquier error en la instalación no se cuenta con un tiempo de respuesta establecido y tampoco el usuario tiene el proceso definido para reportar novedades o incidentes.

Entrevista N 10	Proceso 21 al 26 - Intalación de aplicaciones		
Realizado por:	Fany Cacuango y Erika Mora		
		SI	NO
Existe procesos establecidos para implementación de aplicaciones a empleados?			X
Tienen roles definidos para la asignación de los perfiles?		X	
Tienen tiempos establecidos para la creación y notificación de los usuarios?			X
Los requerimientos son solicitados por medios de mails o forma verbal?		X	
El comunicado de asignación de roles lo efectúa el departamente de Talento Humano?		X	
Existes procesos establecidos para comunicar a los usuarios que pueden ingresar a la			X
Requiere soporte de proveedores para la intalación de las aplicaciones de terceros?			X
Tienen procesos de SLA defininos para gestión de requerimientos?			X
Existen procesos de solicitud de atención a incidentes o nuevos requerimientos?			X
Gestionan los contratos de proveedor para conocer niveles de serivicio?			X
Observación:			

Entrevista N10 - Proceso 51 al 53 – Respaldo de Base de Datos

Interpretación: No tienen procesos establecidos para efectuar respaldos de la Base de Datos lo que efectúa es ejecutar desde línea de comandos “export” de la BDD del sistema Financial. Tampoco existen procesos para efectuar recuperaciones y tampoco esquemas de validación de integridad de los datos.

Análisis: Se debe estructurar un plan de ejecución de respaldos para asegurar la integridad de información, custodiar la información en lugares de almacenamientos propios, etiquetar las cintas. Como parte del plan debe existir un proceso de recuperación y que se verifique la consistencia de la información almacenada en la BDD.

Entrevista N 11	Proceso 51 y 53 - Resplado de Base de Datos y Recuperación de BDD
Realizado por:	Fany Cacuango y Erika Mora

	SI	NO
Existe procesos establecidos para efectuar respaldos y recuperación de BDD del Core?		X
Tiene otro ambiente para efectuar la recuperación de la BDD del Core?		X
Tienen tiempos establecidos para habilitar una nueva BDD?		X
Tienen procesos para efectuar la custodia de información?		X
Tiene procesos para etiquetar respaldos?	X	
Tienen procesos para verificar que una restauración de BDD está completa?		X
Cumplen con el procesos de LOPS de almacenamiento?	X	

Observación:

En el siguiente cuadro se consolida las respuestas que los dueños de los procesos dieron a las preguntas que se efectuaron, esto permitió levantar por medio de lluvias de ideas 22 problemas que se identificaron.

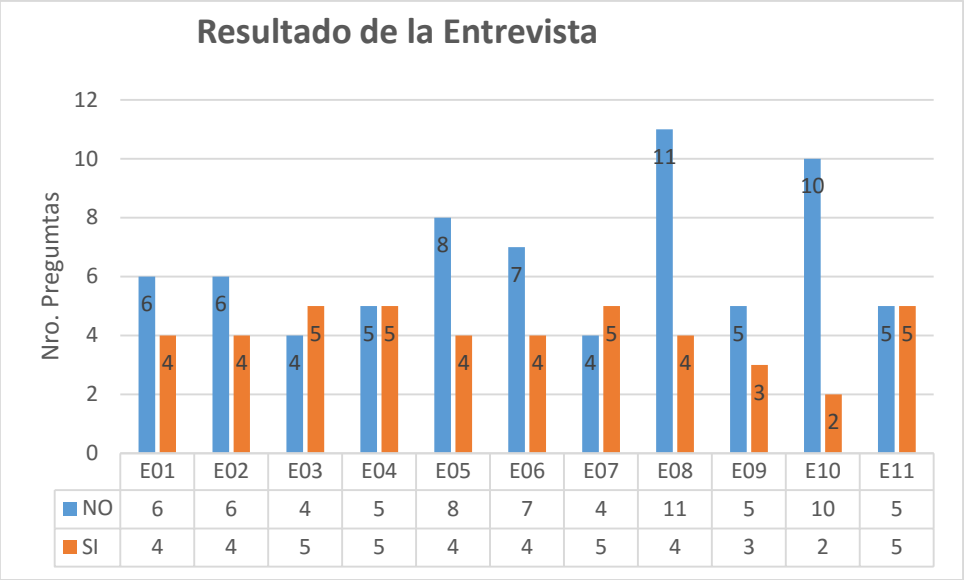
Para dar prioridad a los problemas se aplicó la priorización de forma cualitativa, el resultado de la misma es tener identificado 9 problemas sobre lo que se aplica el análisis de riesgos y mapeos utilizando la matriz IPM.

Consolidado de la Entrevista - Cooperativa "Pedro Moncayo Ltda."

No	Preguntas Generales	E01	E02	E03	E04	E05	E06	E07	E08	E09	E10	E11
1	Existe procesos definidos para gestión de los procesos de TIC ……...?	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
2	Existe procedimientos definidos para atención de requerimientos …….?	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
3	Existe tiempos establecidos para la gestión de los requerimientos internas?	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
4	Existe procesos de verificación para la instalación/mantenimiento/reconfirmación de punto de red, equipos/, configuración, ect?	NO	NO	NO	NO	NO	NO	SI	NO	NO	NO	NO
5	Los sistemas internos y extenos lo administra TIC?	-	-	-	NO	-	-	-	NO	-	NO	-
6	Tienen procesos de backup, restauración para los procesos de BDD y cámara de vigilacia?	-	-	-	-	-	-	-	NO	-	-	SI
7	Tiene procesos de SLA para provedores?	NO	NO	-	-	NO	NO	-	NO	-	NO	NO
8	Tienen roles y permisos establecidos para el cumplimientos de las tareas?	SI	SI	SI	SI	SI	SI	SI	SI	-	NO	SI
9	Cuenta con el personal suficiente para el desarrollo de los procesos?	NO	NO	SI	SI	NO	NO	NO	NO	-	NO	SI
10	Existe procesos establecidos para validar cambios de proveedores?	-	-	-	-	NO	-	-	NO	-	NO	-
11	Cumplen con los procesos de seguridad definidos por la LOPS?	-	-	-	-	NO	NO	-	NO	NO	-	SI
12	Las ejecuciones de procesos se efectúan en base a conocimiento adquirido	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
13	Existe proyectos para generar la documentación y flujos requeridos?	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
14	Ejecutan bajo cierta frecuencia los procesos?	SI	SI	SI	SI	SI	SI	SI	SI	SI	NO	SI

El cuadro siguiente consolida las preguntas efectuadas a los dueños de los procesos de Operaciones, Negocio y Tecnología TI, determinando que 4 procesos requieren que se apliquen planes de acción dado que afectan a los usuarios internos y podrían ocasionar indisponibilidad del servicio.

- Proceso 50 - Configuración de cuenta de correo electrónico a nuevo usuario
- Proceso 14 a 19 - Procesos de creación de usuarios a las aplicaciones de la cooperativa
- Proceso 21 al 26 - Instalación de aplicaciones



Resultados de la Entrevista

Anexo 2. Matriz de Riesgos

La Tabla 41 presenta la información detallas que se utilizó para medir los riesgos. Información que contiene son os riesgos asociado a las amenazas y vulnerabilidades que se ha identificado en las actividades que el Departamento de “TIC”.

COD. RIESGO	RIESGO	INCIDENTE / PROBLEMA IDENTIFICADO	AMENAZA	VULNERABILIDAD	CONTROLES EXISTENTES IDENTIFICADOS	CRITICIDAD	PROBABILIDAD	IMPACTO
R1	Pérdida económica por indisponibilidad del servicio provocada por falla en los sistemas tecnológicos	P01. No existe documentación sobre la operación de las actividades de "TIC". P02. No existe ninguna actividad de gestión de eventos y gestión de incidentes. P03. No existe ninguna actividad de custodia de información. P04. No existe ninguna actividad de restauración de base de datos. P05. No existe ninguna actividad de gestión de solución de problemas. P06. No existe ninguna actividad de gestión de niveles de servicio. P07. No existe ninguna actividad de gestión de proveedores. P08. No existe ninguna actividad de gestión de seguridad P09. No cuentan con una inducción adecuada de las actividades internas	P01-A1- La actividad de monitoreo se lo lleva de manera empírica, es decir, no tiene están documentadas. P02-A1. No tienen actividades de gestión: solicitudes, requreimientos e incidentes P04-A1. Pérdida de clientes P05-A1. Afectación a los usuarios internos en su productividad P06-A1. Incumplimiento de proveedores por no contar con acuerdos de niveles de servicio P07-A1. Desconocimiento de escalamiento a proveedores P08-A1. No existe ninguna cultura sobre el cuidado y protección de las credenciales de usuarios P09-A1. Falta de conocimiento del flujo de actividades internas entre áreas para requerimientos de TI	P01-V1. El conocimiento del flujo y la operativa de este proceso lo tiene el Jefe del área de Tecnología de la Información y Comunicaciones únicamente P02-V1. La actividad de monitoreo no posee niveles de atención para resolución de eventos o incidentes tecnológicos internos (empleados, funcionarios de la Cooperativa) o externos (clientes) P02-V2. No tiene proceso de escalamiento para el restablecimiento de servicio con los proveedores, en base a la criticidad, frecuencia e impacto que ayude a erradicar la causa del evento o incidente. P03-V1. Los activos de información que se obtienen principalmente de la base de datos, son primordiales para el negocio. P04-V1.No tiene un proceso formal de restauración de la información que se extrajo de las bases de datos, existe la posibilidad de que los datos no guarden la integridad requerida y esto ocasione problemas legales con los entes de control, con los socios o clientes, con los proveedores, entre otros de la Cooperativa P05-V1. No tiene un proceso de gestión de solución de problemas puede convertirse en una vulnerabilidad crítica que atenta contra la calidad de servicio que la Cooperativa quiere dar a sus clientes o socios. P06-V1. Afectación en tiempo de solución a los usuarios internos/externos P07-V1. No existe un proceso de gestión de proveedores por lo	1. actividad se lo tienen de forma emperíca 2. Reportes a proveedores vía Skype o mail 3. Informalidad de actividades	Alto	5,0	4,0
R2	Pérdida de confiabilidad en los clientes o socios debido a lentitud en la atención y desmejoramiento de la calidad de servicio	P02. No existe ninguna actividad de gestión de eventos y gestión de incidentes. P03. No existe ninguna actividad de custodia de información. P05. No existe ninguna actividad de gestión de solución de problemas. P06. No existe ninguna actividad de gestión de niveles de servicio. P08. No existe ninguna actividad de gestión de seguridad	P02-A1. No tienen actividades de gestión: solicitudes, requreimientos e incidentes P05-A1. Afectación a los usuarios internos en su productividad P06-A1. Incumplimiento de proveedores por no contar con acuerdos de niveles de servicio P08-A1. No existe ninguna cultura sobre el cuidado y protección de las credenciales de usuarios	P01-V1. El conocimiento del flujo y la operativa de este proceso lo tiene el Jefe del área de Tecnología de la Información y Comunicaciones únicamente P02-V1. La actividad de monitoreo no posee niveles de atención para resolución de eventos o incidentes tecnológicos internos (empleados, funcionarios de la Cooperativa) o externos (clientes) P02-V2. No tiene proceso de escalamiento para el restablecimiento de servicio con los proveedores, en base a la criticidad, frecuencia e impacto que ayude a erradicar la causa del evento o incidente. P03-V1. Los activos de información que se obtienen principalmente de la base de datos, son primordiales para el negocio. P04-V1.No tiene un proceso formal de restauración de la información que se extrajo de las bases de datos, existe la posibilidad de que los datos no guarden la integridad requerida y esto ocasione problemas legales con los entes de control, con los socios o clientes, con los proveedores, entre otros de la Cooperativa P05-V1. No tiene un proceso de gestión de solución de problemas puede convertirse en una vulnerabilidad crítica que atenta contra la calidad de servicio que la Cooperativa quiere dar a sus clientes o socios. P06-V1. Afectación en tiempo de solución a los usuarios internos/externos P07-V1. No existe un proceso de gestión de proveedores por lo la Cooperativa puede estar expuesta a robo, destrucción, uso inadecuado de información confidencial y crítica para el negocio.	1. actividad se lo tienen de forma emperíca 2. Reportes a proveedores vía Skype o mail 3. Informalidad de actividades	Alto	4,7	4,0

COD. RIESGO	RIESGO	INCIDENTE / PROBLEMA IDENTIFICADO	AMENAZA	VULNERABILIDAD	CONTROLES EXISTENTES IDENTIFICADOS	CRITICIDAD	PROBABILIDAD	IMPACTO
R3	Pérdida de eficiencia y eficacia de los empleados de la Cooperativa y por incumplimiento a las normativas emitidas por los entes de control debido a desconocimiento de actividades tecnológicos y presencia de eventos anómalos en los sistemas o aplicaciones	P01. No existe documentación sobre la operación de lsa actividades de "TIC". P03. No existe ninguna actividad de custodia de información. P04. No existe ninguna actividad de restauración de base de datos. P05. No existe ninguna actividad de gestión de solución de problemas. P06. No existe ninguna actividad de gestión de niveles de servicio. P07. No existe ninguna actividad de gestión de proveedores. P08. No existe ninguna actividad de gestión de seguridad P09. No cuentan con una inducción adecuada de las actividades internas	P01-A1- La actividad de monitoreo se lo lleva de manera empírica, es decir, no tiene están documentadas. P04-A1. Pérdida de clientes P05-A1. Afectación a los usuarios internos en su productividad P06-A1. Incumplimiento de proveedores por no contar con acuerdos de niveles de servicio P07-A1. Desconocimiento de escalamiento a proveedores P08-A1. No existe ninguna cultura sobre el cuidado y protección de las credenciales de usuarios P09-A1. Falta de conocimiento del flujo de actividades internas entre áreas para requerimientos de TI	P01-V1. El conocimiento del flujo y la operativa de este proceso lo tiene el Jefe del área de Tecnología de la Información y Comunicaciones únicamente P03-V1. Los activos de información que se obtienen principalmente de la base de datos, son primordiales para el negocio. P04-V1.No tiene un proceso formal de restauración de la información que se extrajo de las bases de datos, existe la posibilidad de que los datos no guarden la integridad requerida y esto ocasione problemas legales con los entes de control, con los socios o clientes, con los proveedores, entre otros de la Cooperativa P05-V1. No tiene un proceso de gestión de solución de problemas puede convertirse en una vulnerabilidad crítica que atenta contra la calidad de servicio que la Cooperativa quiere dar a sus clientes o socios. P06-V1. Afectación en tiempo de solución a los usuarios internos/externos P07-V1. No existe un proceso de gestión de proveedores por lo la Cooperativa puede estar expuesta a robo, destrucción, uso inadecuado de información confidencial y crítica para el negocio. P08-V1. El departamento "TIC" no posee ningún actividad de gestión de seguridad que le garantice confidencialidad, integridad y disponibilidad de la información categorizada como crítica.	1. actividad se lo tienen de forma emperica 2. Reportes a proveedores vía Skype o mail 3. Informalidad de actividades	Medio	3,3	3,3
R4	Falta de programas de capacitación o inducción de actividades de gestión de accesos y usuarios de sistemas y aplicaciones	P01. No existe documentación sobre la operación de las actividades de "TIC". P08. No existe ninguna actividad de gestión de seguridad P09. No cuentan con una inducción adecuada de las actividades internas	P01-A1- La actividad de monitoreo se lo lleva de manera empírica, es decir, no tiene están documentadas. P08-A1. No existe ninguna cultura sobre el cuidado y protección de las credenciales de usuarios P09-A1. Falta de conocimiento del flujo de actividades internas entre áreas para requerimientos de TI	P01-V1. El conocimiento del flujo y la operativa de este proceso lo tiene el Jefe del área de Tecnología de la Información y Comunicaciones únicamente P08-V1. El departamento "TIC" no posee ningún actividad de gestión de seguridad que le garantice confidencialidad, integridad y disponibilidad de la información categorizada como crítica.	1. actividad se lo tienen de forma emperica 2. Reportes a proveedores vía Skype o mail 3. Informalidad de actividades	Bajo	2,0	2,0
R5	No se encuentran implementados servicios tecnológicos que permitan robustecer el departamento de "TIC"	P01. No existe documentación sobre la operación de las actividades de "TIC". P02. No existe ninguna actividad de gestión de eventos y gestión de incidentes. P05. No existe ninguna actividad de gestión de solución de problemas. P06. No existe ninguna actividad de gestión de niveles de servicio. P07. No existe ninguna actividad de gestión de proveedores. P08. No existe ninguna actividad de gestión de seguridad	P01-A1- La actividad de monitoreo se lo lleva de manera empírica, es decir, no tiene están documentadas. P02-A1. No tienen actividades de gestión: solicitudes, requreimientos e incidentes P07-A1. Desconocimiento de escalamiento a proveedores P08-A1. No existe ninguna cultura sobre el cuidado y protección de las credenciales de usuarios	P01-V1. El conocimiento del flujo y la operativa de este proceso lo tiene el Jefe del área de Tecnología de la Información y Comunicaciones únicamente P02-V1. La actividad de monitoreo no posee niveles de atención para resolución de eventos o incidentes tecnológicos internos (empleados, funcionarios de la Cooperativa) o externos (clientes) P02-V2. No tiene proceso de escalamiento para el restablecimiento de servicio con los proveedores, en base a la criticidad, frecuencia e impacto que ayude a erradicar la causa del evento o incidente. P03-V1. Los activos de información que se obtienen principalmente de la base de datos, son primordiales para el negocio. P06-V1. Afectación en tiempo de solución a los usuarios internos/externos P07-V1. No existe un proceso de gestión de proveedores por lo la Cooperativa puede estar expuesta a robo, destrucción, uso inadecuado de información confidencial y crítica para el negocio.	1. actividad se lo tienen de forma emperica 2. Reportes a proveedores vía Skype o mail 3. Informalidad de actividades	Alto	4,3	3,7

Anexo 3. Glosario

BDD: Base de Datos

BMIS: Business Model for Information Security (*Modelo de negocio para la seguridad de la información*).

BSC: Balanced Scorecard (Cuadro de Mando Integral)

CEO: Chief Executive Officer (*Director Ejecutivo*).

COSO: Committee of Sponsoring Organizations of the Treadway Commission):

ISACA: Information Systems Audit and Control Association (*Asociación de Auditoría y Control de Sistemas de Información).*

ISO: International Organization for Standardization (*Organización Internacional de Estándares*).

ITA: IT Assurance Framework (Marco de Aseguramiento de TI).

ITIL: Information Technology Infrastructure Library (*Biblioteca de Infraestructura de Tecnologías de la Información*).

LOEPS: Ley Orgánica de Economía Popular y Solidaria.

MIES: Ministerio de Inclusión Económica y Social.

MPI: Matriz de Probabilidad de Impacto.

RACI: Matriz de la Asignación de Responsabilidades.

SEPS: Superintendencia de Economía Popular y Solidaria.

TIC: Tecnología de la Información y de la Comunicación.

TOGAF: The Open Group Architecture Framework (*Marco de la Arquitectura del Grupo Abierto*).