ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

MAESTRIA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

III PROMOCIÓN

TESIS DE GRADO MAESTRIA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

TEMA: "DISEÑO DE UN MODELO DE EVALUACIÓN DE LA GESTION DE LAS TIC'S PARA LA COAC TEXTIL 14 DE MARZO"

AUTORES: ESPÍN, ROBERTO MIGUEL

GRANDA, ALEX MARCELO

DIRECTOR: ING. HERMOSA, EDGAR MGT.

SANGOLQUÍ, ENERO DEL 2015

CERTIFICACION

Certifico que el presente trabajo fue realizado en su totalidad por el Ing. Alex Marcelo Granda Egas y el Ing. Roberto Miguel Espín Villacrés, como requerimiento parcial para la obtención del título de MAGISTER EN EVALUACION Y AUDITORIA DE SISTEMAS TECNOLÓGICOS.

Sangolquí, Enero del 2015

Ing. Edgar Hermosa Mgt.

TUTOR DE TESIS

UNIVERSIDAD DE LAS FUERZAS ARMADAS

DIRECCION DE POSTGRADO

DECLARACION DE DERECHOS

ALEX MARCELO GRANDA EGAS

ROBERTO MIGUEL ESPIN VILACRES

DECLARAMOS QUE:

El presente proyecto de grado denominado: "DISEÑO DE UN MODELO DE EVALUACIÓN DE LA GESTION DE LAS TICS PARA LA COOPERATIVA DE AHORRO Y CREDITO TEXTIL 14 DE MARZO", es producto de una investigación primaria y secundaria siendo fuentes necesarias de consulta, respetando todos los derechos intelectuales que sirvieron como origen de consulta las citas bibliográficas están acordes a las normas APA vigentes para normas bibliográficas universales, han sido incorporadas en citas textuales, contextuales y bibliográficas. Todo lo que está escrito son ideas propias de los Autores.

En virtud de esta declaración, la veracidad y el contenido de la presente investigación tienen el oportuno alcance científico – metodológico para el proyecto de grado en mención.

Sangolquí, Enero del 2015

ALEX MARCELO GRANDA EGAS ROBERTO MIGUEL ESPIN VILLACRES

AUTORIZACION

Nosotros, Alex Marcelo Granda Egas y Roberto Miguel Espín Villacrés, autorizamos a la Universidad de las Fuerzas Armadas la publicación del presente trabajo de investigación "DISEÑO DE UN MODELO DE EVALUACIÓN DE LA GESTION DE LAS TICS PARA LA COOPERATIVA DE AHORRO Y CREDITO TEXTIL 14 DE MARZO", en la biblioteca física y virtual como repositorio institucional.

Sangolquí, Enero del 2015

ALEX MARCELO GRANDA EGAS ROBERTO MIGUEL ESPIN VILLACRES

DEDICATORIA

A la persona que no conforme con darme la vida, me ha entregado la suya. Mi madre.

Alex Granda Egas

DEDICATORIA

Primeramente a Dios por haberme dado la vida y por permitirme haber llegado a este momento de mi formación profesional.

Con todo mi cariño y amor a mis padres por su apoyo, consejos, comprensión, amor, ayuda y en general porque hicieron todo para que yo pueda lograr mis sueños. Me han dado todo lo que soy como persona, mis valores, principios, perseverancia para conseguir mis objetivos.

A mis hermanos por estar siempre presentes, acompañándome para poder llegar a cumplir mis objetivos.

A tu paciencia y comprensión, por sacrificar tu tiempo para que yo pudiera cumplir con mi trabajo. Porque me inspiraste en ser mejor para ti. Gracias por estar siempre a mi lado Aracely.

A mis familiares y amigos que siempre estuvieron pendientes del desarrollo en la elaboración de este trabajo

Roberto Espín Villacrés

AGRADECIMIENTO

En todo este tiempo de trabajo en investigación recibí una cantidad innumerable de apoyos, consejos, informaciones, estímulos, enseñanzas, compañías, experiencias, discusiones, críticas, datos y vivencias, que me acompañaron en mi vida personal y en mi carrera académica permitiendo la realización y finalización de esta tesis. Creí oportuno poder ocupar un espacio para poder agradecer a aquellos que transitaron conmigo este viaje, con mayor o menor intensidad.

Antes que nadie, quiero recalcar y agradecer eternamente el apoyo espiritual y vivencial constante ofrecido por mi madre, quien es una fuente de estímulo enorme, que se enorgullece con cada paso en mi carrera y que me llena de combustible y ganas por seguir adelante ante cualquier tipo de dificultad que surja. No está demás agradecer su persistente ayuda con distintas cuestiones de la vida cotidiana familiar que me permitió concentrarme enteramente con la confección de esta tesis. Dicen que las más importantes oportunidades que pueden cambiar la vida de la gente surgen de la combinación exacta de estar precisa y simultáneamente en un determinado tiempo, lugar y con las personas indicadas. Ninguna otra situación es más explicativa que ésta, para describir el inicio de mi carrera académica y profesional que en dicha confluencia de fenómenos se destaca por haberme topado con el Ing, Edgar Hermosa. Siempre le agradeceré por su eterna confianza, por darme múltiples oportunidades, por aconsejarme constantemente acerca del próximo paso a seguir, por transformarse en un amigo. No me imagino cuál sería mi realidad profesional si no me hubiera reunido con él. Mi agradecimiento hacia él se extiende nuevamente, por su rol de director de esta tesis.

Probablemente, me haya olvidado de muchas otras personas que se relacionan directamente con aportes u otro tipo de colaboraciones para el desarrollo de esta tesis. Igualmente, les agradezco a ustedes y a todos los recién mencionados por su ayuda en la generación de esta tesis, que si bien es consecuencia de un trabajo individual, contó con el gran apoyo realizado desinteresadamente por parte de mucha gente.

Alex Granda Egas

AGRADECIMIENTO

Primeramente quisiera agradecer a Dios por haberme permitido llegar hasta donde he llegado.

Les doy gracias a mis padres Martha y Francisco por apoyarme en todo momento, por los valores que me han inculcado y sobre todo por ser un ejemplo de vida a seguir. También quisiera agradecer a mis hermanos porque son una parte muy importante en mi vida.

Un especial agradecimiento a Aracely por ser una parte importante en mi vida, por estar siempre a mi lado y sobre todo por su paciencia y amor incondicional.

A la Universidad de las Fuerzas Armadas por haberme brindado la oportunidad de estudiar la maestría.

A mi director de tesis, Ing. Edgar Hermosa por su esfuerzo y dedicación, quien con sus conocimientos, experiencia, paciencia y su motivación ha logrado que pueda culminar mis estudios.

Un agradecimiento a Alex por ser un buen amigo y compañero de tesis, con quien he compartido incontables horas de trabajo.

También me gustaría agradecer a mis compañeros y profesores que durante la maestría, aportaron con su conocimiento y experiencia a mi formación.

En general a todas aquellas personas que directa o indirectamente contribuyeron en la realización de este trabajo que fortalecerá a la COAC Textil 14 de Marzo.

Roberto Espín Villacrés

INDICE

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

El presente trabajo fundamentalmente se lo realizó con la finalidad de ser una ayuda al sector financiero de las Cooperativas de Ahorro y Crédito, ya que por la nueva normativa de la SEPS (Superintendencia de Economía Popular y Solidaria), se les exige una serie de requisitos para su normal funcionamiento. En caso de que las instituciones no cumplan con estas normativas, existen sanciones económicas llegando incluso al cierre definitivo de la institución. Se realizó un análisis de la Normativa de la SEPS que se basa en la Norma de Riesgo Operativo de la SBS (Superintendencia de Bancos y Seguros), seguidamente se realizó una estudio de los marcos de trabajos propuestos para el desarrollo de la tesis como son COBIT 4 y 5, ITIL y Val IT con la finalidad de proponer un modelo que cubra todos los requerimientos de la Norma de Riesgo Operativo y que sea aplicable a instituciones de este sector financiero. Además se realizó un análisis de los principales riesgos que pueden afectar el normal funcionamiento del área de tecnología de una Cooperativa de Ahorro y Crédito, el caso práctico se desarrolló en la Cooperativa de Ahorro y Crédito Textil 14 de Marzo.

Palabras Clave:

- **MODELO DE GESTIÓN**
- **COBIT PARA COOPERATIVAS**
- **VAL-IT PARA COOPERATIVAS**
- **ITIL PARA COOPERATIVAS**

Abstract

This paper mainly it 's purpose is as an aid to the financial sector of the Credit Unions , since the new rules of the SEPS , they are required a number of requirements for normal operation . If institutions do not comply with these regulations, economic sanctions are coming even to the decommissioning of the facility. Normative analysis of SEPS based on Standard Operational Risk SBS (Superintendency of Banking and Insurance) was performed, followed by one study of frameworks proposed for the development work of the thesis are performed as COBIT 4 and 5, ITIL and Val IT in order to propose a model that meets all the requirements of the Standard Operational Risk and applicable to financial institutions in this sector. Further analysis of the principal risks that may affect the normal operation of the technology area of the Cooperative Credit Union Textile March 14 was performed. It should be mentioned that the proposed model is applicable to any cooperative, however at work oriented toward the study institution such as the Cooperative Savings and Credit Textile March 14.

Key Words:

- **MODELO DE GESTIÓN**
- **COBIT PARA COOPERATIVAS**
- **VAL-IT PARA COOPERATIVAS**
- **ITIL PARA COOPERATIVAS**

CAPITULO I

1.1. Introducción

Este trabajo tiene como finalidad desarrollar un modelo de evaluación de la gestión de las Tecnologías de Información y Comunicación (TIC's) para Cooperativas de Ahorro y Crédito. Este modelo facilitará la estructuración de un adecuado nivel de control de riesgo para la gestión de TIC's, que permita entre otros evitar y/o disminuir las fallas en los sistemas, redes, internet y todo el patrimonio informático (hardware, software y datos) de ataques o desastres, antes que éstos ocurran y en el caso de estos ocurrir minimizar su impacto. Es evidente la importancia y urgencia de este tema hoy en día. Se presentaran las normas, estándares y leyes más relevantes relacionadas con el tema, y se discutirán brevemente los diversos aspectos involucrados en la formulación del modelo. El modelo a proponer se fundamentará en los lineamientos entregados en las normas, estándares y mejores prácticas nacionales e internacionales del área (COBIT, VAL-IT, ITIL y La Norma de Riesgo Operativo de la Superintendencia de Bancos y Seguros), lo cual permitirá que el modelo entregue las bases para que las cooperativas puedan realizar un uso seguro de sus TIC's.

1.2. Justificación e Importancia

Actualmente es impensable concebir una empresa que no use las Tecnologías de la Información y Comunicación, para el desarrollo y gestión de sus actividades inherentes, es más las TIC's han dejado de ser una herramienta de soporte y/o un área accesoria para convertirse en un activo estratégico de cualquier organización coadyuvando activamente a su competitividad. Pero es innegable que son muchos los problemas que se presentan al gestionar estas Tecnologías de la Información y Comunicación. Las Cooperativas de Ahorro y Crédito no escapan a esta difícil situación.

¿Cómo lograr que las TIC's sean una inversión con retorno y no solamente un gasto necesario, y mejor aún, conlleven a una ventaja competitiva para la COAC Textil 14 de Marzo?.

Hoy en día existen una diversidad de normas, estándares y conjuntos de buenas prácticas para la gestión de TIC's, tales como , COBIT, VAL-IT, ITIL y La Norma de Riesgo Operativo de la Superintendencia de Bancos y Seguros, que permitirían lograr una ventaja competitiva para la COAC Textil 14 de Marzo.

Más los problemas en la gestión de TIC's, son muchos y de variada naturaleza y se presentan indistintas instancias del ciclo de vida de la implementación de las TIC's en una organización. Para cada uno de los problemas hay más de un estándar aplicable para gestionar dichas problemáticas, el modelo para la COAC Textil 14 de Marzo es una combinación de ellos, que se adapta a sus necesidades, políticas empresariales y particularmente a su misión institucional.

El propósito de definir un modelo para la Unidad de Auditoría Interna de la COAC Textil 14 de Marzo es contar con una guía de evaluación y monitoreo de las TIC's, que permita determinar si los controles establecidos son suficientes y efectivos para proteger a la organización, contra los riesgos que podrían afectarla en los sistemas de información y procesos de negocio. Esto es, evaluar la confiabilidad, disponibilidad y continuidad de los controles utilizados para prevenir o detectar y corregir las causas de los riesgos y minimizar el impacto que estos tendrían en caso de llegar a materializarse.

1.3. Planteamiento del Problema

La COAC (Cooperativa de Ahorro y Crédito) Textil 14 de Marzo en su estructura orgánica cuenta con la Unidad de Auditoría Interna, la misma que no dispone de un modelo para evaluar la gestión de las Tecnologías de Información y Comunicación que le permita medir la eficacia, eficiencia y la productividad de su aplicación, así como determinar si los controles establecidos, ofrecen la protección apropiada para reducir los riesgos a niveles aceptables para la organización, ya que se han presentado incidentes como: caída de servidores de cajeros, no hay una adecuada actualización de la información de los clientes, cuando existen cortes de energía eléctrica no se cuenta con los respaldos que permitan la continuidad de los servicios, caídas de enlaces de comunicaciones con las agencias, etc.

Es bueno resaltar, que la aplicación en la COAC Textil 14 de Marzo de controles internos relacionados con las TIC's en sus operaciones, conducirá a conocer la

situación real de la misma, es por eso, la importancia de tener un modelo de evaluación de la gestión de las TIC's.

El modelo de control interno de las TIC's estará alineado con directrices internacionales y nacionales como, COBIT, VAL-IT, ITIL y La Norma de Riesgo Operativo de la Superintendencia de Bancos y Seguros.

1.4. Formulación del Problema a Resolver

- ¿La COAC Textil 14 de Marzo cuenta con algún modelo o norma técnica para la evaluación periódica de la gestión de las TIC's?
- ¿Se puede confiar en el Sistema de Control Interno de TIC's de la COAC Textil 14 de Marzo?
- ¿Cómo identificar, documentar, evaluar y priorizar los riesgos en la gestión de las TIC's?
- ¿Cómo monitorear el cumplimiento de los controles establecidos y diseñar las acciones de mejoramiento requeridas?

1.5. Objetivo General

Diseñar un modelo de evaluación de la gestión de TIC's para la COAC Textil 14 de Marzo en base a los marcos de referencias y estándares, COBIT, VAL-IT, ITIL y La Norma de Riesgo Operativo de la Superintendencia de Bancos y Seguros.

1.6. Objetivos Específicos

- Revisar el Sistema de Control Interno de TIC's de la COAC Textil 14 de Marzo.
- Identificar los riesgos y el nivel de control sobre los mismos para los procesos críticos de informática en la COAC Textil 14 de Marzo.
- Analizar las normas, estándares y mejores prácticas que permitan elaborar un modelo para identificar, documentar, evaluar y priorizar los riesgos a las operaciones de la tecnología de información aplicables a las cooperativas de ahorro y crédito.
- Entregar a la Unidad de Auditoría Interna de la COAC Textil 14 de Marzo un modelo de evaluación de la gestión de TIC's que permita documentar, evaluar la efectividad y monitorear los controles internos de las TIC's.

CAPITULO II

2.1. Marco Teórico

2.1.1. Sistema de Control Interno

El término "Sistema de control interno" significa todas las políticas y procedimientos (controles internos) adaptados por la administración de una entidad para ayudar a lograr el objetivo de la administración de asegurar, tanto como sea factible, la conducción ordenada y eficiente de su negocio, incluyendo adhesión a las políticas de administración, la salvaguarda de activos, la prevención y detección defraude y error, la precisión e integralidad de los registros contables, y la oportuna preparación de información financiera confiable.

Control Interno son las políticas, principios y procedimientos adoptados por la administración para lograr las metas y objetivos planificados y con el fin de salvaguardar los recursos y bienes económicos, financieros, tecnológicos a través de su uso eficiente y aplicando la normativa vigente, así como las políticas corporativas establecidas (IAPC, 2002).

2.1.2. Normas, Estándares y Mejores Prácticas

2.1.2.1. COBIT

Acrónimo de "Control Objectives for Information and Related Technology" (Objetivos de Control para la Información y Tecnologías Relacionadas), es un estándar desarrollado por la Information Systems Audit and Control Foundation (ISACA), la cual fue fundada en 1969 en EE.UU., y que se preocupa de temas como gobernabilidad, control, aseguramiento y auditorias para TIC. Actualmente tiene más de 60.000 miembros en alrededor de 100 países. Esta organización realiza eventos y conferencias, y desarrolla estándares en TI de gobierno, aseguramiento y seguridad, siendo COBIT el más importante. En los últimos años ha cobrado fuerza debido a que fue desarrollado en específico para el ámbito de las TIC's (ISACA, 2012).

2.1.2.2. ITIL

Es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI) de alta calidad. ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir de guía para que abarque toda infraestructura, desarrollo y operaciones de TI.

Uno de los principales beneficios propugnado por los defensores de ITIL dentro de la comunidad de TI es que proporciona un vocabulario común, consistente en un glosario de términos precisamente definidos y ampliamente aceptados.

ITIL fue desarrollado al reconocer que las organizaciones dependen cada vez más de las TI para alcanzar sus objetivos corporativos. Esta dependencia en aumento ha dado como resultado una necesidad creciente de servicios TI de calidad que se correspondan con los objetivos del negocio, y que satisfaga los requisitos y las expectativas del cliente. A través de los años, el énfasis pasó de estar sobre el desarrollo de las aplicaciones TI a la gestión de servicios TI.

La aplicación TI (a veces nombrada como un sistema de información) sólo contribuye a realizar los objetivos corporativos si el sistema está a disposición de los usuarios y, en caso de fallos o modificaciones necesarias, es soportado por mantenimiento y operaciones.

2.1.2.3. VAL-IT

Val-IT es un conjunto de documentos que proveen un marco de trabajo para el gobierno de las inversiones en TI, creado por el ITGI (Instituto de Gobierno de las TI). Es una declaración formal de los principios y procesos para la administración del portafolio de TI.

El objetivo del Val-IT es ayudar a asegurar que las organizaciones consigan valor de las inversiones en TI, con un costo adecuado y un aceptable nivel de riesgo. Esta propuesta del ITGI es proporcionar guías, procesos y prácticas de soporte para ayudar a la dirección a comprender y llevar a cabo las inversiones en TI.

Val-IT establece que los proyectos de TI se manejen como una cartera de inversiones, con un valor comercial y sean gestionados durante su ciclo de vida

económico completo. Este marco extiende y complementa a otra buena práctica como lo es COBIT (Arrianto Mukti, s.f.).

2.1.2.4. Norma de Riesgo Operativo

La Norma de Riesgo Operativo para la gestión y administración del riesgo operacional es un conjunto de mejores prácticas para la gestión emitida por la Superintendencia de Bancos y Seguros (SBS) ha organizado un conjunto de mejores prácticas para mitigar o controlar los riesgos que forman la base del riesgo operacional.

La desregulación y globalización de los servicios financieros, junto con la creciente sofisticación de la tecnología financiera están haciendo que las actividades de las cooperativas, y en consecuencia, sus perfiles de riesgo, cada vez más complejos. Adicionalmente a los riesgos de crédito, de tasa de interés y de mercado, el riesgo operacional puede ser sustantivo y las tendencias de pérdidas parecen indicar que se está incrementando. Como resultado, una sólida gestión del riesgo operativo es cada vez más importante para cooperativas, con riesgos operativos emergiendo en un número de áreas críticas, tales como las siguientes:

- Mayor uso de tecnología automatizada (por ejemplo: riesgos derivados de la automatización de procesos manuales, errores de procesamiento y riesgos de fallas en los sistemas).
- Proliferación de productos nuevos y altamente complejos.
- Crecimiento de transacciones electrónicas y aplicaciones de negocios relacionadas.
- Adquisiciones de gran escala, fusiones y consolidaciones.
- Aparición de instituciones que actúan como proveedores de servicios a gran escala.
- Desarrollo y uso de técnicas de mitigación de riesgos (por ejemplo: garantías, seguros, derivados de crédito, etc.).
- Integración global de servicios financieros (por ejemplo: riesgos de transacciones de pago procesadas en múltiples aplicaciones, crecientes transacciones comerciales, etc.).

Este compendio de mejores prácticas preparado por el equipo de riesgos de la SBS representa un conjunto importante de cambios que permitirán a las empresas mejorar sus controles sobre el riesgo operacional, pero también representan un importante conjunto de inversiones en esfuerzo y presupuesto para las instituciones (SBS, 2012).

De acuerdo a la resolución del organismo de control (Superintendencia de Economía Popular y Solidaria) del sector de las Cooperativas de Ahorro y Crédito, se tomará en consideración el artículo de la Norma de Riesgo Operativo de la Superintendencia de Bancos y Seguros donde se especifican los lineamientos de la gestión de las TIC's para el desarrollo de esta tesis.

2.1.3. Análisis de Gestión de Riesgos

Previo a un Análisis y Gestión de Riesgos dentro de una Organización, es importante conocer el concepto de seguridad, el mismo que se define como la capacidad de las redes o de los sistemas para resistir, con un determinado nivel de confianza, los accidentes o acciones licitas o mal intencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

Por tal razón, la misión de la Organización es proteger la información, lo cual hace indispensable considerar las dimensiones de seguridad:

- **Disponibilidad:** Permite que el personal autorizado tenga acceso a la información y a sus activos asociados cuando sea necesario.

La falta de disponibilidad podría interrumpir el servicio, afectando directamente a la productividad de la Organización.

- **Integridad:** Garantiza exactitud, completitud y corrección de la información.

Si la información aparece manipulada, corrupta o incompleta, las funciones de la Organización quedarían afectadas y por ende su desempeño.

- **Confidencialidad:** Certeza de que la información llegue únicamente a las personas autorizadas.

La falta de confidencialidad podría dar lugar a la salida y entrada de información a personas no autorizadas, así como acceso no autorizado.

- **Autenticidad:** Que la persona que se hace responsable de la información o prestación de servicio sea confiable y no exista duda sobre él, para evitar que se generen suplantación de identidad y engaños que buscan realizar un fraude.

Las características antes mencionadas son las que pretenden conseguir toda Organización, para esto es necesario poner medios y esfuerzos para conseguirlas, aplicando un Análisis y Gestión de Riesgos.

Para entender esta metodología partiremos con la definición de:

- **Riesgo:** Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. Dicho concepto nos indica lo que le podría suceder a nuestros activos si no son protegidos adecuadamente.

Es necesario conocer las características importantes de cada activo, así como el peligro en las que se encuentran, para lo cual será necesario analizar el sistema.

- **Análisis de Riesgo:** Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

El análisis de riesgo proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas; y es la piedra angular para controlar todas las actividades con fundamento.

El análisis de riesgos permite determinar cómo es, cuanto vale y como de protegidos se encuentran los activos.

Una vez identificado y analizado los riesgos es necesario tomar decisiones con el fin de contrarrestar dichos riesgos.

- **Gestión de Riesgos:** Selección e implementación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

La Gestión de Riesgos es la estructuración de las acciones de seguridad para satisfacer las necesidades detectadas por el análisis.

En coordinación de los objetivos, estrategia y política de la Organización, las actividades de Gestión de Riesgos permiten elaborar un plan de seguridad que implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la dirección.

En toda Organización siempre existirá cierto nivel de riesgo y no podrá ser reducido a cero, debido a que la seguridad absoluta no existe, por tanto siempre hay que aceptar un cierto nivel de riesgo, el mismo que debe ser conocido y sometido a su más bajo nivel.

La Organización al aceptar cierto nivel de riesgo es consciente y sabe de las condiciones en las cuales trabaja, dando la confianza al sistema de ajustarse con las actividades diarias, con el fin de tener menos incertidumbre.

Para elaborar el Análisis de Gestión de Riesgos en una Organización, se debe establecer una metodología, la misma que permita gestionar Seguridad de la Información. El modelo MAGERIT es la metodología mejor recomendada para el análisis y gestión de riesgos, el cual permite realizar una evaluación profunda de la seguridad de los sistemas de información en una Organización.

2.1.3.1. Objetivos del Análisis de Riesgos

1. Identificar los activos relevantes que posee la organización
2. Identificar las amenazas a las que están expuestos dichos activos.
3. Determinar si existen salvaguardas para los activos.
4. Estimar el impacto si una amenaza llegara a materializarse.

El análisis de riesgos permite como es, cuanto vale y como de protegidos se encuentran los activos evaluando de manera metódica para llegar a conclusiones con fundamento.

2.1.3.2. Elementos del Análisis de Riesgo

1. Activos, no son más que los elementos del sistema de información (o las que se encuentran relacionadas con este) que generan valor a la organización.

2. Amenazas, son eventos que les puede pasar a los activos provocando daños a la organización.

3. Salvaguardas, son mecanismos de defensa utilizados para que aquellas amenazas no causen tanto daño.

Con los elementos anteriormente mencionados se puede identificar:

1. El impacto, lo que podría pasar.
2. El riesgo, lo que probablemente pase.

La siguiente grafica recoge lo mencionado anteriormente:

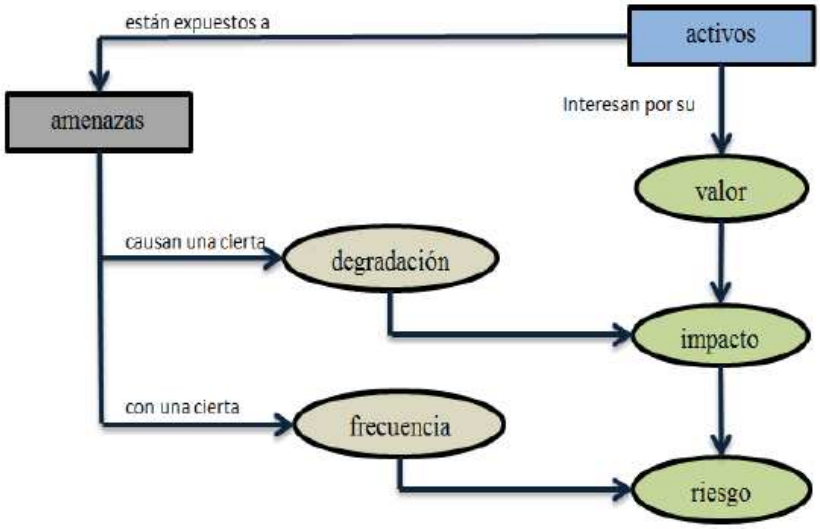


Figura2.1. Análisis de Riesgos

Para el desarrollo de esta etapa, la recolección de información será desarrollada mediante encuestas y entrevistas a los usuarios responsables de los sistemas de información de la COAC Textil 14 de Marzo, también se consideran las inspecciones físicas realizadas a la organización.

Esta actividad tiene una importancia crucial por dos motivos: la información a recoger condiciona el conocimiento del equipo del proyecto; y la recogida en si es una operación delicada que exige una confianza mutua profunda (la transmisión de información es siempre delicada y más si concierne a la seguridad).

2.1.3.3. Identificación de Activos

Se denomina activos, los recursos del sistema de información o relacionados con este, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su organización.

El activo esencial es la información que maneja el sistema; es decir los datos y alrededor de estos datos se pueden identificar otros activos relevantes que integran los Sistemas de Información como son:

- Los servicios que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) que permiten hospedar datos, aplicaciones, y servicios.
- Las redes de comunicación que permiten intercambiar datos.
- los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.

La identificación de activos es importante ya que permite materializar con precisión el alcance del proyecto, permite valorar los activos con exactitud e identificando y valorando las amenazas a las que están expuestos dichos activos.

[S] Servicios

Función que satisface una necesidad de los usuarios (del servicio). Para la prestación de un servicio se requiere una serie de medios.

Los servicios aparecen como activos de un análisis de riesgos bien como servicios finales (prestados por la organización a terceros), bien como servicios instrumentales (donde tanto los usuarios como los medios son propios), bien como servicios contratados (a otra organización que les proporciona con sus propios medios).

[SW] Aplicaciones (software)

Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) esto se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

[HW] Equipos Informáticos (hardware)

Dícese de bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

[COM] Redes de Comunicaciones

Incluyendo tanto instalaciones dedicadas como servicio de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

[SI] Soportes de Información

Se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

[AUX] Equipamiento Auxiliar

Se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con los datos.

[SS] Servicios Subcontratados

Se consideran servicios subcontratados a los convenios con otras instituciones para satisfacer la demanda ciudadana.

[L] Instalaciones

Aquí entran los lugares donde se hospedan los sistemas de información y comunicaciones.

[P] Personal

Aquí aparecen las personas relacionadas con los sistemas de información.

2.1.3.4. Identificación de Amenazas

Luego de la identificación de los activos se deben identificar las amenazas que pueden afectar a cada activo, por lo que una amenaza puede desencadenar muchas más.

Las amenazas son eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o perdidas inmateriales en sus activos.

Consideraremos las amenazas obtenidas de encuestas realizadas a los responsables de los sistemas de información de la institución.

La frecuencia y degradación de las amenazas se realizo de forma manual para una mayor comprensión.

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera se caracteriza con una fracción del valor del activo.

Tabla No. 2.1 Escala de Degradación

50%	Medio
100%	Muy alto

La frecuencia es cada cuanto se materializa la amenaza, se modela como una tasa anual de ocurrencia, siendo valores típicos.

Tabla No. 2.2 Escala de Frecuencia

12	Mensualmente
2	Dos veces al año
1/12	Cada varios años

2.1.3.5. Identificación de Salvaguardas

Una vez identificado las amenazas, se identificara los mecanismos de salvaguarda implantados en aquellos activos, describiendo las dimensiones de seguridad que estos ofrecen (Disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad).

Salvaguarda son procedimiento, dispositivo, físico o lógico, que reduce el riesgo.

2.1.3.6. Identificación de Vulnerabilidades

Una vez identificado las amenazas y las salvaguardas existentes de los activos, la siguiente actividad es la identificación de vulnerabilidades.

Vulnerabilidad es la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.

2.1.3.7. Identificación de Impactos

El objetivo es esta actividad es, conocer el alcance del daño producido en el dominio (Y por tanto sobre todos los activos que se encuentran en dicho dominio), como resultado de la materialización de las amenazas sobre los activos.

La identificación de impacto de impacto o valoración de dominios se desarrollara con repercusiones a las dimensiones de valoración que son: (D) Disponibilidad, (I) Integridad, © Confidencialidad, (A) Autenticidad, y (T) Trazabilidad de la información.

Las dimensiones de valoración son características o atributos que hacen valioso un activo.

Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que se recibe en una cierta dimensión es la medida del perjuicio para la organización si los activos se ven dañados en dicha dimensión.

Los criterios de valoración que hemos implantado son los siguientes:

Tabla No. 2.3 Escala de Criterios de Valoración

4-7	Medio	Daño importante a la organización
0-1	Despreciable	Irrelevante a efectos prácticos

2.1.3.8. Identificación del Riesgo

En esta actividad, luego del análisis de los activos en lo que se refiere a las amenazas, salvaguardas existentes, vulnerabilidades e identificación de impactos, se identificará los activos que poseen niveles de riesgo considerables.

En el siguiente cuadro se puede observar los activos y su nivel de riesgo y su valoración.

Tabla No. 2.4 Nivel de Riesgo

	Bajo [1 -]	Medio 2.9]	Alto [3 -]	Muy Alto 4.9]	Crítico [5 - 5.9]

2.1.3.9. Identificación de Riesgo Críticos

En toda organización los activos están expuestos a riesgos, pero lo importante es conocer cuáles de los activos poseen un mayor nivel riesgo con el fin de implementar salvaguardas para evitar que las amenazas se materialicen

Una vez evaluado los activos y conocido el riesgo a los que están expuestos los mismos, hemos seleccionado los activos que poseen un nivel de alto riesgo.

2.1.3.10. Mitigación del Riesgo Crítico

Es una actividad de la Gestión de Riesgos, que indica las decisiones que se van a efectuar en la mejora de la seguridad, en un determinado tiempo para un caso especifico de la gestión.

2.1.4. Metodología MAGERIT

El CSAE (Consejo Superior de Administración Electrónica) de España, ha elaborado y promueve MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas) como respuesta a la percepción de que la administración (y en general toda la sociedad) depende de

forma creciente de las tecnologías de la información para la consecución de sus objetivos de servicio.

La razón de ser de MAGERIT está pues directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero que también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que garanticen la autenticación, confidencialidad, integridad y disponibilidad de los sistemas de información y generen confianza cuando se utilicen tales medios (Lopez, Amutiol, & Candau, 2006).

Una organización no alcanzará sus objetivos, metas y misión si no tiene a su alcance los elementos informáticos básicos e indispensables que le ayuden y soporten sus decisiones.

2.1.4.1. Objetivos de MAGERIT

MAGERIT persigue los siguientes objetivos:

Directos:

- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de detenerlos a tiempo.
- Ofrecen un método sistemático para realizar tales riesgos.
- Ayudar a distribuir y planificar las medidas oportunas para mantener los riesgos bajo control.

Indirectos:

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

2.1.4.2. Elementos de MAGERIT

A continuación definimos brevemente los elementos considerados significativos por MAGERIT para el estudio de los sistemas de información.

- **Activos:** Recursos del sistemas de información o relacionados con éste, necesarios para que la organización funcione correctamente y alance los objetivos propuestos por la Dirección.

- **Amenazas:** Eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- **Vulnerabilidad de un activo:** Potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.
- **Impacto de un activo:** Consecuencia sobre éste de la materialización de un activo.
- **Riesgo:** Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la Organización.
- **Servicio de salvaguarda:** Acción que reduce el riesgo.
- **Mecanismos de salvaguarda:** Procedimiento, dispositivo, físico o lógico, que reduce el riesgo.

La siguiente figura muestra los elementos y sus interrelaciones:

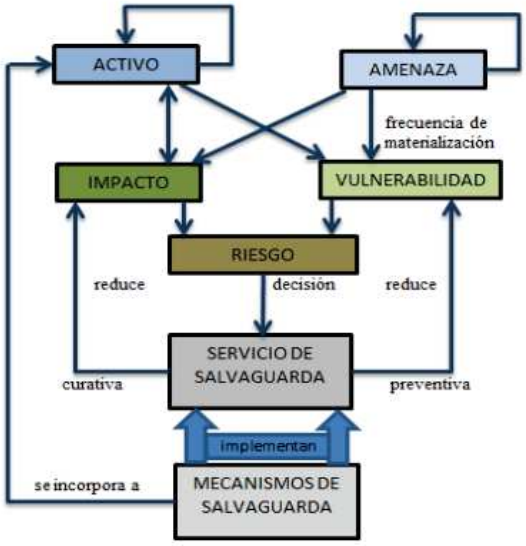


Figura No. 2.2 Elementos de MAGERIT

Fuente: (Lopez, Amutiol, & Candau, 2006)

2.2. Marco Conceptual

Las cooperativas de ahorro y crédito se encuentran expuestas a diferentes niveles de exposición de riesgo operativo. El riesgo operativo se basa en la posibilidad de que se ocasionen pérdidas financieras en las cooperativas por eventos o hechos derivados de fallas o insuficiencias en sus procesos estratégicos, administrativos o

del negocio, las personas internas o relacionadas, la tecnología de información usada y por eventos externos.

La evolución del cooperativismo obliga a contar con un plan integral para la gestión de TI que incluya la vigilancia de los actores involucrados para identificar, evaluar, seguir, controlar y mitigar todos los riesgos significativos. El proceso para la gestión de TI deberá ser revisado periódicamente en función de los cambios que se produzcan en el perfil de riesgo de la entidad y en el mercado.

Es por esto que la Superintendencia de Economía Popular y Solidaria (SEPS) resolvió que las cooperativas de ahorro y crédito deben implementar la Norma de Riesgo Operativo de la Superintendencia de Bancos y Seguros. Pero debido a la falta de conocimiento a nivel directivo, se ha notado una subestimación de las exigencias de la Norma de Riesgo Operativo, es decir no se ha dimensionado con claridad en las Cooperativas cual es el esfuerzo y recursos económicos que deberán invertir para poder implementar satisfactoriamente las disposiciones de la SEPS.

La Norma de Riesgo Operativo presenta diferentes aspectos resumidos en la siguiente tabla:

Tabla No. 2.5 Síntesis de la Norma de Riesgo Operativo

Reportes sobre el Riesgo Operativo	Detalle de los eventos de riesgo operativo, el grado de cumplimiento de los procesos, políticas y procedimientos, indicadores de gestión para evaluar la eficiencia y eficacia.

Continua

Procesos	Procesos definidos, clasificados, aprobados, inventariados, difundidos, aplicados, controlados, medidos, evaluados, asignados a un responsable, mejorados continuamente, con la respectiva identificación de cuales son críticos y considerando una adecuada segregación de funciones.
Eventos Externos	Oficialmente y estructuradamente se considera la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos al control, tales como: - fallas en los servicios públicos, - ocurrencia de desastres naturales, - atentados y - otros actos delictivos.

Continua ➡

Continuidad del Negocio	Planes de contingencia y de continuidad, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción severa del negocio. Proceso de administración de la continuidad de los negocios.

El presente trabajo brinda un modelo en donde se encuentran los lineamientos para realizar una buena gestión de TI basado en la Norma de Riesgo Operativo de acuerdo a las exigencias del organismo de control (SEPS). El modelo además de implementar la Norma de Riesgo Operativo, se apoya en buenas prácticas y estándares internacionales como son COBIT 4.1 y 5.0, ITIL y Val II para de esta manera, complementar o brindar una visión clara de los requerimientos de la cooperativa como por ejemplo: que la inversión que se realiza en tecnología brinde sus réditos a la institución.

Este modelo representa un conjunto importante de cambios que permitirán a las cooperativas mejorar en su gestión de TI, pero también representan un importante conjunto de inversiones en esfuerzo y presupuesto, los cuales deberán ser programados de acuerdo a las exigencias de la SEPS.

Dentro del tema analizado se han planteado varios conceptos que son necesarios aclarar para tener una mejor comprensión del tema a desarrollarse como son:

Diseñar: Es seleccionar entre todas las posibilidades, cuál es la que a nuestro entender se adapta mejor a los requisitos y restricciones, hasta quedarnos con una única solución (Mordecki, 2004).

Modelo: Es un bosquejo que representa un conjunto real con cierto grado de precisión y en la forma más completa posible, pero sin pretender aportar una réplica de lo que existe en la realidad. Los modelos son muy útiles para describir, explicar o comprender mejor la realidad, cuando es imposible trabajar directamente en la realidad en sí.

Evaluar: "Proceso sistémico de recogida y valoración de información útil para una eventual toma de decisiones". (Aguilar, María José y Ander-Egg, Ezequiel, 1994, pag. 12).

TIC's: Tecnologías de la Información y Comunicaciones se conciben como el universo de dos conjuntos, representados por las tradicionales Tecnologías de la Comunicación (TC) - constituidas principalmente por la radio, la televisión y la telefonía convencional - y por las Tecnologías de la Información (TI) caracterizadas por la digitalización de las tecnologías de registros de contenidos (informática, de las comunicaciones, telemática y de las interfaces) (PNUD, 2002).

Norma: Es un documento, establecido por consenso y aprobado por un organismo reconocido (nacional o internacional), que proporciona para un uso común y repetido, una serie de reglas, directrices o características para las actividades de calidad o sus resultados, con el fin de conseguir un grado óptimo de orden en el contexto de la calidad.

Estándares una especificación técnica o un conjunto de criterios que han sido aprobados por una organización reconocida de estándares o comité y que sirve como punto de referencia para comparación.

Mejores Prácticas: Las podemos definir como una serie de metodologías, sistemas, herramientas, y técnicas aplicadas y probadas con resultados sobresalientes en empresas que han sido reconocidas como de clase mundial. Pero también es cierto, que este concepto no debe de ser limitativo a lo que este tipo de empresas han implementado, sino que también el concepto de debe de incluir aquellas prácticas

que las empresas pequeñas, medianas, grandes o locales han desarrollado e implementado para obtener mejores resultados, o aquellas que se han tomado, adaptado y transformado para cubrir adecuadamente sus necesidades.

Auditar: Para este proyecto de tesis consiste en estudiar los mecanismos de control que están implementados en una empresa u organización determinando si los mismos son adecuados y cumplo en objetivos y estrategias.

Gestión de riesgos: Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

Amenaza: Es cualquier cosa que puede suceder y que, cuando ocurre, tiene consecuencias negativas sobre el valor de los activos.

Impacto: se denomina impacto a la medida del daño sobre el activo derivad de la materialización de una amenaza.

Riesgo: estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

Riesgo Residual: Riesgo remanente que existe después de que se haya tomado medidas de seguridad.

Evitar: Eliminar la causa. Cambiar el plan del proyecto, modificar la tarea.

Mitigar: Reducir la probabilidad o el impacto.

CAPITULO III

3. Formulación del Modelo

3.1 Introducción

La creciente disponibilidad de información electrónica y procesos soportados por recursos informáticos y de comunicación que son capaces de satisfacer las circunstancias tanto funcionales como económicas, de oportunidad y efectividad de las entidades financieras, hacen que el auditor se vea en la necesidad de poseer el conocimiento suficiente de los sistemas de información por computadora para planear, dirigir, supervisar y revisar el trabajo a desarrollar.

La naturaleza especializada de la auditoría de Gestión a las Tecnologías de la Información y Comunicaciones (TIC's), requiere de habilidades y conocimientos técnicos informáticos, para desarrollar este tipo de auditorías, además es necesario para el desarrollo de la auditoria, la implementación de normativa legal y técnica en el Área de Tecnología de Información y Comunicaciones de la administración pública y promulgación de normas generales para la auditoría a los sistemas de información.

Para realizar auditoría de Gestión a las Tecnologías de Información y Comunicaciones requiere realizar una adecuada planeación de la auditoría, se debe tener un conocimiento general razonable que permita determinar el alcance, tamaño y características de cada área de Tecnología de la Información y Comunicación dentro de la organización que se auditará, sus sistemas, procesos sistematizados, normativa técnica utilizada por la entidad, adopción e implementación de estándares internacionales relacionados con seguridad de la información, control interno y servicios tecnológicos, organización y equipo físico y lógico.

3.2. Definición de Auditoría de Gestión a las TIC's

La Auditoría de Gestión a las Tecnologías de Información y Comunicaciones, consiste en el examen de carácter objetivo(independiente), crítico (evidencia), sistemático (normas) y selectivo (muestral) de las políticas, normas, funciones, actividades, procesos e informes de una entidad, con el fin de emitir una opinión profesional (imparcial) con respecto a:eficiencia en el uso de los recursos

informáticos, validez y oportunidad de la información, efectividad de los controles establecidos y la optimización de los recursos tecnológicos.

Este enfoque es totalmente compatible con las prácticas y controles contenidos en los estándares o normativa COBIT, ITIL y VAL-TI que se relacionan con La Norma de Riesgo Operativo de la Superintendencia de Bancos y Seguros, que hacen referencia a las pistas de auditoría en los sistemas informáticos, controles de acceso a los sistemas, bases de datos, Áreas de Tecnología de la Información y Comunicaciones (TIC´s), área de servidores, codificación de la información, prevención de virus, fraude, detección y mitigación de intrusos, entre otros; estos estándares nos proporcionan un criterio legal aplicable si no han sido adoptados por la entidad, pero sí procedimientos de auditoría para examinar la Gestión de Tecnológica en las diferentes organizaciones del sector financiero.

3.3. Estándares Internacionales que Intervienen en el Proceso de una Auditoría de Gestión a las Tecnologías de Información y Comunicaciones.

El auditor de las Tecnologías de Información y Comunicaciones, deberá de tener conocimientos de los diferentes estándares que ayudan al control, operación y administración de los recursos tecnológicos, control de inversiones en tecnología de información y comunicaciones a nivel físico y lógico y procesos documentados de tecnología de información y comunicaciones. Dichos estándares inciden en el proceso de la auditoria, ya que las entidades financieras los implementan según sus necesidades de resguardo, uso y protección de la información, que es un activo importante dentro de la organización para asegurarse que la información se encuentre disponible, oportuna y utilizada por los funcionarios autorizados.

Para la realización de una auditoría de TICS, existen Normas relacionadas a la Auditoría de Sistemas las cuales son emitidas por el Consejo Normativo de la Asociación de Auditoría y Control de Sistemas de Información (Information Systems Audit and Control Association – ISACA).

3.3.1. Normas, Estándares y Mejores Prácticas

3.3.1.1. COBIT

COBIT – Objetivos de Control para la Información y Tecnologías Afines (Control Objetives for Information and Related Technology).

COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los Interesados (Stakeholders). COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares.

COBIT, enfatiza el cumplimiento normativo, ayuda a las organizaciones a incrementar el valor de TI, apoya el alineamiento con el negocio y simplifica la implantación de COBIT.

Cuando importantes actividades son planeadas para iniciativas de Gobierno de TI, o cuando se prevé la revisión de la estructura de control de la empresa, es recomendable empezar con la más reciente versión de COBIT.

COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de la misma.

- Beneficios de implementar COBIT como un marco de referencia de Gobierno de TI:
  - Mejor alineación, con base en su enfoque de negocios
  - Una visión, entendible para la gerencia, de lo que hace TI
  - Propiedad y responsabilidades claras, con base en su orientación a procesos
  - Aceptación general de terceros y reguladores
  - Cumplimiento de los requerimientos para el ambiente de control de TI.

Misión de COBIT

Investigar, desarrollar, publicar y promover un conjunto de objetivos de control en TI con autoridad, actualizados, de carácter internacional, y aceptados generalmente para el uso cotidiano de gerentes de empresas u organizaciones y auditores.

Enfocándose en los procesos.

En la Figura No. 3.1 se ilustra el Marco de Trabajo General de COBIT por un modelo que divide TI en 34 procesos alineados con las áreas de responsabilidad de planificación, desarrollo, operación y monitoreo, proveyendo una visión de principio a fin (end-to-end) de TI ((ISACA), Information Technology Governance Institute).

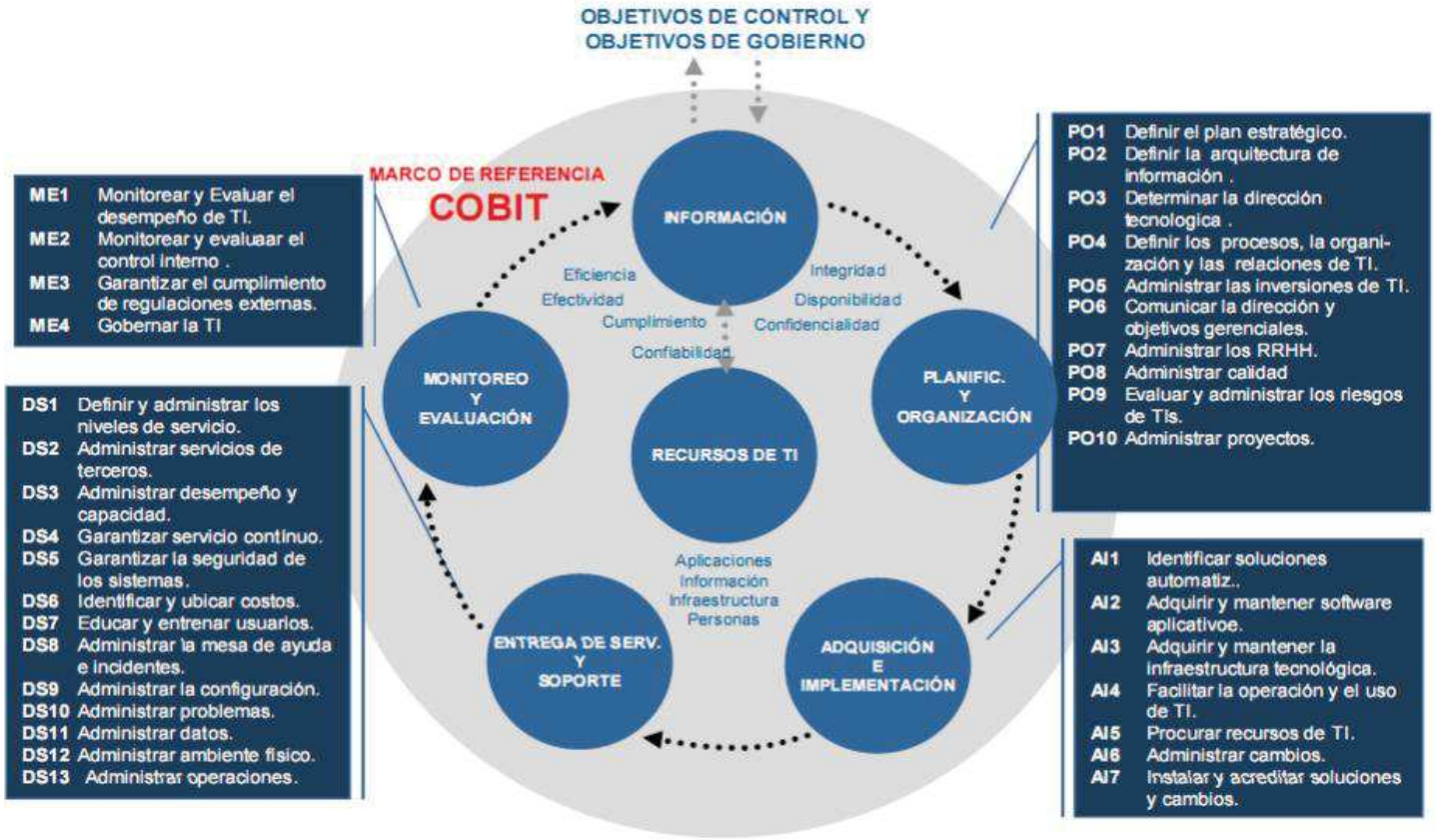


Figura No. 3.1 Marco de Trabajo General de COBIT

Fuente: COBIT (ISACA, 2012)

COBIT define las actividades de TI en un modelo de procesos genéricos con cuatro dominios:

PLANEAR Y ORGANIZAR (PO)

Este dominio cubre estrategias y tácticas, y se preocupa en identificar la manera en que TI puede contribuir mejor a alcanzar los objetivos de negocios.

ADQUIRIR E IMPLEMENTAR (AI)

Para realizar la estrategia de TI, se necesita identificar soluciones de TI así como también implementarlas e integrarlas en el proceso de negocio.

ENTREGAR Y SOPORTAR (DS)

Este dominio trata de la entrega real de los servicios requeridos, lo cual incluye entrega, gestión de seguridad y continuidad, soporte de servicio, y gestión de datos y suministros operativos.

MONITOREAR Y EVALUAR (ME)

Este dominio trata de la gestión de funcionamiento, monitoreo de control interno, conformidad regulatoria y gobierno del aprovisionamiento (ISACA, 2012).

3.3.1.2. ITIL

Conjunto de lineamientos sobre mejores prácticas para la administración de servicios de tecnología de información. ITIL es propiedad de la OGC (Office of Government Commerce) y consiste de una serie de publicaciones que proporcionan lineamientos sobre el aprovisionamiento de calidad en los servicios de TI y sobre los procesos e instalaciones necesarios para soportarlos. Los puntos claves de ITIL se muestran en la Figura No. 3.2 y se describen a continuación:

- **Service strategy (estrategia del servicio)**

Tiene como objetivo proporcionar a las organizaciones las habilidades para diseñar, desarrollar e implementar la Gestión de Servicios como un acto estratégico, así como para pensar y actuar de una manera estratégica. Asimismo, formula las

directrices y guías a seguir en la gestión dentro del modelo de ciclo de vida del servicio.

Establece los siguientes procesos: estrategia del servicio, gestión del portafolio de servicios, gestión de la demanda y gestión financiera. Por otro lado, establece los siguientes roles: Director de Contratación de Servicios, Director de la Gestión de los Servicios, Gerente de Contratos, Gerente de Productos y Representante de Negocio.

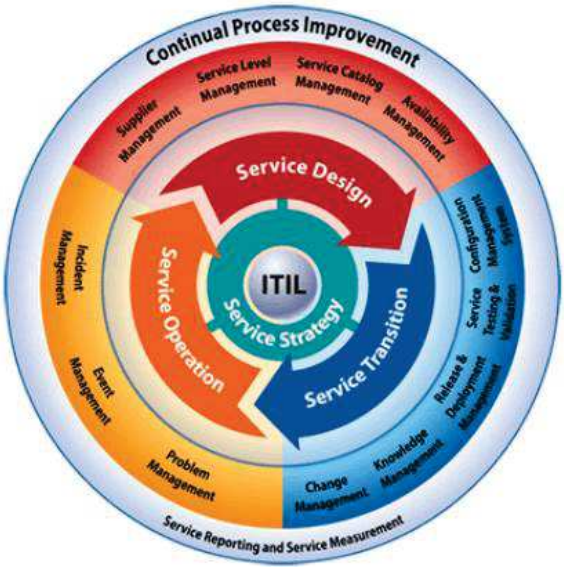


Figura No. 3.2 Puntos Claves de ITIL

Fuente: ITIL (osiatis)

- **Service design (diseño del servicio)**

Tiene como objetivo diseñar un servicio nuevo o modificado para su introducción en el entorno real. Asimismo, se preocupa en entregar servicios redituables y de calidad, así como asegurar el cumplimiento de los requerimientos del negocio.

Establece los siguientes procesos: gestión de niveles de servicio, gestión del catálogo de servicios, gestión de la disponibilidad, gestión de la seguridad de información, gestión de proveedores, gestión de la capacidad y gestión de la continuidad de los servicios de TI.

Entrega los siguientes roles: Gerente de Diseños del Servicio, Planificador de TI, Diseñador/Arquitecto TI, Gerente de Niveles de Servicio, Gerente de Catálogo de

Servicios, Gerente de Disponibilidad, Gerente de la Seguridad, Gerente de Proveedores, Gerente de Capacidades y Gerente de la Continuidad del Servicio.

- **Service transition (transición del servicio)**

Tiene como objetivo establecer las expectativas del cliente acerca de cómo se puede utilizar el servicio para habilitar los procesos de negocio. Asimismo, permite que el proveedor de servicios se enfrente a volúmenes más altos de cambios sin impactar la calidad del servicio.

Establece los siguientes procesos: planeación y soporte en la transición, gestión de cambios, gestión de activos de servicio y de configuraciones, gestión de liberaciones e implementación, validación del servicio y pruebas, evaluación y gestión del conocimiento.

Establece los siguientes roles: Gerente de Activos de Servicio, Gerente de Configuraciones, Gerente de Cambios, Comité Asesor de Cambios, Gerente de Liberaciones e Implementaciones, Gerente de Paquetes y Creación de Versiones e Implementación.

- **Service operation (operación del servicio)**

Tiene como objetivo la gestión continua de la tecnología que se emplea para entregar y soportar los servicios. Asimismo, ejecuta y mide los planes, diseño y optimizaciones. Desde el punto de vista del cliente, la operación del servicio es donde se percibe el valor real, pues la necesidad de efectividad para ayudar a que el negocio cumpla sus resultados es lo que impulsa la eficiencia de las operaciones.

Establece los siguientes procesos: Gestión de Eventos, Gestión de Incidentes, Gestión de Solicitudes del Servicio, Gestión de Problemas y Gestión de Accesos.

Las áreas funcionales establecidas son: Centro de Servicio de Usuario (CSU), Gestión Técnica, Gestión de Operaciones de TI y Gestión de Aplicaciones.

Establece los siguientes roles: Gerente de Incidentes, Gerente de Problemas, Gerente de Centro de Servicios al Usuario, Supervisor del Centro de Servicio al Usuario y Analista del Centro de Servicio al Usuario.

Incidente: Es la interrupción no planeada de un servicio de TI o la reducción en la calidad de un servicio de TI. También, es un incidente la falla de un elemento de configuración que aún no impacta el servicio.

Como ejemplo de incidentes, se tiene la inoperatividad del sistema transaccional de pagos vía web, un disco de un servidor que está lleno totalmente o los tiempos de respuesta del sistema de calificación de clientes ha aumentado sin necesidad de generar indisponibilidad total.

En otra acepción, es un evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Problema: Es la causa desconocida de uno o más Incidentes. Por lo regular, se desconoce la causa al momento de crear un registro de problema y el proceso de la gestión de problemas es responsable de continuar con la investigación.

Solución Temporal: Es la técnica que reduce o elimina el impacto de un incidente o problema para el cual aún no hay disponible una solución completa.

Error Conocido: Es un problema que se tiene identificada la causa raíz y la solución temporal.

Base de datos de errores conocidos (KEDB): Es la base de datos que contiene todos los registros de errores conocidos. Su propósito es almacenar el conocimiento generado de los incidentes y problemas y cómo se pueden resolver, para permitir un diagnóstico y resolución rápidos en caso de que ocurran de nuevo.

Continual Service Improvement - CSI (servicios de mejora continua): Tiene como objetivo alinear continuamente los servicios de TI con los requerimientos de negocio, al identificar e implementar oportunidades de mejora para soportar los procesos de negocio. CSI busca maneras para mejorar la efectividad y la eficiencia para reducir costos.

Establece el siguiente modelo: ¿Cuál es la visión? (visión, misión, metas y objetivos del negocio), ¿Dónde estamos ahora? (evaluaciones de la línea base), ¿Dónde queremos estar? (objetivos medibles), ¿Cómo llegamos ahí? (mejora del servicio y proceso), ¿Llegamos? (mediciones y métricas), ¿Cómo hacemos que el momento continúe?

Establece el siguiente rol: Gerente de la Mejora Continua del Servicio.

Gestión de servicios TI: La administración o gestión de Servicios es un conjunto de capacidades organizacionales especializadas para proporcionar valor a los clientes a través de servicios.

- La administración de servicios toma la forma de un conjunto de funciones y procesos para gestionar servicios a lo largo de su ciclo de vida.
- La administración de servicios también es una práctica profesional respaldada por un extenso conjunto de conocimientos, experiencia y habilidades.
- Es el acto de trasformar los recursos en servicios durante un ciclo de vida.
- Representa la capacidad, competencia y confianza para actuar de una organización de servicios.

Las capacidades de la administración de servicios están influidas por los retos que distinguen los servicios de otros sistemas de creación de valor como la manufactura, minería y agricultura:

- La naturaleza intangible del resultado y los productos intermedios de los procesos del servicio los vuelve difíciles de medir, controlar y validar o probar.
- La naturaleza perecedera de los resultados del servicio y la capacidad del servicio; los clientes necesitan contar con la seguridad de que el servicio seguirá siendo suministrado con una calidad consistente, en tanto que los proveedores necesitan asegurar un suministro estable de demanda por parte de los clientes.
- La demanda está sumamente vinculada a la demanda de activos por parte del cliente para estimular la producción de servicios.

- A medida que se incrementa la madurez de la administración de servicios, se pueden entregar niveles más altos de utilidad y garantía sin un incremento proporcional en el uso de los recursos, en concreto los costos y personal (Repositorio digital de Tesis PUCP).

3.3.1.3. VAL-IT

El marco de trabajo Val IT del IT Governance Institute (ITGI) permite a las organizaciones optimizar la realización de valor de las inversiones en TI. Donde se fundamenta en dominios, procesos, prácticas claves que ayudan a la alta dirección a comprender y desempeñar sus roles relacionados con dichas inversiones. VAL IT proporciona los medios para medir, monitorizar y optimizar la realización de valor de negocio a partir de la inversión en TI.

El marco de Val IT se centra en la decisión de invertir (¿estamos haciendo lo correcto?) y la realización de beneficios (¿estamos obteniendo beneficios?), proporciona un complemento de procesos de soporte y otros materiales de orientación desarrollados para ayudar al consejo y a la dirección ejecutiva a comprender y desempeñar sus papeles relacionados con las inversiones de negocio posibilitadas por TI.

COBIT establece las buenas prácticas que contribuyen a la creación de valor de los procesos y VAL IT establece buenas prácticas proporcionando a las empresas la estructura que necesitan para realizar una adecuada gestión de las inversiones TI que le generen valor. Además de inversiones se incluyen los servicios de tecnología, activos y otros recursos.

El marco de trabajo hace énfasis en la palabra Valor siendo una cualidad o apreciación que dan las partes interesadas a algo en términos financieros o no financieros. Dentro del marco se define el "valor como el ciclo de vida total de los beneficios netos relacionados con los costos, ajustados al riesgo y el valor en el tiempo del dinero" y en muchos casos desafía la medición cuantitativa siendo complejo y dinámico. El valor para las organizaciones sin ánimo de lucro, es un concepto más complejo y a menudo de carácter no financiero, el cual, depende de las métricas del negocio, el aumento de los ingresos, calidad de servicio y demás

factores. VAL IT establece un lenguaje común para la gestión de cartera/Portafolio, programas y proyectos. Los principios de VAL IT están encaminados a lo siguiente

- Las inversiones habilitadas por TI deben:
    - Ser administradas por una Cartera/Portafolio de inversiones.
    - Incluir todas las actividades necesarias para alcanzar el valor del negocio.
    - Gestionarán a través de su ciclo de vida económico completo.
- Las prácticas para la entrega de valor deben:
    - Reconocer que hay diferentes categorías de inversiones.
    - Definir y monitorear las métricas clave.
    - Involucrar a los Stakeholders y asignar las responsabilidades apropiadas para la entrega de capacidades y la realización de los beneficios negocio.
    - Continuamente deben ser monitoreadas, evaluadas y mejoradas.

Los principios de VAL IT deben ser aplicados en dominios que a su vez incluyen procesos y prácticas claves de gestión. Los dominios son los siguientes:

Figura No. 3.3 VAL-IT

Fuente: VAL IT - ISACA ((ISACA), Information Technology Governance Institute)

Gobierno de valor (VG – Value Governance):

El objetivo es asegurar el valor óptimo de las inversiones posibilitadas por TI a partir del ciclo de vida económico completo. El Gobierno de la empresa debe ayudar a las organizaciones a establecer un marco de Gobierno para la gestión de valor que se encuentre integrado con el Gobierno general de la empresa, proporcionar dirección estratégica para la toma de decisiones de inversión, definir características de la cartera para apoyar las nuevas inversiones y por ultimo mejorar continuamente la gestión de valor teniendo como base las lecciones aprendidas, observe la Figura No. 3.3.

Gestión de Cartera/Portafolio (PM- Portfolio Management):

Garantiza el valor óptimo a través de la cartera de inversiones ayudando a las empresas a: Establecer y gestionar los perfiles de los recursos de inversión, Definir los límites de inversión, Evaluar, priorizar, seleccionar, aplazar o rechazar las nuevas inversiones, gestionar y optimizar la cartera global y monitorear e informar sobre los resultados de la cartera. Los programas de inversiones posibilitados por TI deben ser gestionados como parte de la cartera total de inversiones, siendo así administradas sobre una base común. Los programas de la cartera deben ser gestionados de forma activa a través de sus ciclos de vida económicos, para optimizar el valor de los programas individuales y de la cartera total. Incluyendo la optimización de los recursos, la gestión de riesgo, portafolio de inversiones a nivel directivo, la identificación y corrección temprana de problemas.

Gestión de inversiones (IM Investment Management):

Asegura que las inversiones individuales de las empresas sean posibilitadas por TI. Cada uno de los dominios de VAL IT tiene niveles de madurez que identifican la situación actual de la empresa y los estados futuros posibles. Proporciona una escala incremental de 0 a 5. Cada nivel involucra conocimiento, comunicación, responsables, fijación de objetivos, políticas, estándares, herramientas y automatización. Los procesos de VAL IT tienen unas prácticas de gestión que

proporcionan una guía para establecer y gestionar los procesos de gestión de valor y su entorno. Las prácticas de gestión que componen cada dominio se pueden ver en detalle en el Marco de VAL IT. Cada práctica de gestión se compone de los siguientes ítems: Entradas y salidas, Roles y responsabilidades (Cada proceso de Val IT tiene en RACI un Responsable ®, Rendidor de cuentas ®, Persona que Consulta © y Persona que se la informa (I)) y Objetivos y métricas (Se definen en tres niveles: Dominio, proceso y actividad).

Las practicas de gestión de los procesos y los modelos de madurez complementan la información de cada dominio y son base para que las organizaciones puedan implementar VAL IT (Universidad ICESI).

3.3.1.4. Norma de Riesgo Operativo

La Norma de Riesgo Operativo para la gestión y administración del riesgo operacional emitida por el equipo técnico de la Superintendencia de Bancos y Seguros (SBS) ha organizado un conjunto de mejores prácticas para mitigar o controlar los riesgos que forman la base del riesgo operacional.

Entre las fuentes de referencia el equipo ha considerado las recomendaciones del Comité de Basilea, modelos de Sistemas de Aseguramiento de la Información tales como ISO/IEC 17799, modelos de Administración de la Tecnología Informática a nivel de Gobierno Corporativo tales como COBIT, entre otros modelos reconocidos como los mejores a nivel global.

Este compendio de mejores prácticas preparado por el equipo de riesgos de la SBS representa un conjunto importante de cambios que permitirán a las empresas mejorar sus controles sobre el riesgo operacional, pero también representan un importante conjunto de inversiones en esfuerzo y presupuesto para las instituciones (Riesgo operativo en el Ecuador).

3.4. Conocimiento de la Entidad y Entorno del Área de Tecnología de Información y Comunicación.

Para el desarrollo de una auditoría de gestión a las TIC´s, es muy importante que el auditor, conozca el entorno de la entidad y del Área de Tecnología de la Información, procesos sistematizados, organización del área de tecnología de información y comunicaciones, planes estratégicos de TIC, planes operativos, planes de contingencia y/o continuidad del negocio relacionado con la tecnología de la información, planes de mantenimiento preventivo y correctivo de la plataforma tecnológica con la que cuenta la entidad, de manera que le permita una adecuada planificación de su trabajo, pues ese conocimiento le brinda un marco conceptual, que le permite evaluar si la organización sigue un enfoque estructurado de gestión informática y si el mismo es adecuado.

3.4.1. Organización de Área TIC

El auditor debe de conocer, comprender y analizar la arquitectura organizacional de la Entidad de manera general, identificando las ideas rectoras, organización, instrumentos administrativos, recursos humanos (principales funcionarios), productos y servicios de la entidad, así como la relación que mantiene con otras organizaciones y del conocimiento de la función del área de Tecnología de Información y Comunicaciones principalmente en aspectos como: Arquitectura Organizacional, Ideas Rectoras, Objetivos y metas operativas, Instrumentos Administrativos, Organización y función, Procesos, Productos y/o Servicios, Insumos y el entorno de la función de Tecnología de Información y Comunicaciones (clientes), aplicando procedimientos general estales como:

- Revisar y evaluar si la función de TIC está alineada con la misión, visión, valores, objetivos y estrategias de la organización y deberá revisar el desempeño esperado por la empresa (eficacia y eficiencia) y evaluar su cumplimiento.
- Revisar y evaluar la eficacia de los recursos de TIC y el desempeño de los procesos administrativos.
- Se debe utilizar un enfoque basado en riesgos para evaluar la función de TIC.
- Se deberá revisar y evaluar el ambiente de control de la organización.

- Se deberá de revisar las áreas físicas de TIC´s, con el propósito si está en condiciones para la operatividad de las Tecnologías de la Información y Comunicaciones.
- Se deberá de revisar las funciones de cada uno de los técnicos para comprobar si estos cuentan con herramientas y condiciones necesarias para realizar su trabajo y de la optimización de los recursos tecnológicos.
- Se deberá de verificar y analizar el Manual de funciones sea aplicable y acorde a la realidad de las funciones desarrolladas por el capital humano del Área de Tecnología de Información y Comunicaciones.

3.4.2. Infraestructura Tecnológica de la Entidad

El auditor debe conocer, comprender y analizar de forma general la Gestión en Tecnología de la Información, la infraestructura o plataforma tecnológica y los sistemas de información aplicados a la entidad, tales como:

- Granja de Servidores y sus características.
- Seguridad Perimetral.
- Estructura de redes.
- Sistemas Operativos.
- Software y hardware de seguridad.
- El inventario de Hardware y Software con el propósito de establecer el nivel de obsolescencia o actualización.
- Servicios tercerizados contratados por la entidad y vinculados con la tecnología de la información y comunicaciones.
- Adquisiciones (Inversiones) en recursos de Tecnología de la información.
- Infraestructura eléctrica, entre otras.

Sistemas de Información (Aplicaciones)

- Procesos y/o funciones (sustantivos, apoyo y administrativos) de la entidad, que están soportados con tecnología de información y comunicaciones.
- La Administración de Sistemas y Bases de Datos.

- Adopción de Metodologías de Análisis y desarrollo de Sistemas.
- Lenguajes de programación.
- Aplicaciones en producción y desarrollo
- Gestores de bases de datos.

3.4.3. Plan Maestro de Tecnología de Información y Comunicaciones

Como producto del proceso de gestión, el área de tecnología de información y comunicaciones debe elaborar un plan maestro, definido como un documento a largo plazo que contenga la estrategia de proyectos de modernización de los procesos institucionales a través de los recursos tecnológicos, con el objetivo de brindar con calidad el servicio ofrecido a los usuarios (Clientes) de la entidad, entre los aspectos mínimos que conforman dicho plan se encuentran los siguientes:

- Objetivos estratégicos institucionales.
- Misión
- Visión
- Acciones estratégicas.
- Procesos que serán automatizados.
- Usuarios que intervienen en el proceso.
- Recursos humanos, materiales, financieros y técnicos.
- Cronograma de implementación de proyectos.

3.4.4. Planes Operativos

Los planes operativos son un instrumento de control a corto plazo que el auditor debe revisar, y que éstos contengan el desglose de las actividades y acciones a desarrollar que conforman cada línea estratégica del plan maestro, plasmándose lo siguiente:

- Objetivo general
- Objetivos específicos
- Líneas estratégicas y acciones a corto plazo
- Responsables de los proyectos a desarrollar.
- Recursos humanos, materiales, financieros y técnicos

- Cronogramas de actividades a desarrollar en el periodo.

3.4.5. Planes de Continuidad

Es un conjunto de tareas que el área de TIC debe realizar en caso de fallas en los sistemas impidan el normal funcionamiento de los servicios TIC, el fin es recuperar a la brevedad las operaciones de la organización.

El auditor debe conocer y analizar el plan de contingencia implementado por la entidad para poder auditarlo, con el propósito de determinar el grado de efectividad y eficiencia para brindar continuidad en los servicios de TIC y minimizar la probabilidad y el impacto de interrupciones en los servicios, funciones y procesos claves del negocio.

Además se debe de conocer y comprender que el área de TIC´s ha requerido procedimientos para los planes de contingencia de servicios tecnológicos y de comunicaciones contratados con terceros con el propósito garantizar la continuidad del negocio, alinear los procesos de recuperación y determinar el impacto de la contingencia; para esto deberá de realizar con los proveedores pruebas de contingencia para determinar la veracidad del plan presentado.

3.4.6. Planes de Mantenimiento

El auditor debe comprender y analizar los planes de mantenimiento de la Infraestructura o plataforma Tecnología (hardware y software) implementado por el área de TIC, con el objetivo de verificar que la plataforma tecnológica garantice un funcionamiento continuo, disponibilidad y oportunidad de la información.

3.4.7. Presupuesto Tecnológico

El auditor debe revisar que las inversiones en recursos tecnológicos hechas por las entidades del sector público, han contribuido a maximizar el desempeño de la organización y si éstas fueron administradas adecuadamente.

El área de Tecnología de Información y Comunicaciones debe concentrar un presupuesto tecnológico institucional que considere todas las necesidades de

(hardware y software), para lo que, el auditor debe verificar que toda contratación se incluya y se autorice en el plan anual de compras.

El auditor con base a este plan debe evaluar el proceso de contratación, priorizando en el cumplimiento de las especificaciones técnicas, recepción del bien o servicio y utilidad de los mismos de acuerdo a las necesidades requeridas por las unidades solicitantes.

3.5. Plan de Trabajo de Auditoria TIC´s

Después que los auditores han conocido la entidad y el área de tecnología de información y comunicaciones e identificado posibles asuntos de importancia (líneas preliminares a examinar) que hayan llamado la atención, se listan y se agruparán por proyectos, deberá de incluir su conocimiento y análisis en un documento metodológico que evidencia la estrategia y alcance de la auditoría, el contenido se describe a continuación:

- Antecedentes la entidad y el área TIC
- Organigrama de TIC
- Objetivos general y específicos de TIC
- Naturaleza y alcance de la auditoria
- Estrategia de la auditoría
- Enfoque de la auditoria
- Fundamento de la auditoría
- Agrupación de Asuntos de Importancia y Determinación de
- Proyectos a Examinar en la Fase de Análisis Previo.
- Leyes aplicables al proceso de la auditoria
- Recursos (humanos, materiales y técnicos) del equipo de auditoria
- Cronograma de trabajo
- Programa de auditoría para iniciar la etapa de análisis previo.

Uno de los estándares que más se están utilizando en el mundo para ser tomado como base para realizar una metodología de auditoría en el ambiente de tecnología informática y sistemas de información, es el denominado COBIT. El marco de referencia COBIT otorga especial importancia al impacto sobre los

recursos de tecnología informática, así como a los requerimientos de negocios en cuanto a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad que deben ser satisfechos. Además, el marco de referencia proporciona definiciones para los requerimientos de negocio que son derivados de objetivos de control superiores en lo referente a calidad, seguridad y reportes fiduciarios en tanto se relacionen con tecnología de información.

La orientación a negocios es el tema principal de COBIT. Está diseñado no sólo para ser utilizado por usuarios y auditores, sino que en forma más importante, está diseñado para ser utilizado como una lista de verificación detallada para los propietarios de los procesos de negocio. En forma incremental, las prácticas de negocio requieren de una mayor delegación y otorgamiento de autoridad de los dueños de procesos para que éstos posean total responsabilidad de todos los aspectos relacionados con dichos procesos de negocio. En forma particular, esto incluye el proporcionar controles adecuados y herramientas al propietario de procesos de negocio que faciliten el cumplimiento de esta responsabilidad.

3.6. Análisis Previo

Como resultado de los procedimientos aplicados al conocimiento y comprensión del área de Tecnología de Información y Comunicación y de la Plataforma Tecnológica de la entidad, se elaborarán programas de auditoría dirigidos a examinar lo que a criterio del equipo de auditoría les llamó la atención, para dirigir de forma adecuada los procedimientos que desarrollarán los objetivos de la auditoria.

3.6.1. Áreas Preliminares a Examinar

3.6.1.1. Organización y Planificación de TI

El auditor debe de realizar una evaluación y análisis de la estructura organizativa y la planificación del Área de TIC, con el propósito obtener una definición clara de las funciones, líneas de autoridad y responsabilidad de las diferentes unidades que conforman el Área de Tecnología de Información y Comunicaciones, además se debe analizar si es recomendable la ubicación actual dentro del organigrama institucional o amerite que el Área de tecnología de

información y comunicaciones debe estar al más alto nivel de la pirámide administrativa para cumplimiento de sus objetivos y cuente con el apoyo necesario de la máxima autoridad.

El auditor debe de constatar y analizar que el área de TIC ha implementado y está cumpliendo con los controles siguientes:

Se debe evitar que una misma persona tenga el control de toda una operación. Se refiere a la definición clara de funciones, línea de autoridad y responsabilidad del área de TIC, en labores tales como:

- Diseñar un sistema
- Elaborar los programas
- Operar el sistema
- Control de calidad

Acciones a seguir:

- La unidad informática debe estar al más alto nivel de la pirámide administrativa de manera que cumpla con sus objetivos, cuente con el apoyo necesario y la dirección efectiva.
- Las funciones de operación, programación y diseño de sistemas deben estar claramente delimitadas.
- Deben existir mecanismos necesarios a fin de asegurar que los programadores y analistas no tengan acceso a la operación del computador y los operadores a su vez no conozcan la documentación de programas y sistemas.
- Debe existir una unidad de control de calidad, tanto de datos de entrada como de los resultados del procesamiento.
- El manejo y custodia de dispositivos y archivos magnéticos deben estar expresamente definidos por escrito.
- Las actividades del área de TIC deben obedecer a planificaciones a corto, mediano y largo plazo sujetos a evaluación y ajustes periódicos “Plan Maestro de Informática”

- Debe existir una participación efectiva de directivos, usuarios y personal del área de TIC en la planificación y evaluación del cumplimiento del plan.
- Las instrucciones deben impartirse por escrito.

Deben existir mecanismos necesarios a fin de asegurar que los programadores y analistas no tengan acceso a la operación del computador y los operadores a su vez no conozcan la documentación de programas y sistemas.

Los accesos a programas y sistemas deben estar segmentados de acuerdo al perfil del usuario. La clasificación general es:

- Los usuarios del sistema:
- Los usuarios del sistema son los que podrán generar transacciones reales, o usar las funciones del sistema en producción. Podrán también accesar a los archivos generados por el sistema producto de las transacciones.
- Los programadores del sistema y, analistas:
- Los programadores solo deben tener acceso al ambiente de pruebas o desarrollo. No deben tener acceso a transacciones reales o a accesar a funciones del sistema en producción.
- Debe existir una unidad de control de calidad, tanto de datos de entrada como de los resultados del procesamiento.
- El manejo y custodia de dispositivos y archivos magnéticos deben estar expresamente definidos por escrito.
- Las instrucciones deben impartirse por escrito.

3.6.1.2. Procesamiento Electrónico de Datos

Los auditores deberán revisar los controles en las operaciones del procesamiento electrónico de datos en los siguientes aspectos:

1.- Revisión de controles en el equipo.

Se hace para verificar si existen formas adecuadas de detectar errores de procesamiento, prevenir accesos no autorizados y mantener un registro detallado de todas las actividades del computador que debe ser analizado periódicamente.

2.- Revisión de programas de operación.

Se verificará que el cronograma de actividades para procesar los datos, asegure la utilización efectiva del computador.

3.- Revisión de controles ambientales.

Se hace para verificar si los equipos tienen un ambiente físico adecuado, es decir si se cuenta con aire acondicionado, fuentes de energía continua, extintores de incendios, etc.

4.- Revisión del plan de mantenimiento.

Se verificará que todos los equipos principales tengan un adecuado mantenimiento que garantice su funcionamiento continuo.

5.- Revisión del sistema de administración de archivos.

Se hace para verificar que existan formas adecuadas de organizar los archivos en el computador, que estén respaldados, así como asegurar que el uso que le dan es el autorizado.

6.- Revisión del plan de contingencias.

En esta sección se verificará si el plan de contingencia es apropiado para garantizar la continuidad del negocio, las operaciones y la recuperación de información ante contingencias humanas o naturales que puedan poner en peligro las operaciones, pérdida de información, infecciones de virus entre otras, el cual debe de contener como requisitos mínimos los siguientes:

- Considera requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI.
- Cubre los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.
- Considera los requerimientos de respuesta y recuperación para diferentes niveles de prioridad, por ejemplo, de una a cuatro horas, de cuatro a 24 horas, más de 24 horas y para periodos críticos de operación del negocio.
- Se ha centrado la atención en los puntos determinados como los más críticos en el plan de continuidad para construir resistencia y establecer prioridades en situaciones de recuperación.

- Procedimientos de control de cambios, para asegurar que el plan de continuidad se mantenga actualizado y que refleje de manera continúa los requerimientos actuales del negocio.

3.6.1.3. Evaluación de los Sistemas Informáticos

Evaluación de los diferentes sistemas informáticos en operación (flujo de información, procedimientos, documentación, redundancia, organización de archivos, estándares de programación, controles, utilización de los sistemas).

Los puntos a evaluar son:

- Entradas.
- Salidas.
- Procesos.
- Especificaciones de datos.
- Especificaciones de proceso.
- Métodos de acceso.
- Operaciones.
- Manipulación de datos (antes y después del proceso electrónico de datos).
- Proceso lógico necesario para producir informes.
- Identificación de archivos, tamaño de los campos y registros.
- Proceso en línea o lote y su justificación.
- Frecuencia y volúmenes de operación.
- Sistemas de seguridad.
- Sistemas de control.
- Responsables.
- Número de usuarios.

Dentro del estudio de los sistemas en uso se deberá solicitar:

- Manual del usuario.
- Descripción de flujo de información y/o procesos.
- Descripción y distribución de información.
- Manual de formas.
- Manual de reportes.

- Lista de archivos y especificaciones.

Lo que se debe determinar en el sistema:

En el procedimiento:

- ¿Quién hace, cuando y como?
- ¿Qué formas se utilizan en el sistema?
- ¿Son necesarias, se usan, están duplicadas?
- ¿El número de copias es el adecuado?
- ¿Existen puntos de controlo faltan?

En la gráfica de flujo de información:

- ¿Es fácil de usar?
- ¿Es lógica?
- ¿Se encontraron lagunas?
- ¿Hay faltas de control?

En el diseño:

- ¿Cómo se usará la herramienta de diseño si existe?
- ¿Qué también se ajusta la herramienta al procedimiento?

Evaluación del avance de los sistemas informáticos en desarrollo y congruencia con el diseño general.

Seguridad física y lógica de los sistemas informáticos, su confidencialidad y respaldos.

3.6.1.4. Controles de Sistema en Desarrollo y Producción

El auditor debe de verificar y asegurarse que el Área de Tecnología de Información y Comunicaciones ha justificado que los sistemas informáticos adquiridos a terceros y desarrollados internamente han sido la mejor opción para la entidad y que proporcionen oportuna y efectiva información, y se han desarrollado bajo un proceso planificado y se encuentren debidamente documentado.

Procedimientos a seguir:

Asegurarse que los usuarios han participado en el diseño e implantación de los sistemas informáticos, pues aportan conocimiento y experiencia de su área y esta

actividad coadyuva a una mejor cultura tecnológica en el cambio de los procesos institucionales.

Verificar que el área de auditoría interna ha formado parte del grupo de diseño para sugerir y solicitar la implantación de rutinas de huellas de auditoría.

- Evaluar si el desarrollo, diseño y mantenimiento de sistemas obedece a planes específicos, metodologías del ciclo de vida de desarrollo de sistemas, procedimientos y en general a normativa escrita y aprobada.
- Evaluar si cada fase concluida esta aprobada y documentada por los usuarios mediante actas u otros mecanismos, a fin de evitar reclamos posteriores.
- Constatar si los aplicativos antes de pasar a producción son probados con datos que agoten todas las excepciones posibles.
- Comprobar si todos los sistemas informáticos están debidamente documentados y actualizados.
- Evaluar si han implantado procedimientos de solicitud, aprobación y ejecución de cambios a programas, formatos de los sistemas en desarrollo.
- Verificar si el sistema informático es entregado al usuario previo entrenamiento y elaboración de los manuales de operación respectivos
- Para el procesamiento electrónico de datos en los sistemas informáticos el auditor debe de considerar:
- Evaluar la validación de datos de entrada, procesamiento y salida, este proceso es realizado en forma automática.
- Verificar que la preparación de los datos de entrada sea responsabilidad de los usuarios y consecuentemente su corrección.
- Verificar la adopción de acciones necesaria para correcciones de errores.
- Evaluación de la planificación del mantenimiento del hardware y aplicativos informáticos, tomando todas las medidas de seguridad para garantizar la integridad.

3.6.1.5. Evaluación de los Equipos

- Capacidades
- Utilización

- Nuevos Proyectos
- Seguridad física y lógica

El auditor debe de constatar que el Área de la Tecnología de Información y Comunicaciones ha implementado controles tales como:

Controles de Adquisición:

El propósito es asegurar que el hardware y software adquirido a terceros proporcione mayores beneficios que cualquier otra alternativa y garantizar la selección adecuada de equipos y sistemas informáticos.

Procedimientos a seguir:

- Revisión de un informe técnico en el que se justifique la adquisición del equipo, software y servicios informáticos incluyendo un estudio costo-beneficio.
- Formación de un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación
- Elaborar un instructivo con procedimientos a seguir para la selección y adquisición de equipos, programas y servicios informáticos. Este proceso debe enmarcarse en normas y disposiciones legales.
- Revisar el respaldo de mantenimiento y asistencia técnica de los equipos informáticos.

3.6.1.6. Evaluación de la Seguridad de la Información

Los equipos informáticos son instrumentos que estructuran grandes cantidades de información, la cual puede ser confidencial para la entidad y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta; además pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de las actividades de procesamiento electrónico de datos. Esta información puede ser de suma importancia, y al no contar con ella en el momento preciso puede provocar retrasos sumamente costosos.

Al auditar los sistemas informáticos, el auditor debe verificar y constatar lo siguiente:

- Que no se tengan copias “piratas” o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión de virus.
- Que se hayan implementado procesos físicos y lógicos para la protección del hardware y datos procesados, así como a las instalaciones de ingreso al área de procesamiento de datos y servidores. Contemplando las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.
- Implementación de mecanismos para garantizar la seguridad lógica del software, a la protección de los datos e información, procesos y programas, así como la restricción de usuarios no autorizados al acceso de la información.

3.7. Modelo de Auditoria

El Modelo muestra como la Norma de Riesgo operativo se alinea con otros estándares y mejores prácticas como COBIT (4.1 y 5.0), ITIL y VAL - IT.

A continuación se presenta una parte del modelo, para observarlo en su totalidad ver el Anexo 1, Modelo de Auditoria (CD).

Tabla 3.1 Modelo de Auditoria

Continua ➡

	SS 5.4 Métodos de gestión del portafolio de servicios.	PM13 Volver a priorizar la cartera. IM2 Desarrollar un caso de negocio del concepto de programa inicial. IM3 Adquirir un claro entendimiento de los programas candidatos. IM4 Realizar análisis de alternativas. IM5 Desarrollar un plan de programas.

Continua ➡

	IM6 Desarrollar un plan de realización de beneficios. IM7 Identificar costes y beneficios de todo el ciclo de vida. IM8 Desarrollar un caso de negocio detallado del programa. IM9 Asignar claramente la responsabilidad y propiedad.

3.8. Organigrama de la COAC Textil 14 de Marzo

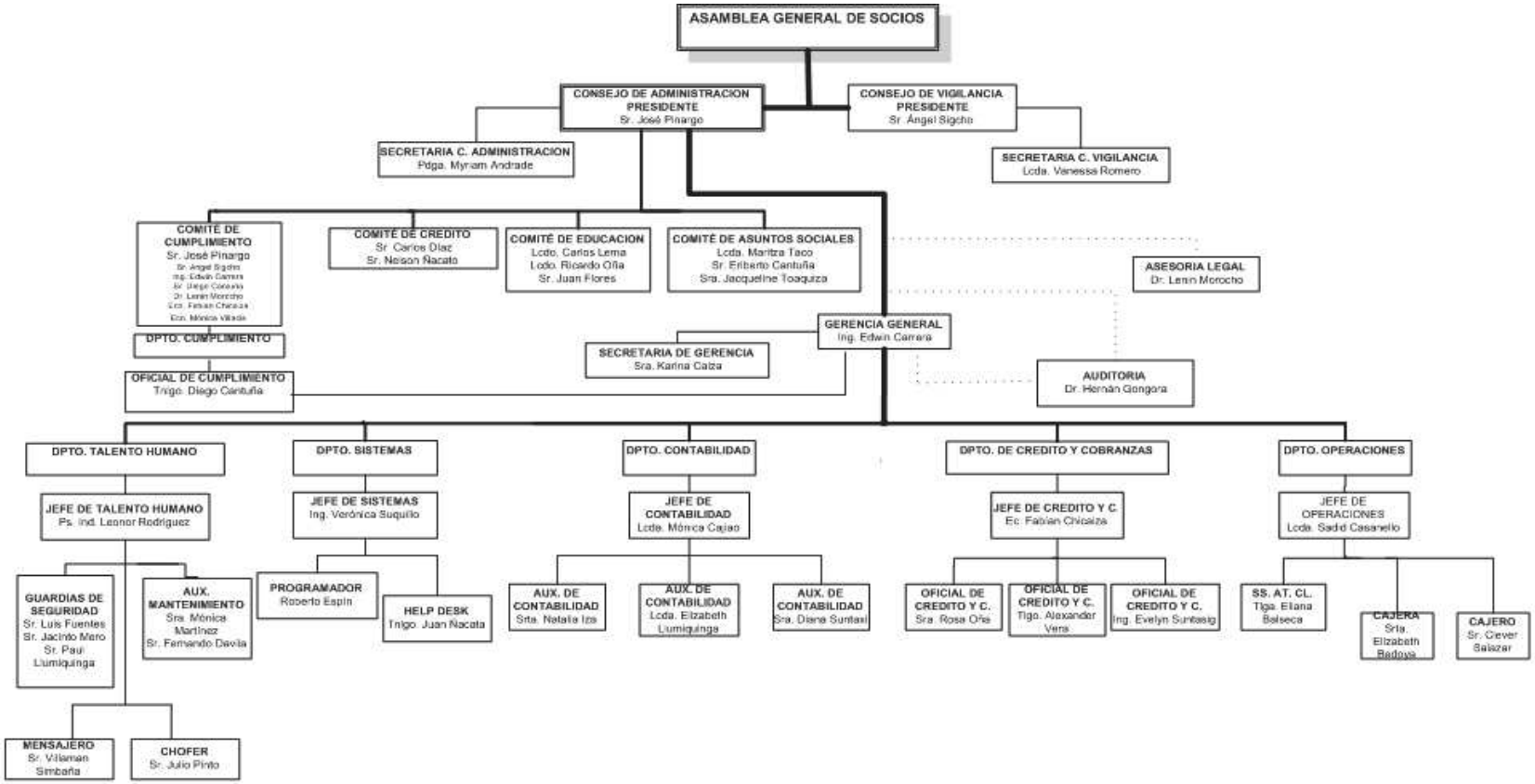


Figura No. 3.4 Organigrama de la COAC Textil 14 de Marzo

Fuente: VAL IT - ISACA

3.9. Directrices de Auditoria

Contienen los pasos de auditoría correspondientes para cada uno de los ítems de la Norma de Riesgo Operativo que han sido tomados como base, recordando que han sido alineados con COBIT (4.1 y 5.0), ITIL y VAL IT, como se puede ver en Tabla No. 3.1. Estos pasos proporcionaran asistencia a los auditores de sistemas en la revisión de los procesos de TI.

Con el fin de proporcionar la información que la empresa necesita para alcanzar una adecuada gestión de TIC's se han definido 250 objetivos de control, ver Tabla No. 3.2.; que cubren todos los aspectos de información y de la tecnología que la soporta.

El cumplimientos de estos objetivos se alcanzara a través de entrevistas con los distintos miembros de la organización, ver Figura No. 3.4 y obteniendo de estas entrevistas información, ver Tabla No. 3.3.

Los objetivos de control que deben cumplirse para tener el proceso de TI bajo control son:

Tabla No. 3.2 Objetivos de Control

Aceptación de Riesgos	**Obj.2**
Acreditación/Certificación Independiente de la Seguridad y el Control Interno de los Proveedores Externos de Servicios	**Obj.4**
Actividades de Seguimiento	**Obj.6**

Continua

Administración de Almacenamiento	**Obj.9**
Administración de Llaves Criptográficas	**Obj.11**
Adquisición de Productos de Software	**Obj.13**
Almacenamiento de Software	**Obj.15**
Aprobación de las Fases del Proyecto	**Obj.17**
Aprobación del Proyecto	**Obj.19**
Arquitectura de Información	**Obj.21**
Aseguramiento Independiente del Cumplimiento de Requerimientos Regulativos y Legales y de Compromisos Contractuales por parte de Proveedores Externos de Servicios	**Obj.23**
Aspectos sobre los Acuerdos de Nivel de Servicio	**Obj.25**
Balanceo y Conciliación de Datos de Salida	**Obj.27**
Bitácoras de Operación	**Obj.29**

Continua

Cambios Significativos a Sistemas Actuales	Obj.32
Capacitación para el Plan de Continuidad de TI	Obj.34
Clasificación de Datos	Obj.36
Comunicación de la Sensibilización de Seguridad de la TI	Obj.38
Confianza en el Colega	Obj.40
Contenido del Plan de Continuidad de TI	Obj.42
Continuidad de Procesamiento	Obj.44
Contratación de Auditoría	Obj.46
Control de Abastecimiento	Obj.48
Control de la Configuración	Obj.50
Controles Económicos de Seguridad	Obj.52
Criterios y Desempeño de Pruebas en Paralelo/Piloto	Obj.54
Cumplimiento con los Contratos de Seguros	Obj.56

Continua

Cumplimiento de Políticas, Procedimientos y Estándares	**Obj.58**
Definición de Requerimientos de Información	**Obj.60**
Definición y Documentación de Requerimientos de Archivos	**Obj.62**
Definición y Documentación de Requerimientos de Procesamiento	**Obj.64**
Derechos de la Propiedad Intelectual	**Obj.66**
Diccionario de Datos y Reglas de Sintaxis de Datos de la Corporación	**Obj.68**
Diseño para la Recopilación de Datos Fuente	**Obj.70**
Distribución de Salida de Datos	**Obj.72**
Distribución del Plan de Continuidad de TI	**Obj.74**
Documentación y Procedimientos	**Obj.76**

Continua

Entrenamiento al Personal sobre los Software de Aplicaciones	Obj.79
Ergonomía	Obj.81
Escalamiento de Problemas	Obj.83
Especificaciones de Programas	Obj.85
Estado de Cuenta	Obj.87
Estipulaciones de Integridad TI para Software de Programas de Aplicación	Obj.89
Estudio de Factibilidad Económica	Obj.91
Ética y Estándares Profesionales	Obj.93
Evaluación de la Satisfacción de los Requerimientos del Usuario	Obj.95
Evaluación de Nuevo Hardware y Software	Obj.97
Evaluación del Riesgo del Negocio	Obj.99

Continua ➡

Evaluar el Desempeño	Obj.102
Formulación de Acciones Alternativas	Obj.104
Funciones y Responsabilidades de los Miembros de la Organización	Obj.106
Herramientas de Modelado	Obj.108
Identificación de necesidades de entrenamiento	Obj.110
Identificación, Autenticación y Acceso	Obj.112
Inicio y Control de Requisiciones de Cambio	Obj.114
Instalaciones de Tecnología de Información	Obj.116
Integridad de Procesamiento de Datos	Obj.118
Interface Usuario -Máquina	Obj.120
Justificación de Costos	Obj.122
Manejo de Errores de Documentos Fuente	Obj.124
Manejo de Errores en la Entrada de Datos	Obj.126

Continua

Manejo de las Medidas de Seguridad	Obj.128
Manejo y Retención de Salida de Datos	Obj.130
Mantenimiento de Políticas	Obj.132
Mantenimiento del Plan de Continuidad de TI	Obj.134
Mantenimiento Preventivo para Hardware	Obj.136
Manual de Procedimientos de Operación e Instrucciones	Obj.138
Marco de Referencia para Continuidad de TI	Obj.140
Marco Referencial para la Administración de Proyectos	Obj.142
Material de Entrenamiento	Obj.144
Medición de Riesgos	Obj.146
Métodos de Diseño de Software Documentados	Obj.148
Miembros y Responsabilidades del Equipo del Proyecto	Obj.150
Monitoreo de Atención a Clientes	Obj.152
Monitoreo de Tendencias y Regulaciones Futuras	Obj.154

Continua

Continua

Prevención, Detección y Corrección del Software Dañino	Obj.181
Procedimientos de Autorización de Entrada de Datos	Obj.183
Procedimientos de Preparación de Datos	Obj.185
Programa de Mejoramiento del Servicio	Obj.187
Pronóstico de Carga de Trabajo	Obj.189
Propiedad y Custodia de los Activos de TI	Obj.191
Protección de Información Sensible	Obj.193
Protección de las Funciones de Seguridad	Obj.195
Protección del Valor Electrónico	Obj.197
Prueba de Aceptación Final	Obj.199
Prueba Operacional	Obj.201
Pruebas de Software de Aplicación	Obj.203
Realización del Trabajo de Auditoría	Obj.205
Recolectar Datos de Monitoreo	Obj.207

Continua

Continua

Salud y Seguridad del Personal	**Obj.235**
Seguimiento de Problemas y Pistas de Auditoría	**Obj.237**
Seguridad de Acceso a Datos en Línea	**Obj.239**
Seguridad Física	**Obj.241**
Sistema de Administración de la Librería de Medios	**Obj.243**
Software no Autorizado	**Obj.245**
Tecnología de Información como parte del Plan a Largo y Corto Plazo	**Obj.247**
Validación y Edición de Procesamiento de Datos	**Obj.249**

Los objetivos de control son auditados al obtener un entendimiento a través de entrevistas con los diferentes miembros de la organización obteniendo:

Tabla No. 3.3 Obtenibles

Continua ➡

Archivos personales que muestren las credenciales y experiencia profesional del personal de la Mesa de Ayuda	Obt. 3
Contenido del material de entrenamiento de seguridad para nuevos empleados	Obt. 5
Contratos con proveedores relacionados con servicios de desarrollo de aplicación	Obt. 7
Contratos, presupuestos, reportes previos e historial de desempeño de aseguramiento independiente	Obt. 9
Copia del documento de planeación de recuperación/contingencia en caso de desastre	Obt. 11
Copias de los contratos de los proveedores de servicios de transmisión de datos	Obt. 13
Copias de todos los contratos de seguros relacionados con el Departamento de Sistemas	Obt. 15

Continua ➡

Descripción de los puestos clave del Departamento de Sistemas	**Obt. 17**
Detalles de la base sobre la cual se miden los riesgos y la exposición a los riesgos	**Obt. 19**
Documentación del Departamento de Sistemas relacionada con: **o Reportes de desempeño de nivel de servicio** **o Programas de mejora del servicio** **o Acuerdos de nivel de servicio con usuarios y proveedores.**	**Obt. 21**

Continua ➡

Documentos de disponibilidad, capacidad, carga de trabajo y planeación de recursos	**Obt. 24**
Documentos de evaluación de riesgos del negocio	**Obt. 26**
Documentos de planeación del Departamento de Sistemas con objetivos para cada grupo de recursos y el desempeño real en comparación con dichos planes	**Obt. 28**
El documento del marco referencial de seguridad y control interno especifica la política, propósito, objetivos, estructura administrativa, alcance dentro de la organización, asignación de responsabilidades y definición de sanciones y acciones disciplinarias de seguridad y control interno asociados con la falta de cumplimiento de las políticas de seguridad y control interno	**Obt. 30**

Continua ➡

Esquema de clasificación de datos	**Obt. 33**
Estándares relacionados con el comercio electrónico	**Obt. 35**
Estándares/declaraciones contables nacionales o internacionales relacionadas con el uso de comercio electrónico	**Obt. 37**
Existe un programa de conocimiento y conciencia formal para proporcionar comunicación y entrenamiento relacionados con el ambiente positivo de control de la administración	**Obt. 39**
Existen políticas y procedimientos organizacionales para asegurar que los recursos adecuados y apropiados son asignados para implementar las políticas de la organización de manera oportuna	**Obt. 41**

Continua ➡

Existen procedimientos que consideren la necesidad de revisar y aprobar periódicamente estándares, directivas, políticas y procedimientos clave relacionados con tecnología de información	**Obt. 43**
Expedientes del personal seleccionado de la evaluación de riesgos	**Obt. 45**
Funciones y responsabilidades de planeación de la Asamblea General de Socios	**Obt. 47**
Funciones y responsabilidades del Departamento de Sistemas	**Obt. 49**
Historial de experiencia y educación continua del personal de auditoría	**Obt. 51**

Continua ➡

Inventario de dispositivos de encriptación de datos y de estándares de encriptación	**Obt. 54**
Inventario del contenido del almacenamiento fuera de las instalaciones, equipo, archivos, manuales y formas, incluyendo material en manos de los proveedores	**Obt. 56**
La administración del Departamento de Sistemas asegura que la calidad de la filosofía, las políticas y objetivos sea comprendida, implementada y mantenida a todos los niveles del Departamento de Sistemas	**Obt. 58**
La Asamblea General de Socios ha aceptado la responsabilidad total sobre el desarrollo de un marco referencial para el enfoque general de seguridad y control interno	**Obt. 60**

Continua

Las listas de seguridad de acceso con los perfiles y recursos disponibles para los vendedores de TI	**Obt. 63**
Las políticas de seguridad y control interno identifican el proceso de control interno de la organización e incluye componentes de control tales como: **ambiente de control** **reevaluación de riesgos** **actividades de control** **información y comunicación** **monitoreo**	**Obt. 65**

Continua ➡

Lista de los proveedores de servicios utilizados en la transmisión de datos	**Obt. 68**
Listas del contenido de las distintas librerías prueba, desarrollo y producción	**Obt. 70**
Los acuerdos de confidencialidad para todas las relaciones con terceras partes	**Obt. 72**
Los resultados de las pruebas de los planes para usuario de recuperación de desastre/contingencia y reanudación del negocio/contingencia más recientes	**Obt. 74**
Minutas de las reuniones en las que se discuten la planeación de la capacidad, las expectativas de desempeño y la "afinación" del desempeño	**Obt. 76**
Objetivos y planes a corto y largo plazo del Gerente General con respecto a tecnología de información	**Obt. 78**

Continua

Objetivos y planes organizacionales a corto y largo plazo con respecto al retorno de la inversión en TI	**Obt. 81**
Organigrama a nivel de toda la organización y manual de políticas y procedimientos	**Obt. 83**
Organigrama organizacional que muestre la relación entre el Departamento de Sistemas y otros departamentos	**Obt. 85**
Orientación del asesor legal sobre los requerimientos "uberrimae fidei" (de buena fe) para los contratos de seguros (Uberrimae fidei requiere que ambas partes divulguen completamente a la otra todo lo relacionado con el riesgo En caso de no mostrarse buena fe en este sentido, el contrato será anulable por la parte agraviada y no podrá ser puesto en vigor nuevamente por la parte culpable)	**Obt. 87**
Plan de Aseguramiento de la Calidad del Software (Software Quality Assurance Plan (SQAP))	**Obt. 89**
Plan de infraestructura tecnológica	**Obt. 91**

Continua ➡

Plano de los edificios/habitaciones que contienen recursos de sistemas de información	**Obt. 93**
Política de seguridad del usuario o de protección de la información	**Obt. 95**
Políticas de seguros que cubren el riesgo residual	**Obt. 97**
Políticas organizacionales relacionadas con la utilización de software o equipo no autorizado	**Obt. 99**
Políticas y procedimientos del Departamento de Sistemas relacionadas con el monitoreo y el reporte de los controles internos y la frecuencia de las revisiones	**Obt. 101**

Continua ➡

Políticas y procedimientos del Departamento de Sistemas relacionadas con políticas, planeación del ciclo de vida de desarrollo de sistemas para programas, unidades, planes de prueba del sistema, entrenamiento de usuarios, migración de sistemas de prueba a producción, aseguramiento de la calidad y entrenamiento	**Obt. 104**
Políticas y procedimientos del Departamento de Sistemas relacionadas con: el enlace de la capacidad con el plan del negocio, la disponibilidad de los servicios, la planeación de la disponibilidad, el monitoreo continuo y la administración del desempeño	**Obt. 106**

Continua ➡

Políticas y procedimientos del Departamento de Sistemas relacionadas con: seguridad y acceso a los sistemas de información	**Obt. 109**
Políticas y procedimientos del Departamento de Sistemas relacionados con el manejo de problemas, incluyendo procesos de reconocimiento, registro, solución, escalamiento, seguimiento y reporte	**Obt. 111**
Políticas y procedimientos del Departamento de Sistemas relacionados con la disposición o plano de las instalaciones, la seguridad física y lógica, acceso, mantenimiento, visitantes, salud, seguridad y requerimientos ambientales, mecanismos de entrada y salida, reporte de seguridad, contratos de seguridad y mantenimiento, inventario de equipo, procedimientos de vigilancia, y requerimientos regulatorios	**Obt. 113**

Continua ➡

Políticas y procedimientos del Departamento de Sistemas relacionados específicamente con la adquisición, disposición y mantenimiento de los recursos de la configuración	**Obt. 115**
Políticas y procedimientos generales para la organización asociadas a las relaciones proveedor/usuario	**Obt. 117**
Políticas y procedimientos generales para la organización relacionados con el proceso de planeación de recuperación/contingencia	**Obt. 119**

Continua ➡

Políticas y procedimientos globales para la organización relacionados con la disponibilidad ,monitoreo y reporte del desempeño, pronóstico de la carga de trabajo, administración de la capacidad y calendarización	**Obt. 122**
Políticas y procedimientos inherentes al proceso de planeación	**Obt. 124**
Políticas y procedimientos organizacionales relacionadas con la planeación, administración, monitoreo y reporte del desempeño	**Obt. 126**
Políticas y procedimientos organizacionales relacionados con la administración de operaciones y el rol de sistemas de información en el cumplimiento de los objetivos del negocio	**Obt. 128**

Continua ➡

Políticas y procedimientos organizacionales relacionados con la adquisición, inventario y disposición de software y equipo computacional comprado, rentado o arrendado	**Obt. 130**

Continua ➡

○ **Reportes administrativos utilizados para monitorear actividades e inventarios**	
Políticas y procedimientos organizacionales relacionados con: ○ **Planeación estratégica y objetivos del negocio, planeación de sistemas de información y desarrollo de aplicaciones.** ○ **Políticas y procedimientos del Departamento de Sistemas, incluyendo: organigrama, metodología del ciclo de vida de desarrollo de sistemas, planeación de capacidad, manuales de usuarios y operaciones, materiales de entrenamiento, pruebas y migración a estatus de producción y documentos de planeación de reanudación/ contingencia.** ○ **Políticas y procedimientos generales para la organización con respecto a la capacitación sobre controles y conciencia de seguridad, beneficios para los empleados enfocados al desarrollo, programas de capacitación para los**	**Obt. 133**

Continua ➡

○ **Programas de capacitación disponibles (tanto internos como externos) para seguridad y conciencia de controles introductorios y continuos, así como para entrenamiento dentro de la organización**	
Políticas y procedimientos relacionadas con la organización y las relaciones de tecnología de información	**Obt. 135**
Políticas y procedimientos relacionados con el aseguramiento de la calidad	**Obt. 137**

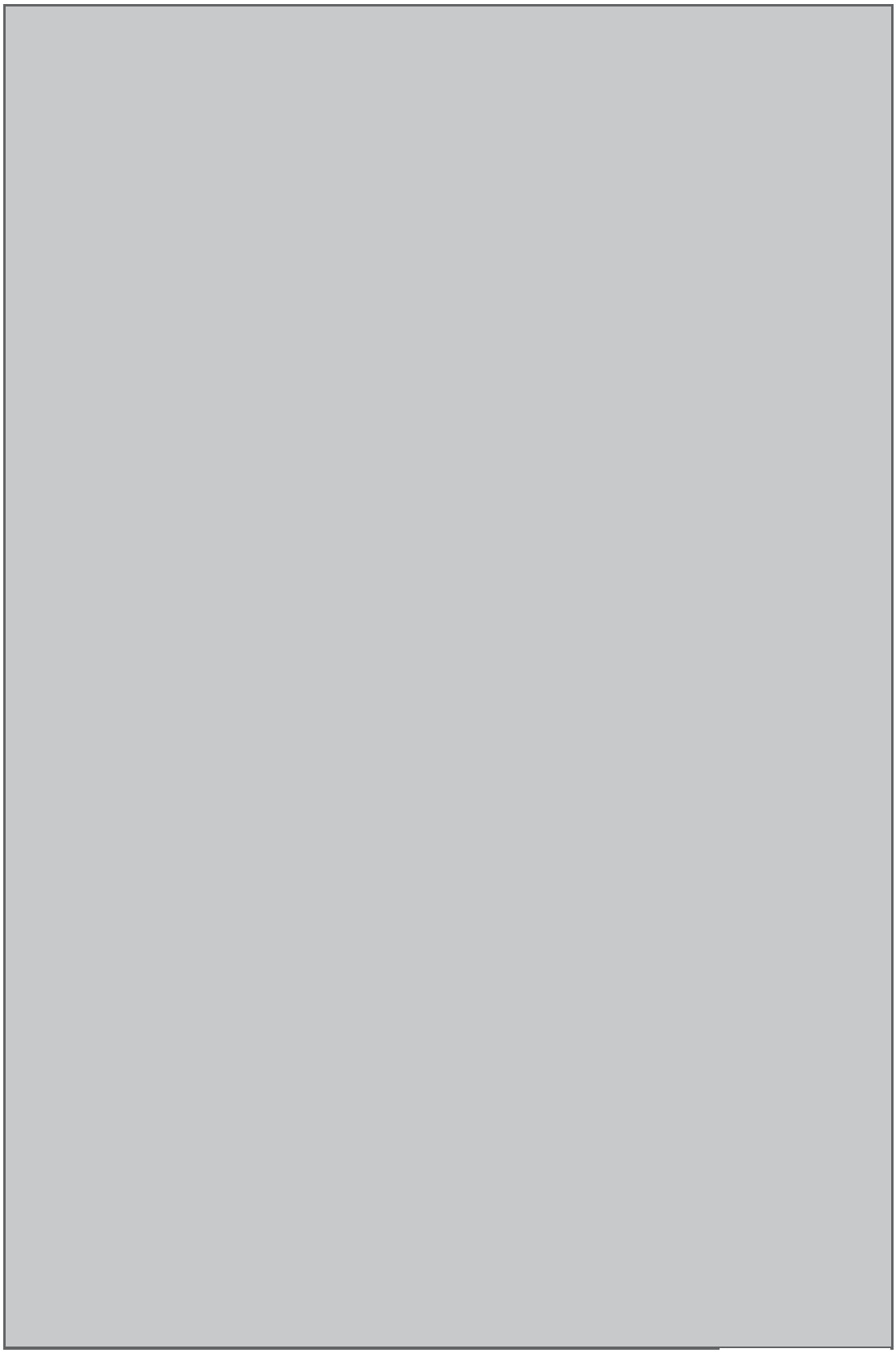
Continua ➡

Políticas y procedimientos relacionados con el marco referencial de administración de proyectos	**Obt. 139**
Políticas y procedimientos relacionados con la evaluación de riesgos	**Obt. 141**

Continua ➡

Políticas y procedimientos relacionados con la metodología de administración de proyectos	**Obt. 143**
Políticas y procedimientos relacionados con la planeación y el monitoreo de la infraestructura tecnológica	**Obt. 145**
Políticas y procedimientos relacionados con los planes de aseguramiento de la calidad	**Obt. 147**
Políticas y procedimientos relativos al proceso de auditoría independiente	**Obt. 149**

Continua ➡



Continua

Políticas y procedimientos sobre la arquitectura de información	**Obt. 151**
Políticas, métodos y procedimientos organizacionales relacionados con la elaboración del presupuesto y las actividades de costeo	**Obt. 153**
Presupuesto de TI anual incluyendo las suposiciones relacionadas con la capacidad y el desempeño	**Obt. 155**
Procedimientos de administración de cuentas de usuario	**Obt. 157**
Procedimientos de seguimiento, solución y escalamiento de problemas	**Obt. 159**
Programas, políticas y procedimientos de entrenamiento y de educación del Departamento de Sistemas relacionados con controles y conciencia de seguridad, seguridad técnica y controles	**Obt. 161**

Continua ➡

Reportes de auditoría de auditores externos, proveedores de servicios como terceras partes y dependencias gubernamentales relacionadas con la seguridad de los sistemas	**Obt. 164**
Reportes de calidad del Proyecto	**Obt. 166**
Reportes de las actividades del Departamento de Sistemas incluyendo, pero no limitados a: reportes internos, reportes de auditorías internas, reportes de auditorías externas, reportes de usuarios, encuestas de satisfacción de los usuarios, planes de desarrollo de sistemas y reportes de avance, minutas del comité de auditoría y cualquier otro tipo de evaluación del uso de los recursos del Departamento de Sistemas de la organización	**Obt. 168**
Reportes de variaciones y otros comunicados relacionados con el control y monitoreo de variaciones	**Obt. 170**
Reportes muestra de estatus de tentativas de desarrollo de sistemas	**Obt. 172**
Reportes relacionados con adiciones, eliminaciones y cambios a la configuración de los sistemas	**Obt. 174**

Continua ➡

Reportes relacionados con la preguntas de los usuarios, su solución y estadísticas de desempeño de la Mesa de Ayuda	**Obt. 176**
Requerimientos legales y regulativos pertinentes y compromisos contractuales	**Obt. 178**
Tareas y responsabilidades de planeación de la Asamblea General de Socios	**Obt. 180**
Un inventario de la configuración: hardware, software de sistema operativo, software de aplicaciones, instalaciones y archivos de datos dentro y fuera de las instalaciones	**Obt. 182**
Un resumen de las instalaciones y posiciones de manejo de problemas	**Obt. 184**

Continua

Una lista de los acuerdos de desempeño, capacidad y nivel de servicios con respecto a las expectativas de desempeño de los recursos de los sistemas de información (equipo e instalaciones), incluyendo estándares industriales	**Obt. 186**
Una lista de los problemas reportados durante un período representativo, incluyendo la fecha de ocurrencia, la fecha de escalamiento (sí aplica), la fecha de solución y los tiempos de solución	**Obt. 188**

Continua ➡

Seguridad en los reportes de procesamiento de salidas distribuidos **o Seguridad de los datos transmitidos y entre aplicaciones** **o Disposición de documentación sensible de entrada, proceso y salida** **o Procedimientos de control de proveedores como terceras partes con respecto a preparación, entrada, procesamiento y salida**	**Obt. 189**
Una lista de todos los productos actuales del proveedor en lo referente a hardware, software, comunicaciones y periféricos	**Obt. 191**

Con el objeto de garantizar que la administración de la tecnología de información soporte adecuadamente los requerimientos de operación actuales y futuros de la entidad, las instituciones controladas deben contar al menos con lo siguiente:

4.3.1.1 –El apoyo y compromiso formal del directorio u organismo que haga sus veces y la alta gerencia.

Objetivos de control:

O bj.42	Ob j.45	Ob j.51	Ob j.58	Ob j.59	Ob j.61	Ob j.63	Ob j.64	Ob j.65	O bj.74
O bj.134	Ob j.145	Ob j.146	Ob j.148	Ob j.150	Ob j.166	Ob j.169	Ob j.170	Ob j.171	O bj.172
O bj.220	Ob j.222	Ob j.224	Ob j.228	Ob j.234	Ob j.236	Ob j.238	Ob j.248	Ob j.250	

Información recopilada a través de entrevistas con:

- Asamblea General de Socios
- Gerente General
- Jefe de Contabilidad
- Jefe de Sistemas
- Jefe de Talento Humano
- Programador
- Help Desk

Obteniendo:

O bt. 25	Ob t. 26	Ob t. 27	Ob t. 28	Ob t. 30	Ob t. 31	Ob t. 32	Ob t. 38	Ob t. 40	bt. 42
O bt. 64	Ob t. 65	Ob t. 67	Ob t. 72	Ob t. 73	Ob t. 74	Ob t. 75	Ob t. 78	Ob t. 80	bt. 82
O bt. 109	Ob t. 119	Ob t. 120	Ob t. 121	Ob t. 126	Ob t. 135	Ob t. 139	Ob t. 141	Ob t. 143	bt. 144
O bt. 178	Ob t. 183	Ob t. 190							

4.3.1.2 – Un plan funcional de tecnología de información alineado con el plan estratégico institucional; y, un plan operativo que establezca las actividades a ejecutar en el corto plazo (un año), de manera que se asegure el logro de los objetivos institucionales propuestos.

Objetivos de control:

O bj.92	Ob j.96	Ob j.105	Ob j.122	Ob j.133	Ob j.153	Ob j.161	Ob j.165	Ob j.165	O bj.174

Información recopilada a través de entrevistas con:

- Gerente General
- Jefe de Contabilidad
- Jefe de Sistemas
- Programador
- Asamblea general de socios
- Jefe de Talento Humano

Obteniendo:

4.3.1.3 – Tecnología de información acorde a las operaciones del negocio y al volumen de transacciones, monitoreada y proyectada según las necesidades y crecimiento de la institución.

Objetivos de control:

O	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	O
bj.71	j.88	j.89	j.97	j.115	j.120	j.123	j.135	j.136	bj.145

Información recopilada a través de entrevistas con:

- Gerente General
- Jefe de Contabilidad
- Jefe de Sistemas
- Programador
- Help Desk

Obteniendo:

O	Ob	Ob	Ob	Ob	Ob	Ob	Ob
bt. 144	t. 145	t. 155	t. 169	t. 175	t. 177	t. 180	t. 191

4.3.1.4 – Un responsable de la información que se encargue principalmente de definir y autorizar de manera formal los accesos y cambios funcionales a las aplicaciones y monitorear el cumplimiento de los controles establecidos.

Objetivos de control:

O	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	O
bj.26	j.32	j.36	j.40	j.47	j.48	j.51	j.52	j.59	bj.60
O	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	O
bj.86	j.89	j.91	j.92	j.104	j.105	j.106	j.112	j.120	bj.127
O	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	O
bj.186	j.190	j.195	j.197	j.203	j.212	j.216	j.217	j.224	bj.228

Información recopilada a través de entrevistas con:

- Jefe de Sistemas
- Programador
- Gerente General
- Jefe de Contabilidad

Obteniendo:

O	Obt	Obt	O	Obt	Obt	Obt	Obt	Obt	
bt. 80	. 84	. 85	bt. 94	. 109	. 121	. 135	. 137	. 138	bt. 144

4.3.1.5 – Políticas, procesos y procedimientos de tecnología de información definidos bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, debidamente aprobados por el directorio u organismo que haga sus veces, alineados a los objetivos y actividades de la institución.

Objetivos de control:

O	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	O
bj.61	j.66	j.67	j.100	j.101	j.106	j.121	j.129	j.132	bj.142
O	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	
bj.186	j.190	j.210	j.218	j.223	j.224	j.228	j.236	j.248	

Información recopilada a través de entrevistas con:

- Gerente General
- Jefe de Contabilidad
- Jefe de Sistemas
- Programador
- Auditor
- Usuarios seleccionados de los recursos del Departamento de Sistemas

Obteniendo:

Obt. 49	Obt. 50	Obt. 58	Obt. 59	Obt. 60	Obt. 61	Obt. 65	Obt. 66	Obt. 67	Obt. 78
Obt. 139	Obt. 140	Obt. 143	Obt. 146	Obt. 147	Obt. 148	Obt. 152	Obt. 165	Obt. 166	Obt. 167

4.3.1.6 – Difusión y comunicación a todo el personal involucrado de las mencionadas políticas, procesos y procedimientos, de tal forma que se asegure su implementación.

Objetivos de control:

Obj.101	Obj.106	Obj.121	Obj.132	Obj.164	Obj.178	Obj.186	Obj.190	Obj.210	Obj.223

Información recopilada a través de entrevistas con:

- Gerente General
- Jefe de Contabilidad
- Jefe de Sistemas
- Asamblea General de Socios
- Jefe de Talento Humano

Obteniendo:

Obt. 49	Obt. 50	Obt. 58	Obt. 59	Obt. 60	Obt. 61	Obt. 65	Obt. 66	Obt. 67	Obt. 78
Obt. 178	Obt. 183								

4.3.1.7 - Capacitación y entrenamiento técnico al personal del área de tecnología de información y de los usuarios de la misma.

Objetivos de control:

Obj.206

Información recopilada a través de entrevistas con:

- Jefe de Talento Humano
- Jefe de Sistemas
- Help Desk

Obteniendo:

4.3.2 -Con el objeto de garantizar que las operaciones de tecnología de información satisfagan los requerimientos de la entidad, las instituciones controladas deben contar al menos con lo siguiente:

4.3.2.1 - Manuales o reglamentos internos, debidamente aprobados por el directorio u organismo que haga sus veces, que establezcan como mínimo las responsabilidades y procedimientos para la operación, el uso de las instalaciones de procesamiento de información y respuestas a incidentes de tecnología de información.

Objetivos de control:

O	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	O
bj.141	j.147	j.152	j.156	j.184	j.187	j.214	j.227	j.237	bj.244

Información recopilada a través de entrevistas con:

- Jefe de Sistemas
- Programador
- Help Desk
- Usuarios seleccionados de los recursos del Departamento de Sistemas
- Proveedores seleccionados que proporcionan servicios o productos de software por contrato

Obteniendo

O	Ob	Ob	Ob	Obt	Obt	Obt.	Ob
bt. 120	t. 128	t. 176	t. 181	. 184	. 185	188	t. 192

4.3.2.2 - Un procedimiento de clasificación y control de activos de tecnología de información, que considere por lo menos, su registro e identificación, así como los responsables de su uso y mantenimiento, especialmente de los más importantes.

Objetivos de control:

O	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	O
bj.50	j.55	j.67	j.68	j.72	j.75	j.86	j.87	j.93	bj.106
O	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	O
bj.157	j.162	j.164	j.173	j.182	j.183	j.185	j.190	j.193	bj.194
O	Ob	Ob	Ob	Ob	Ob	Ob			
bj.230	j.233	j.236	j.243	j.245	j.248	j.249			

Información recopilada a través de entrevistas con:

- Jefe de Sistemas
- Programador
- Help Desk
- Gerente General
- Jefe de Talento Humano
- Asamblea general de socios
- Usuarios seleccionados de los recursos del Departamento de Sistemas
- Proveedores seleccionados que proporcionan servicios o productos de software por contrato

Obteniendo:

Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob
t. 53	t. 56	t. 71	t. 77	t. 79	t. 78	t. 80	t. 82	t. 83	t. 84
Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob
t. 136	t. 137	t. 142	t. 149	t. 151	t. 152	t. 162	t. 174	t. 182	t. 189

4.3.4 - Con el objeto de garantizar que el sistema de administración de seguridad satisfaga las necesidades de la entidad para salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, las instituciones controladas deben contar al menos con lo siguiente:

4.3.4.1 - Políticas y procedimientos de seguridad de la información que establezcan sus objetivos, importancia, normas, principios, requisitos de cumplimiento, responsabilidades y comunicación de los incidentes relativos a la seguridad; considerando los aspectos legales, así como las consecuencias de violación de estas política.

Objetivos de control:

Obj.128	Obj.181	Obj.197	Obj.217	Obj.231	Obj.239	Obj.250

Información recopilada a través de entrevistas con:

- Jefe de Sistemas
- Programador

Obteniendo:

Obt. 93	Obt. 95	Obt. 109	Obt. 121	Obt. 150	Obt. 154	Obt. 157	Obt. 158	Obt. 159	Obt. 164

4.3.4.2 – La identificación de los requerimientos de seguridad relacionados con la tecnología de información, considerando principalmente: la evaluación de los riesgos que enfrenta la institución; los requisitos legales, normativos,

reglamentarios y contractuales; y, el conjunto específico de principios, objetivos y condiciones para el procesamiento de la información que respalda sus operaciones.

Objetivos de control:

O bj.36	O bj.40	O bj.51	O bj.67	O bj.72	O bj.78	O bj.99	O bj.106	O bj.111	O bj.112
O bj.162	O bj.164	O bj.166	O bj.181	O bj.182	O bj.183	O bj.185	O bj.190	O bj.193	O bj.194
O bj.230	O bj.231	O bj.233	O bj.236	O bj.239	O bj.243	O bj.248	O bj.249	O bj.250	

Información recopilada a través de entrevistas con:

- Gerente General
- Jefe de Contabilidad
- Jefe de Sistemas
- Programador
- Help Desk
- Asamblea general de socios
- Personal seleccionado del Departamento de Sistemas

Obteniendo:

O bt. 48	O bt. 54	O bt. 55	Ob t. 57	Ob t. 68	Ob t. 69	Ob t. 78	Ob t. 80	Ob t. 84	Ob t. 85

Continua

4.3.4.3 – Los controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información administrada.

Objetivos de control:

O bj.70	O bj.72	O bj.85	O bj.117	O bj.118	O bj.119	O bj.120	O bj.124	O bj.125	O bj.126
O bj.198	O bj.203	O bj.208	O bj.212	O bj.221	O bj.225	O bj.226	O bj.230	O bj.233	O bj.243

Información recopilada a través de entrevistas con:

- Jefe de Sistemas
- Programador
- Help Desk

Obteniendo:

4.3.4.4 – Un sistema de administración de las seguridades de acceso a la información que defina las facultades y atributos de los usuarios, desde el registro, eliminación y modificación, pistas de auditoría; además de los controles necesarios que permitan verificar su cumplimiento en todos los ambientes de procesamiento.

Objetivos de control:

Obj.128	Obj.181	Obj.197	Obj.217	Obj.231	Obj.239	Obj.250

Información recopilada a través de entrevistas con:

- Jefe de Sistemas
- Programador
- Help Desk

Obteniendo:

Ob	O	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob
t. 93	bt. 95	t. 109	t. 121	t. 150	t. 154	t. 157	t. 158	t. 159	t. 164

4.3.4.5 – Niveles de autorización de accesos y ejecución de las funciones de procesamiento de las aplicaciones, formalmente establecidos, que garantice una adecuada segregación de funciones y reduzca el riesgo de error o fraude.

Objetivos de control:

O	O	O	O	O	O	O	O	O	O
bj.106	bj.112	bj.127	bj.128	bj.164	bj.181	bj.190	bj.197	bj.217	bj.224

Información recopilada a través de entrevistas con:

- Jefe de Sistemas
- Programador
- Help Desk
- Gerente General
- Jefe de Contabilidad
- Jefe de Talento Humano
- Asamblea General de socios

Obteniendo:

Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob
t. 69	t. 78	t. 80	t. 84	t. 85	t. 93	t. 95	t. 109	t. 121	t. 135

4.3.4.6 – Adecuados sistemas de control y autenticación para evitar accesos no autorizados, inclusive de terceros; y, ataques externos especialmente a la información crítica y a las instalaciones de procesamiento.

Objetivos de control:

O	O	O	O	O	O	O
bj.128	bj.181	bj.197	bj.217	bj.231	bj.239	bj.250

Información recopilada a través de entrevistas con:

- Jefe de Sistemas
- Programador
- Help Desk

Obteniendo:

Ob t. 93	O bt. 95	Ob t. 109	Ob t. 121	Ob t. 150	Ob t. 154	Ob t. 157	Ob t. 158	Ob t. 159	Ob t. 164

4.3.4.7 – Controles adecuados para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, así como instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos y demás software maliciosos.

Objetivos de control:

O bj.51	O bj.112	O bj.127	O bj.128	O bj.181	O bj.197	O bj.213	O bj.217	O bj.231	O bj.239

Información recopilada a través de entrevistas con:

- Jefe de Sistemas
- Programador
- Help Desk
- Personal de soporte de proveedores de software

Obteniendo:

Ob t. 68	Ob t. 69	Ob t. 70	Ob t. 93	Ob t. 95	Ob t. 99	Ob t. 109	Ob t. 114	Ob t. 115	Ob t. 121
Ob t. 182									

4.3.4.8 – Controles formales para proteger la información contenida en documentos; medios de almacenamiento u otros dispositivos externos; el uso e intercambio electrónico de datos contra daño, robo, accesos, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de todo su personal y de sus proveedores.

Objetivos de control:

O bj.36	O bj.40	O bj.42	O bj.51	O bj.53	O bj.67	O bj.68	O bj.72	O bj.74	O bj.86
O bj.126	O bj.127	O bj.128	O bj.130	O bj.134	O bj.135	O bj.136	O bj.140	O bj.151	O bj.157
O bj.197	O bj.198	O bj.200	O bj.208	O bj.209	O bj.211	O bj.217	O bj.220	O bj.221	O bj.224
O bj.248	O bj.249	O bj.250							

Información recopilada a través de entrevistas con:

- Jefe de Sistemas
- Programador
- Help Desk
- Gerente General
- Jefe de Contabilidad
- Jefe de Talento Humano
- Asamblea General de Socios

Obteniendo:

Ob t. 54	Ob t. 55	Ob t. 57	Ob t. 62	Ob t. 68	Ob t. 69	Ob t. 73	Ob t. 74	Ob t. 75	Ob t. 77
Ob t. 119	Ob t. 121	Ob t. 131	Ob t. 135	Ob t. 136	Ob t. 137	Ob t. 142	Ob t. 144	Ob t. 150	Ob t. 151

4.3.4.9 – Instalaciones de procesamiento de información crítica en áreas protegidas con los suficientes controles que eviten el acceso de personal no autorizado y daños a los equipos de computación y a la información en ellos procesada, almacenada o distribuida.

Objetivos de control:

Información recopilada a través de entrevistas con:

- Jefe de Talento Humano
- Guardias de Seguridad

Obteniendo:

4.3.4.10 – Las condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la infraestructura de tecnología de información.

Objetivos de control:

Información recopilada a través de entrevistas con:

- Jefe de Talento Humano
- Guardias de Seguridad

Obteniendo:

4.3.4.11 – Un plan para evaluar el desempeño del sistema de administración de la seguridad de la información, que permita tomar acciones orientada a mejorarlo.

Objetivos de control:

O bj.112	O bj.127	O bj.128	O bj.181	O bj.197	O bj.207	O bj.215	O bj.217	O bj.231	O bj.239

Información recopilada a través de entrevistas con:

- Jefe de Sistemas
- Programador
- Help Desk
- Gerente General
- Auditor
- Usuarios seleccionados de recursos del Departamento de Sistemas

Obteniendo:

Continua

Ob t. 158	Ob t. 159	Ob t. 164	Ob t. 168	Ob t. 171

4.3.4.12 - Las instituciones controladas que ofrezcan los servicios de transferencias y transacciones electrónicas deberán contar con políticas y procedimientos de seguridad de la información que garanticen que las operaciones sólo pueden ser realizadas por personas debidamente autorizadas; que el canal de comunicaciones utilizado sea seguro, mediante técnicas de encriptación de información; que existan mecanismos alternos que garanticen la continuidad del servicio ofrecido; y, que aseguren la existencia de pistas de auditoría.

Objetivos de control:

O bj.151	O bj.154	O bj.157	O bj.175	O bj.177	O bj.200	O bj.209	O bj.211	O bj.220

Información recopilada a través de entrevistas con:

- Jefe de Sistemas
- Programador
- Help Desk
- Gerente General
- Jefe de Contabilidad

Obteniendo:

Continua ➡

Obt. 78	Obt. 80	Obt. 88	Obt. 91	Obt. 93	Obt. 94	Obt. 95	Obt. 96	Obt. 107	Obt. 109
Obt. 171	Obt. 180								

4.3.5 - Con el objeto de garantizar la continuidad de las operaciones, las instituciones controladas deben contar al menos con lo siguiente:

4.3.5.1 – Controles para minimizar riesgos potenciales de sus equipos de computación ante eventos imprevistos, tales como: fallas, daños o insuficiencia de los recursos de tecnología de información; robo; incendio; humo; inundaciones; Polvo; Interrupciones en el fluido eléctrico; desastres naturales; entre otros.

Objetivos de control:

Obj.75	Obj.78	Obj.84	Obj.88	Obj.97	Obj.99	Obj.108	Obj.111	Obj.115	Obj.116
Obj.166	Obj.168	Obj.170	Obj.171	Obj.175	Obj.177	Obj.189	Obj.192	Obj.219	Obj.235

Información recopilada a través de entrevistas con:

- Gerente General
- Jefe de Contabilidad
- Jefe de Sistemas
- Programador

- Personal seleccionado del Departamento de Sistemas
- Guardias de Seguridad
- Usuarios seleccionados de los recursos del Departamento de Sistemas
- Proveedores seleccionados que proporcionan servicios o productos de software por contrato

Obteniendo:

Ob t. 76	Ob t. 78	Ob t. 80	Ob t. 88	Ob t. 91	Ob t. 97	Ob t. 106	Ob t. 112	Ob t. 113	Ob t. 122
Ob t. 167	Ob t. 169	Ob t. 175	Ob t. 177	Ob t. 180	Ob t. 186	Ob t. 187	Ob t. 191	Ob t. 192	

4.3.5.2 – Políticas y procedimientos de respaldo de información periódicos, que aseguren al menos que la información crítica pueda ser recuperada en caso de falla de la tecnología de información o con posterioridad a un evento inesperado.

Objetivos de control:

O bj.119	O bj.124	O bj.125	O bj.126	O bj.130	O bj.134	O bj.140	O bj.162	O bj.182	O bj.183
O bj.221	O bj.225	O bj.226	O bj.230	O bj.233	O bj.243	O bj.249			

Información recopilada a través de entrevistas con:

- Jefe de Sistemas
- Programador
- Help Desk

Obteniendo:

Ob	Ob
t. 142	t. 189

4.3.5.3 – Mantener los sistemas de comunicación y redundancia de los mismos que permitan garantizar la continuidad de sus servicios.

Objetivos de control:

O	O	O	O	O	O	O	O	O	O
bj.74	bj.90	bj.112	bj.127	bj.128	bj.134	bj.140	bj.181	bj.197	bj.200

Información recopilada a través de entrevistas con:

- Jefe de Sistemas
- Programador
- Help Desk

Obteniendo:

Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob
t. 68	t. 69	t. 73	t. 74	t. 75	t. 93	t. 95	t. 96	t. 107	t. 109

4.3.5.4 – Información de respaldo y procedimientos de restauración en una ubicación remota, a una distancia adecuada que garantice su disponibilidad ante eventos de desastre en el centro principal de procesamiento.

Objetivos de control:

Información recopilada a través de entrevistas con:

- Jefe de Sistemas

Obteniendo:

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

4.3.6.1 – Una metodología que permita la adecuada administración y control del proceso de compra de software y del ciclo de vida de desarrollo y mantenimiento de aplicaciones, con la aceptación de los usuarios involucrados.

Objetivos de control:

O	O	O	O	O	O	O	O	O	O
bj.52	bj.54	bj.56	bj.57	bj.59	bj.60	bj.61	bj.63	bj.65	bj.69

Continua

O	O	O	O	O	O	O	O	O
bj.201	bj.202	bj.203	bj.204	bj.212	bj.216	bj.229	bj.232	bj.242

Información recopilada a través de entrevistas con:

- Jefe de Talento Humano
- Jefe de Sistemas
- Programador

Obteniendo:

Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob
t. 132	t. 138	t. 139	t. 143	t. 144	t. 146	t. 147	t. 163	t. 164	t. 167

4.3.6.2 – Documentación técnica y de usuario permanentemente actualizada de las aplicaciones de la institución.

Objetivos de control:

O	O	O
bj.139	bj.144	bj.160

Información recopilada a través de entrevistas con:

- Jefe de Sistemas
- Programador
- Help Desk
- Jefe de Talento Humano
- Usuarios seleccionados de recursos de sistemas de información

Obteniendo:

4.3.6.3 – Controles que permitan asegurar la adecuada administración de versiones de las aplicaciones puestas en producción.

Objetivos de control:

Información recopilada a través de entrevistas con:

- Jefe de Sistemas
- Programador
- Help Desk

Obteniendo:

4.3.6.4 – Controles que permitan asegurar que la calidad de la información sometida a migración, cumple con las características de integridad, disponibilidad y confidencialidad.

Objetivos de control:

Información recopilada a través de entrevistas con:

- Jefe de Sistemas

- Programador
- Help Desk

Obteniendo:

4.3.7 - Las instituciones controladas deberán contar con políticas y procedimientos que permitan la adecuada administración, monitoreo y documentación de las bases de datos, redes de datos, software de base y hardware.

Objetivos de control:

O bj.40	O bj.43	O bj.44	O bj.50	O bj.51	O bj.53	O bj.54	O bj.55	O bj.71	O bj.75
O bj.123	O bj.127	O bj.128	O bj.135	O bj.136	O bj.138	O bj.153	O bj.154	O bj.156	O bj.160
O bj.202	O bj.204	O bj.213	O bj.217	O bj.219	O bj.231	O bj.232	O bj.239	O bj.240	O bj.245

Información recopilada a través de entrevistas con:

- Jefe de Sistemas
- Programador
- Help Desk
- Gerente General
- Jefe de Contabilidad

- Personal de soporte de proveedores de software
- Jefe de Talento Humano
- Usuarios seleccionados de los recursos del Departamento de Sistemas
- Proveedores seleccionados que proporcionan servicios o productos de software por contrato

Obteniendo:

Ob t. 53	Ob t. 54	Ob t. 55	Ob t. 56	Ob t. 57	Ob t. 68	Ob t. 69	Ob t. 70	Ob t. 76	Ob t. 78
Ob t. 106	Ob t. 109	Ob t. 112	Ob t. 114	Ob t. 115	Ob t. 118	Ob t. 121	Ob t. 122	Ob t. 128	Ob t. 130
Ob t. 159	Ob t. 160	Ob t. 161	Ob t. 162	Ob t. 164	Ob t. 169	Ob t. 170	Ob t. 171	Ob t. 172	Ob t. 173

4.3.11.8 - La institución del sistema financiero deberá implementar mecanismos para impedir la copia de los diferentes componentes de su sitio web, verificar constantemente que no sean modificados sus enlaces, suplantados sus certificados digitales, ni modificada indebidamente la resolución de su sistema de nombres de dominio.

Objetivos de control:

Continua ➡

O bj.72	O bj.74	O bj.87	O bj.90	O bj.93	O bj.102	O bj.103	O bj.108	O bj.112	O bj.113
O bj.134	O bj.140	O bj.156	O bj.162	O bj.168	O bj.173	O bj.181	O bj.182	O bj.183	O bj.185
O bj.208	O bj.209	O bj.211	O bj.213	O bj.215	O bj.217	O bj.219	O bj.220	O bj.221	O bj.225

Información recopilada a través de entrevistas con:

- Gerente General
- Jefe de Sistemas
- Auditor
- Guardias de Seguridad
- Programador
- Help Desk
- Personal de soporte de proveedores de software
- Personal seleccionado del Departamento de Sistemas

Obteniendo:

Ob t. 70	O bt. 73	O bt. 74	O bt. 75	O bt. 76	O bt. 82	O bt. 83	O bt. 96	O bt. 99	O bt. 102

Continua ➡

Obt. 182	Obt. 189	Obt. 191

4.3.11.9 - La institución del sistema financiero debe implementar mecanismos de autenticación al inicio de sesión de los clientes, en donde el nombre de usuario debe ser distinto al número de cédula de identidad y éste así como su clave de acceso deben combinar caracteres numéricos y alfanuméricos con una longitud mínima de 6 caracteres**.**

Objetivos de control:

Obj.28	Obj.29	Obj.36	Obj.40	Obj.44	Obj.46	Obj.50	Obj.51	Obj.55	Obj.72
Obj.125	Obj.126	Obj.127	Obj.128	Obj.130	Obj.138	Obj.162	Obj.173	Obj.181	Obj.182
Obj.208	Obj.213	Obj.217	Obj.221	Obj.225	Obj.226	Obj.230	Obj.231	Obj.233	Obj.235

Información recopilada a través de entrevistas con:

- Gerente General
- Jefe de Contabilidad
- Auditor
- Jefe de Sistemas
- Guardias de Seguridad
- Programador

- Proveedores seleccionados que proporcionan servicios o productos de software por contrato
- Help Desk
- Personal seleccionado del Departamento de Sistemas

Obteniendo:

Obt. 83	O bt. 99	O bt. 109	O bt. 112	O bt. 113	O bt. 114	O bt. 115	O bt. 121	O bt. 128	O bt. 129
Obt. 187	O bt. 189	O bt. 192							

4.3.11.10 - Para la ejecución de transacciones de clientes, se deberá implementar mecanismos de autenticación que completen por lo menos dos de tres factores: "algo que se sabe, algo que se tiene, o algo que se es", considerando que uno de ellos debe: ser dinámico por cada vez que se efectúa una operación, ser una clave de una sola vez OTP (one timepassword), tener controles biométricos, entre otros.

Objetivos de control:

Obj.28	O bj.32	O bj.36	O bj.40	O bj.43	O bj.46	O bj.49	O bj.50	O bj.51	O bj.53
Obj.88	O bj.89	O bj.93	O bj.95	O bj.97	O bj.98	O bj.112	O bj.113	O bj.114	O bj.115
Obj.173	O bj.175	O bj.177	O bj.181	O bj.188	O bj.195	O bj.197	O bj.199	O bj.201	O bj.202

Continua

O bj.240	O bj.245	O bj.250

Información recopilada a través de entrevistas con:

- Gerente General
- Jefe de Sistemas
- Jefe de Contabilidad
- Guardias de Seguridad
- Programador
- Help Desk
- Personal seleccionado del Departamento de Sistemas
- Proveedores seleccionados que proporcionan servicios o productos de software por contrato

Obteniendo:

Ob t. 51	O bt. 52	O bt. 56	O bt. 78	O bt. 80	O bt. 79	O bt. 82	O bt. 83	O bt. 86	O bt. 88
Ob t. 121	O bt. 127	O bt. 130	O bt. 132	O bt. 144	O bt. 144	O bt. 145	O bt. 149	O bt. 150	O bt. 162

4.3.11.11 - En todo momento en donde se solicite el ingreso de una clave numérica, los sitios web de las entidades deben exigir el ingreso de éstas a través de teclados virtuales, las mismas que deberán estar enmascaradas.

Objetivos de control:

O	O	O	O	O	O	O	O	O	O
bj.46	bj.50	bj.53	bj.54	bj.59	bj.61	bj.62	bj.63	bj.64	bj.65
O	O	O	O	O	O	O	O	O	O
bj.120	bj.129	bj.135	bj.136	bj.142	bj.145	bj.148	bj.150	bj.152	bj.203
O	O	O	O	O	O	O	O		
bj.204	bj.205	bj.212	bj.213	bj.214	bj.232	bj.240	bj.245		

Información recopilada a través de entrevistas con:

- Gerente General
- Jefe de Sistemas
- Auditor
- Programador
- Guardias de Seguridad
- Help Desk
- Proveedores seleccionados que proporcionan servicios o productos de software por contrato
- Personal seleccionado del Departamento de Sistemas

Obteniendo:

Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob
t. 70	t. 78	t. 78	t. 82	t. 83	t. 89	t. 92	t. 99	t. 104	t. 114
Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	Ob	
t. 149	t. 162	t. 166	t. 167	t. 172	t. 173	t. 174	t. 176	t. 182	

3.10. Análisis y Gestión de Riesgos

Como es de conocimiento general, toda organización se encuentra expuesta a riesgos; debido a que no existe un entorno 100% seguro, ya que la exposición de riesgos es constante. por tal motivo toda organización financiera deberá estar alerta a cualquier cambio o situación extraña y que considera que podría afectar negativamente a un activo o a toda su organización.

Esta etapa se construye en el núcleo central de MAGERIT, y su correcta aplicación condiciona la validez y utilidad de todo el proyecto.

3.10.1.Identificación de Activos

3.10.1.1.[S] Servicios

Para los usuarios internos, la COAC Textil 14 de Marzo presta los siguientes servicios:

1. Telefonea IP
2. Portal WEB
3. Acceso remoto
4. Servidor de correo electrónico
5. Servidor de archivo
6. Internet

Para los usuarios externos, la institución cuenta con los siguiente servicios:

1. Ahorro
2. Crédito
3. Cajero automático

4. Otros pagos:

a. Planillas de teléfono

b. Planillas de luz

c. Pensiones

d. SOAT

e. Sueldos a empleados

3.10.1.2.[SW] Aplicaciones (software)

Entre las aplicaciones que ostenta la institución tenemos los siguientes:

- Sistema financiero
- Ofimática
- Antivirus
- Otros softwares:
  - SQL server

3.10.1.3.[HW] Equipos Informáticos (hardware)

Dentro de los equipos informáticos que posee la institución tenemos los siguientes:

- Servidor de base de datos
- Equipos virtuales
- Routers

- Switches
- Radios
- Firewall
- Computadores de escritorio
- Computadores portátiles
- Impresoras laser
- Impresoras matriciales

3.10.1.4.[COM] Redes de Comunicaciones

Entre los medios de transporte de información tenemos los siguientes:

- Telefonía IP
- Red LAN
- Red WWAN
- Internet

3.10.1.5.[SI] Soportes de Información

En la institución generalmente se utilizan los siguientes soportes de información:

- Dispositivos USB
- Material impreso
- Microfilm

- Discos formato DVD
- Discos formato CD

3.10.1.6.[AUX] Equipamiento Auxiliar

En la institución se cuenta con los siguientes equipos auxiliares:

- Fuentes de alimentación
- Sistema de alimentación ininterrumpida
- Generador eléctrico
- Equipos de climatización
- Cableado de datos
- Robots
- Mobiliario
- Caja fuerte
- Otros equipamientos auxiliares:
    - Biometría
    - Acceso temporizado
    - Detector de incendios
    - Extintor de incendios
    - Cámaras de vigilancia, entre otros.

3.10.1.7.[SS] Servicios Subcontratados

La COAC Textil 14 de Marzo tiene convenios con otras instituciones para satisfacer la demanda ciudadana, entre los servicios subcontratados tiene:

- Ventanilla compartida

3.10.1.8.[L] Instalaciones

Aquí entran los lugares donde se hospedan los sistemas de información y comunicaciones.

La infraestructura donde se localiza los sistemas de información y comunicación se denomina Departamento de Sistemas, ubicado en San Rafael, Av. General Enríquez y la Concordia, esquina.

3.10.1.9.[P] Personal

Dentro del personal de la institución, podemos citar los siguientes:

- Tlgo. Juan Ñacala, Infraestructura y Telecomunicaciones
- Ing. Verónica Suquillo, Administración de Base de Datos
- Ing, Verónica Suquillo, Ingeniería de Software
- Ing. Roberto Espín Programador/Desarrollador
- Tlgo. Juan Ñacala, Soporte a Usuarios, entre otros.

3.10.2.Identificación de Amenazas

En la siguiente tabla se puede observar las diferentes amenazas a las que están expuestos los activos.

Tabla No. 3.4 Identificación de Amenazas

Ahorro	- Corte de suministro eléctrico - Falla de servicio de comunicaciones - Errores del administrador	1	25%
Crédito	- Corte de suministro eléctrico - Falla de servicio de comunicaciones - Errores del usuario		
Cajero automático	- Desastres naturales - Acceso no autorizados - Ataque destructivo - Avería de origen físico o lógico - Corte de suministro eléctrico - Condiciones inadecuadas de temperatura o humedad - Falla de servicio de comunicaciones - Errores del administrador - Suplantación de la identidad del usuario		

Continua ➡

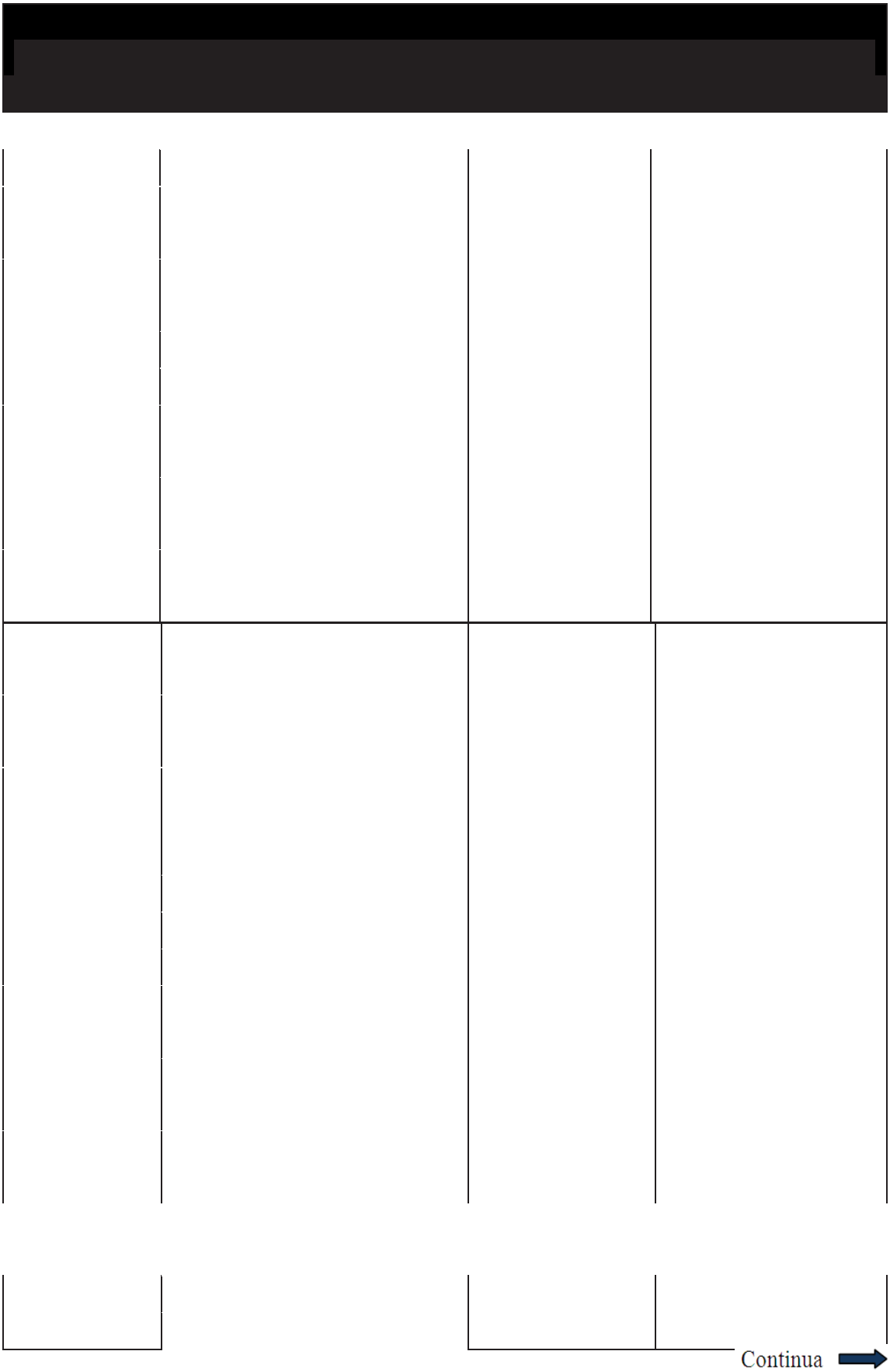
Telefoní a IP	- Desastres naturales - Avería de origen físico o lógico - Falla de servicio de comunicaciones -Degradación de los soportes de almacenamiento de la información - Emanaciones electromagnéticas - Errores de los usuarios - Errores de configuración - Errores de reencaminamiento - Errores de mantenimiento /actualizaciones de programas - Errores de mantenimiento/ actualización de equipos - Manipulación de la configuración - Uso no previsto	2	25%
Portal WEB	- Desastres naturales - Acceso no autorizados - Avería de origen físico o lógico - Corte de suministro eléctrico - Falla de servicio de comunicaciones - Errores del administrador - Suplantación de la identidad del usuario	2	25%
Acceso remoto	- Errores del administrador - Degradación de la información		

Continua

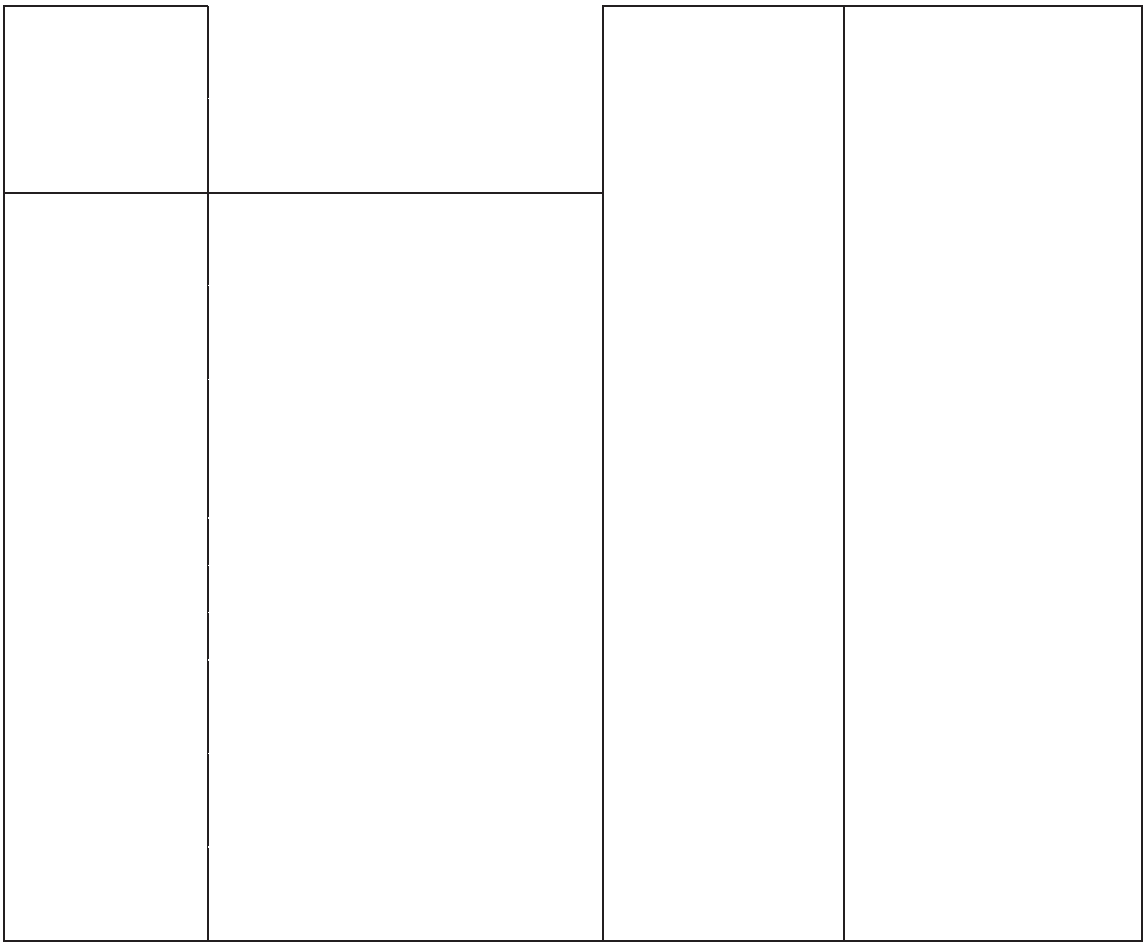
	- Divulgación de la información - Suplantación de la identidad del usuario - Acceso no autorizados - Destrucción de la información - Ataque destructivo		
Acceso remoto	- Errores del administrador - Degradación de la información - Divulgación de la información - Suplantación de la identidad del usuario - Acceso no autorizados - Destrucción de la información - Ataque destructivo		
Servidor de correo electrónico	- Avería de origen físico o lógico - Corte de suministro eléctrico - Falla de servicio de comunicaciones - Errores del administrador - Fugas de información - Errores de mantenimiento /actualizaciones de programas - Suplantación de la identidad del usuario - Denegación de servicio		

Continua ➡

Continua



Continua



Continua ➡

Servidor de base de datos	- Desastres naturales - Avería de origen físico o lógico - Corte de suministro eléctrico - Condiciones inadecuadas de temperatura o humedad - Denegación de servicio - Degradación de los soportes de almacenamiento de la información - Errores de los usuarios - Errores del administrador - Errores de configuración - Abuso de privilegios de acceso - Uso no previsto - Acceso no autorizados - Modificación de información	4	50%
Equipos virtuales	- Fuego - Avería de origen físico o lógico - Corte de suministro eléctrico - Condiciones inadecuadas de temperatura o humedad - Falla de servicio de comunicaciones - Errores del administrador - Errores de configuración - Errores de mantenimiento /actualizaciones de programas - Errores de mantenimiento/		

Continua

	actualización de equipos - Caída del sistema por agotamiento físico de recursos - Indisponibilidad del personal - Manipulación de la configuración - Robo de equipos		
Router	- Daños por agua - Corte de suministro eléctrico - Errores de mantenimiento /actualizaciones de programas - Manipulación de la configuración - Abuso de privilegios de acceso - Acceso no autorizados - Robo de equipos - Ataque destructivo	4	50%
Switch	- Fuego - Daños por agua - Corte de suministro eléctrico - Errores de mantenimiento /actualizaciones de programas - Abuso de privilegios de acceso - Acceso no autorizados - Introducción de falsa información - Robo de equipos		

Continua

	- Ataque destructivo		
Radios	- Fuego - Daños por agua - Avería de origen físico o lógico - Corte de suministro eléctrico - Errores de mantenimiento /actualizaciones de programas - Manipulación de la configuración - Suplantación de la identidad del usuario - Abuso de privilegios de acceso - Acceso no autorizados - Modificación de información - Robo de equipos		
Firewall	- Manipulación de la configuración - Suplantación de la identidad del usuario		

Continua

Computadoras de escritorio	- Fuego - Daños por agua - Corte de suministro eléctrico - Errores de los usuario - Errores del administrador - Errores de configuración - Difusión de software dañino - Errores de mantenimiento /actualizaciones de programas - Perdida de equipos - Manipulación de la configuración - Suplantación de la identidad del usuario	4	50%
Computadoras portátiles	- Fuego - Daños por agua - Corte de suministro eléctrico - Errores de los usuario - Errores del administrador - Errores de configuración - Difusión de software dañino - Errores de mantenimiento /actualizaciones de programas - Perdida de equipos - Manipulación de la configuración - Suplantación de la identidad del usuario		
Impresoras laser	- Daños por agua - Avería de origen fisico o		

Continua

	lógico - Interrupción de otros servicios o suministros esenciales - Errores de los usuarios - Errores de configuración - Manipulación de la configuración - Perdida de equipos		
ACT Impresoras matriciales **IVOS**	- Fuego - Daños por agua - Avería de origen físico o lógico - Interrupción de otros servicios o suministros esenciales - Errores de los usuarios - Errores de configuración - Manipulación de la configuración - Perdida de equipos	4	50%
Equipos de contingencia	- Daños por agua - Condiciones inadecuadas de temperatura o humedad - Errores de los usuarios - Perdida de equipos - Robo de equipos		

Continua

Telefonía IP	- Desastres naturales - Avería de origen físico o lógico - Falla de servicio de comunicaciones - Degradación de los soportes de almacenamiento de la información - Emanaciones electromagnéticas - Errores de los usuarios - Errores de configuración -Errores de reencaminamiento - Errores de mantenimiento /actualizaciones de programas - Errores de mantenimiento/ actualización de equipos - Manipulación de la configuración - Uso no previsto - Interceptación de información (escucha)	4	25%

Continua

Red WWAN	- Daños por agua - Avería de origen físico o lógico - Corte de suministro eléctrico - Condiciones inadecuadas de temperatura o humedad - Falla de servicio de comunicaciones - Emanaciones electromagnéticas - Errores del administrador - Errores de configuración - Vulnerabilidad de los programas (software) - Errores de mantenimiento /actualizaciones de programas - Errores de mantenimiento/ actualización de equipos - Análisis de trafico - Abuso de privilegios de acceso - Uso no previsto - Indisponibilidad del personal	4	25%
Internet	- Daños por agua - Corte de suministro eléctrico - Condiciones inadecuadas de temperatura o humedad - Falla de servicio de comunicaciones - Errores de mantenimiento /actualizaciones de programas		

Continua

	- Caída del sistema por agotamiento físico de recursos - Indisponibilidad del personal - Manipulación de la configuración		

Continua

Robots	- Desastres naturales - Contaminación electromagnética - Corte de suministro eléctrico - Falla de servicio de comunicaciones - Emanaciones electromagnéticas	1	25%

Continua

	- Errores de los usuarios		
Mobiliario	- Desastres naturales - Contaminación electromagnética - Corte de suministro eléctrico - Falla de servicio de comunicaciones - Emanaciones electromagnéticas - Errores de los usuarios		
Caja fuerte	- Desastres naturales - Contaminación electromagnética - Corte de suministro eléctrico - Falla de servicio de comunicaciones - Emanaciones electromagnéticas - Errores de los usuarios		
Otros equipamientos auxiliares	- Desastres naturales - Contaminación electromagnética - Corte de suministro eléctrico - Falla de servicio de comunicaciones - Emanaciones electromagnéticas - Errores de los usuarios		
Ventanilla compartida	- Errores del administrador - Errores de configuración	1/12	25%

Continua

Departamento de Sistemas	- Fuego - Daños por agua - Corte de suministro eléctrico - Condiciones inadecuadas de temperatura o humedad - Deficiencia en la organización	1/12	25%
Administración de base de datos	- Deficiencia en la organización - Divulgación de la información - Extorción - Ingeniería social	N/A	N/A
Infraestructura y telecomunicaciones	- Deficiencia en la organización - Divulgación de la información - Extorción - Ingeniería social		
Desarrolladores/ programadores	- Deficiencia en la organización - Divulgación de la información - Extorción - Ingeniería social		
Ingeniería de software	- Deficiencia en la organización - Divulgación de la información		

Continua

	- Extorción - Ingeniería social		
Soporte a usuario	- Deficiencia en la organización - Divulgación de la información - Extorción - Ingeniería social		

3.10.3. Identificación de Salvaguardas

En la siguiente tabla se observa las diferentes salvaguardas que tienen los activos.

Tabla No. 3.5 Identificación de Salvaguardas

Capa del negocio	Ahorro	Según la COAC Textil 14 de Marzo, fortalece el aseguramiento de depósitos bancarios, sea a través de procesos de resolución bancaria, o reintegrándolos en la mayor proporción técnica posible	- Disponibilidad
	Crédito	- Seguro de vida sobre préstamos, bajo esta póliza pueden asegurarse loa prestamos y/o saldos de préstamos concedidos por la COAC Textil 14 de Marzo a sus asociados o clientes, siendo su principal objetivo proteger a la institución, a los familiares, garantes y/o	- Autenticidad

Continua

		garantías que a su fallecimiento o incapacidad total y permanente, el saldo insoluto de la deuda quedara cancelado en su totalidad.	
	Cajero automático	- Protección del equipo dentro de la organización: monitoreo, respaldos periódicos, aire acondicionado, UPS, cámara de seguridad, antivirus, actualizaciones (parches), mantenimiento. - Acceso limitado	- Trazabilidad
Servicios internos	Telefonía IP	- Protección del equipo dentro de la organización.	- Disponibilidad

Continua

	Portal WEB	- Protección del equipo dentro de la organización.	
	Acceso remoto	- Protección del equipo dentro de la organización. - Activación/desactivación cuando sea necesario.	- Confidencialidad
	Servidor de correo	- Protección del equipo dentro de la organización.	- Autenticidad
	Servidor de archivo	- Protección del equipo dentro de la organización.	

Continua

	Internet	- Protección del equipo dentro de la organización.	- Trazabilidad
Aplicaciones	Sistemas financiero	- Protección del equipo dentro de la organización. - Stand By	- Disponibilidad - Integridad - Autenticidad - Trazabilidad
	Ofimática	- Protección del equipo dentro de la organización.	
	Antivirus	- Protección del equipo dentro de la organización.	
	Otros software	- Protección del equipo dentro de la organización.	
Equipos	Servidor de base de datos	- Stand By - RMAN (Backup de base de datos)	- Disponibilidad - Confidencialidad
	Equipos virtuales	- Protección del equipo dentro de la organización.	
	Router	- Claves - Interruptor de reseteo - Protección del equipo dentro de la organización.	
	Switch	- Claves - Protección del equipo dentro de la organización.	
	Radios	- Acceso remoto - Protección del equipo dentro de la organización.	
	Firewall	- Protección del equipo dentro de la organización.	

Continua

	Computadoras de escritorio	- Protección del equipo dentro de la organización.	
	Computadoras portátiles	- Protección del equipo dentro de la organización.	
	Impresora laser	- Protección del equipo dentro de la organización.	
	Impresora matricial	- Protección del equipo dentro de la organización.	
	Equipos de contingencia	- Protección del equipo dentro de la organización.	- Autenticidad
Comunicaciones	Telefonía IP	- Protección del equipo dentro de la organización.	- Disponibilidad
	Ren LAN	- Protección del equipo dentro de la organización.	

Continua

	Red WWAN	- Protección del equipo dentro de la organización. - Subnetting - Seguridad del equipo - Filtrado de redes - Paquetes y puertos	- Confidencialidad
	Internet	- Filtrado de contenido - Firewall - SSL para https	
Elementos auxiliares	Fuentes de alimentación	- Recarga de batería	- Disponibilidad
	Sistema de alimentación ininterrumpida	- Seguridad lógica y física - Seguros con proveedores - Monitoreo y gestión	

Continua

		electrónica y física	
	Generador eléctrico	- Protección del equipo dentro de la organización, - Transferencia automática	
	Equipo de climatización	- Protección del equipo dentro de la organización,	
	Cableado de datos	- Seguridad lógica y física - Monitoreo y gestión electrónica y física	
	Robots	- Seguridad lógica y física - Seguros con proveedores - Monitoreo y gestión electrónica y física	
	Mobiliario	- Seguridad lógica y física - Monitoreo y gestión electrónica y física	- Autenticidad
	Caja fuerte	- Seguridad lógica y física - Seguros con proveedores	

Continua

		- Monitoreo y gestión electrónica y física	
	Otros equipamientos auxiliares	- Seguridad lógica y física - Seguros con proveedores - Monitoreo y gestión electrónica y física	
Servicios subcontratados	Ventanilla compartida	- Respaldos de los servidores - Logs	- Disponibilidad - Autenticidad
Instalaciones	Departamento de Sistemas	- Alarmas - Ventilación (Aire acondicionado) - UPS - Protecciones metálicas - Extintores	- Disponibilidad
Personal	Administración de base de datos	- Plan de contingencia	- Integridad - Confidencialidad - Autenticidad
	Infraestructura y telecomunicaciones	- Plan de contingencia	
	Desarrolladores/ programadores	- Plan de contingencia	
	Ingeniería de software	- Plan de contingencia	
	Soporte a usuarios	- Plan de contingencia	

3.10.4. Identificación de Vulnerabilidades

Las vulnerabilidades identificadas por medio de las encuestas, (Ver Anexo 2 Vulnerabilidad de los Dominios), que podrían generar que una amenaza se materialice son las siguientes:

- **Identificación del atacante - quienes son los atacantes a los activos**

Tabla No. 3.6 Identificación de los Atacantes

Competidor comercial
Personal interno

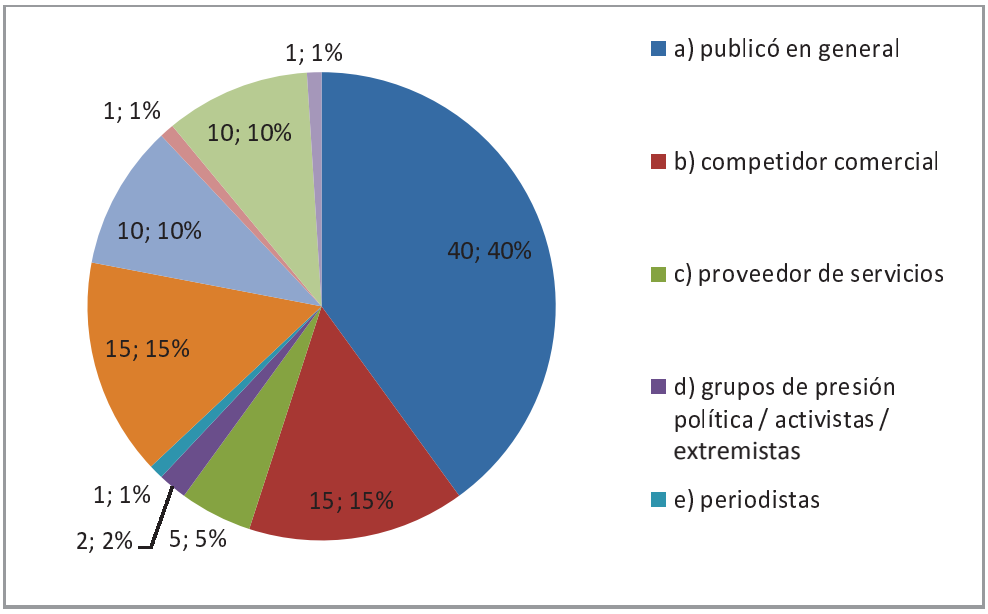


Figura No. 3.5 Resultados de la Identificación de los Atacantes

- **Motivación del atacante**

Tabla No. 3.7 Motivación del Atacante

Beneficios comerciales

Continua ➡

Personal interno

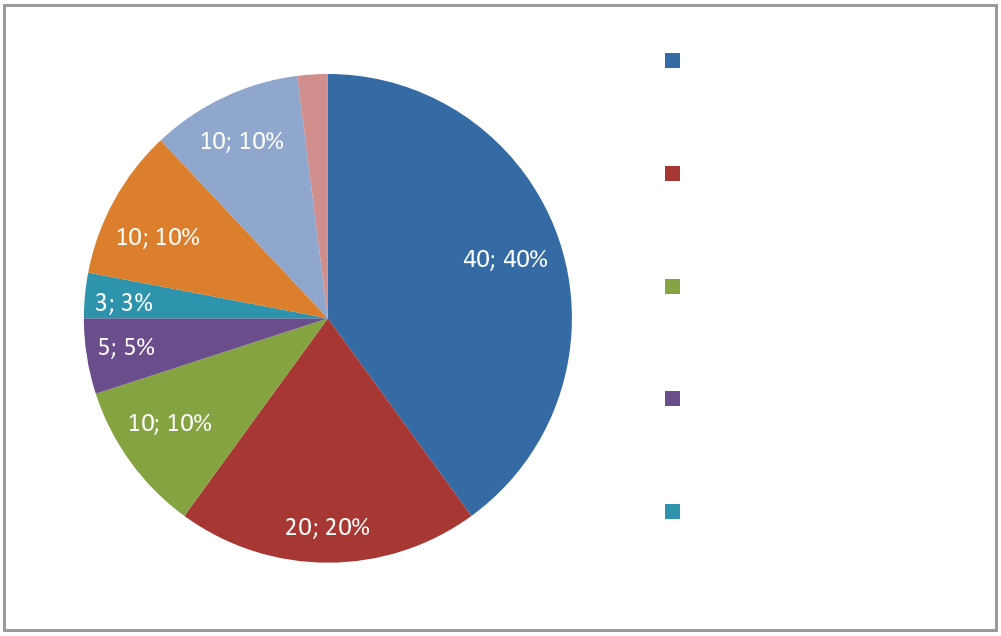


Figura No. 3.6 Resultados de la Motivación del Atacante

- **Motivación del personal interno**

Tabla No. 3.8Motivación del Personal Interno

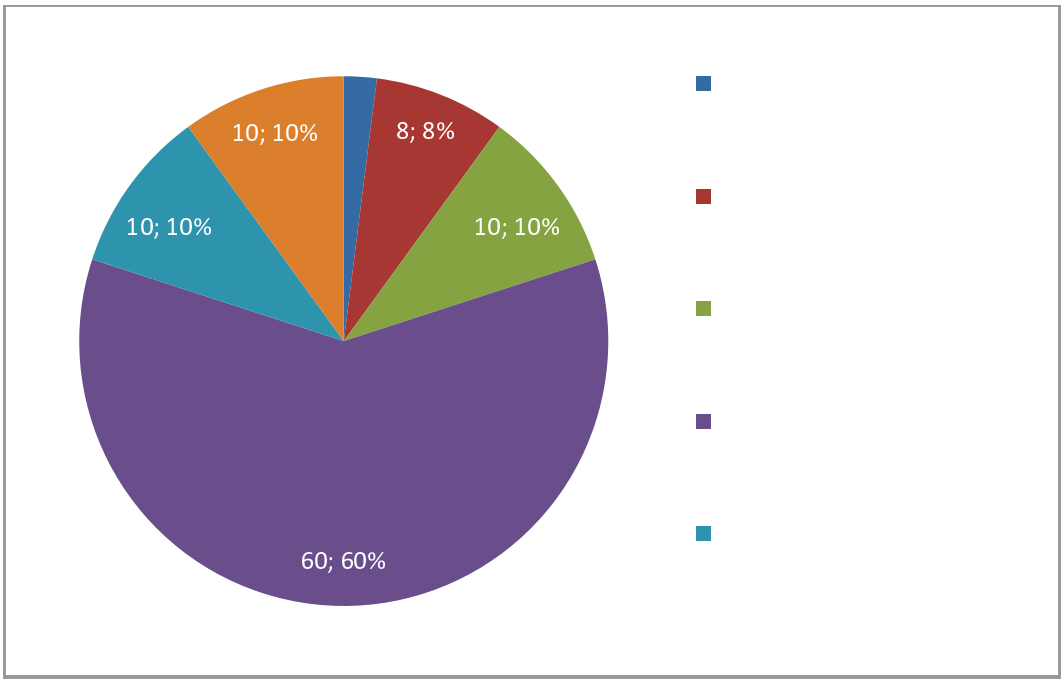


Figura No.3.7 Resultados de la Motivación del Personal Interno

- **Permisos de los usuarios (Derechos)**

Tabla No. 3.9 Permisos de los usuarios (Derechos)

Se permite la instalación de programas sin autorización (Parches y actualizaciones del SO)

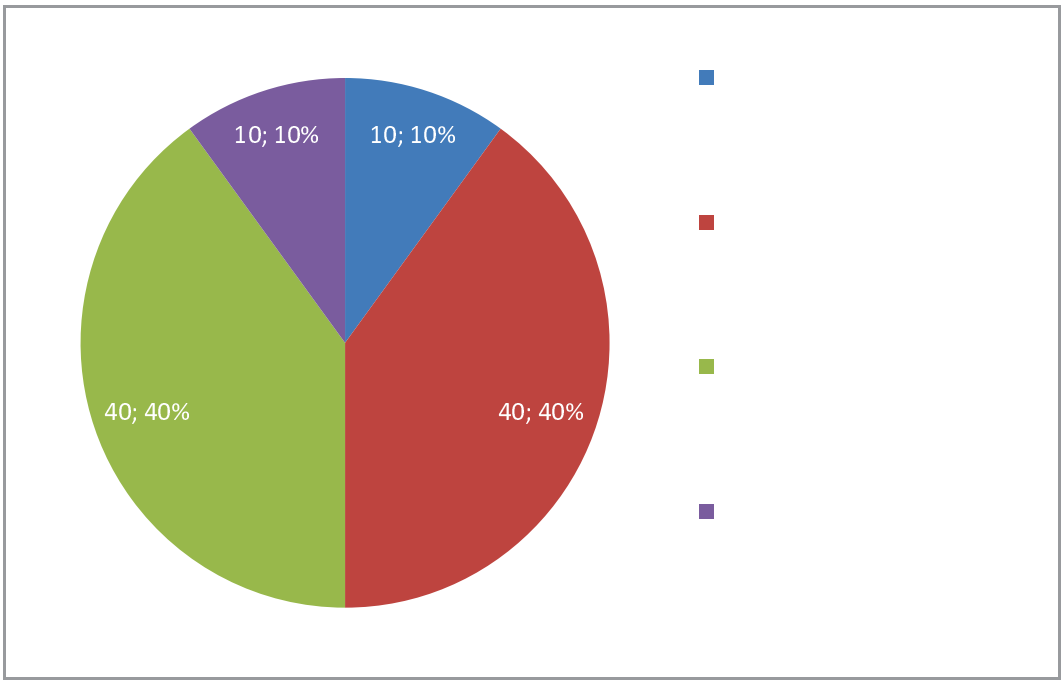


Figura No. 3.8 Resultados de la Motivación Permisos de los usuarios (Derechos)

- **Conectividad del Sistema Financiero**

Tabla No. 3.10 Conectividad del Sistema Financiero

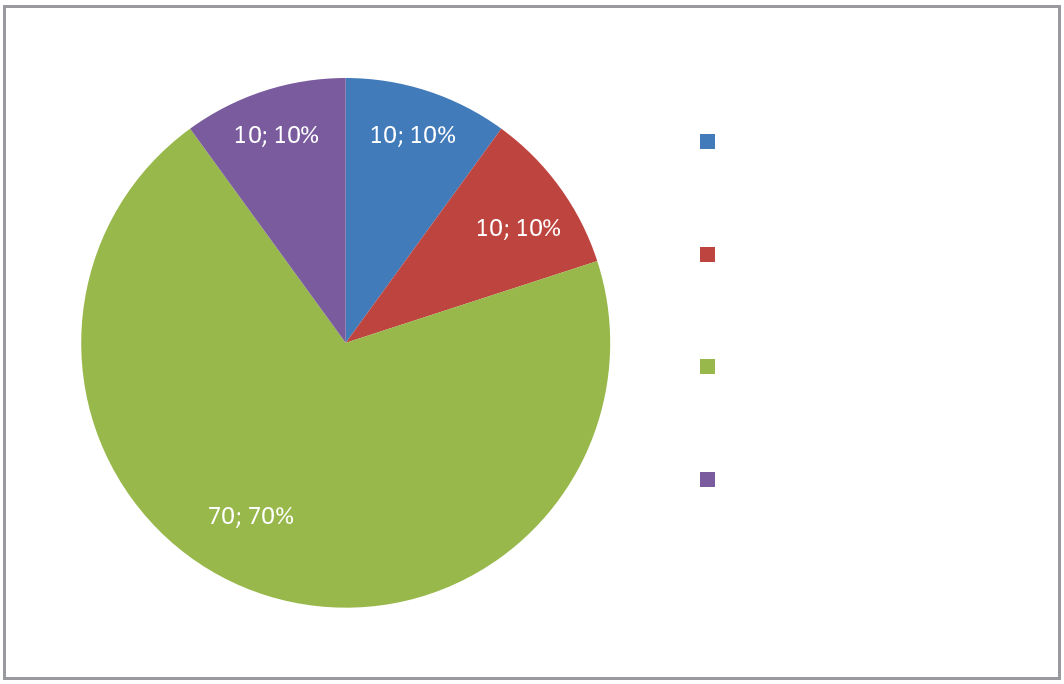


Figura No. 3.9 Resultados de la Motivación Conectividad del Sistema Financiero

- **Ubicación del Sistema Financiero**

Tabla No. 3.11 Ubicación del Sistema Financiero

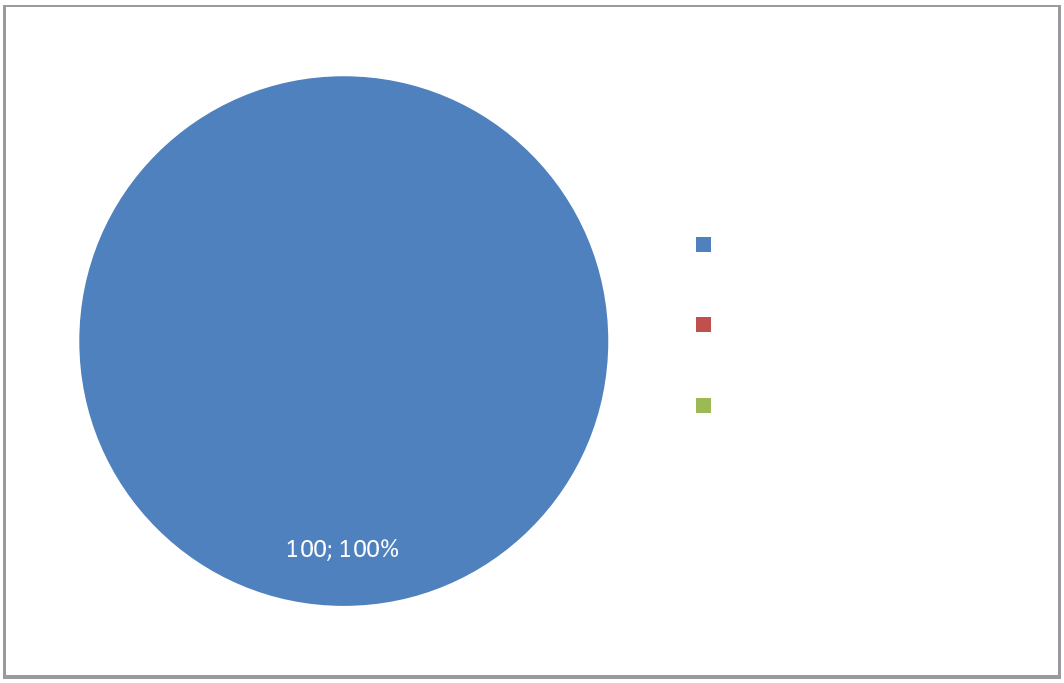


Figura No. 3.10 Resultados de la Ubicación del Sistema Financiero

3.10.5. Identificación de Impactos

A continuación se indican las cinco dimensiones con sus criterios de valoración, obtenidas de las encuestas realizadas. (Ver Anexo 3. Valoración de Dominios).

Disponibilidad

Es el aseguramiento de lo que los usuarios autorizados tienen acceso cuando lo quiera a la información y a sus activos asociados.

Indica la repercusión que tendría en la institución el hecho de que se dejara de prestar el servicio.

Tabla No. 3.12 Disponibilidad y sus Criterios de Valoración

Probablemente cause una interrupción seria de las actividades propias de la organización con un impacto significativo en otras organizaciones.
Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general.
Obligaciones legales: Probablemente cause un incumplimiento grave de una ley o regulación.
Seguridad: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.

Integridad

Es la garantía de la exactitud y completitud de la información y los métodos de su procesamiento.

Indica la repercusión que tendría en la institución el hecho de que la información que se maneja para prestar el servicio fuera incorrecta o incompleta.

Tabla No. 3.13 Integridad y sus Criterios de Valoración

Administración y gestión: Probablemente impediría la operación efectiva de la organización.
Obligaciones legales: Probablemente cause un incumplimiento grave de una ley o regulación.

Confidencialidad

Es el aseguramiento de que la información es accesible sólo para aquellos autorizados de tener acceso.

Indica la repercusión que tendría en la institución el hecho de que la información que se maneja para prestar el servicio fuera accedida por personas no autorizadas.

Tabla No. 3.14 Confidencialidad y sus Criterios de Valoración

Intereses comerciales o económicos: De cierto interés para la competencia, de cierto valor comercial.

Autenticidad

Es el aseguramiento de la identidad u origen.

Indica la repercusión que tendría en la institución el hecho de que no se pudiera confirmar la identidad de quien accedió al servicio o a la información.

Tabla No. 3.15 Autenticidad y sus Criterios de Valoración

Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones, con el público en general.
Obligaciones legales: Probablemente cause un incumplimiento grave de una ley o regulación.
Información personal: Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.

Trazabilidad

Es el aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento.

Indica la repercusión que tendría en la institución el hecho de que no se pudiera conocer a quién se le presta un servicio o a que información y cuando accedió un usuario.

Tabla No. 3.16 Trazabilidad y sus Criterios de Valoración

Intereses comerciales o económicos: Causas de graves pérdidas financieras o mermas de ingresos, facilita ventajas desproporcionadas a individuos u organizaciones, constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros.
Dificulte la investigación o facilite la comisión de delitos.

3.10.6.Identificación del Riesgo

En el siguiente cuadro se puede observar los activos y su nivel de riesgo y su valoración.

Tabla No. 3.17 Nivel de Riesgo

	Bajo 1.9]	Medio [2 -]	Alto [3 -]	Muy 4.9]	Crítico [5 -]

Tabla No. 3.18 Activos, Nivel de Riesgo y su Valoración

	D	I	C	A	T
Capa del negocio					
Ahorro	3.2	2.8	1.0	3.4	

Continua

Crédito	3.2	2.8	1.0	3.4	
Cajero automático	3.2	2.8	1.0	3.4	
Servicios internos					
Telefonía IP	3.1	2.7		3.3	
Portal WEB	3.3	2.9	1.1	3.5	
Acceso remoto	3.2	2.8	1.0	3.4	
Servidor de correo	3.1	2.7		3.3	
Servidor de archivo	3.2	2.8	1.0	3.4	
Internet	1.9	2.4		2.6	
Equipamiento: aplicaciones					
Sistema Financiero	3.3	2.3	1.0	2.8	
Ofimática	1.9	2.4		2.6	
Antivirus	3.2	2.5	1.0	2.7	1.0
Otros softwares	3.2	2.5	1.0	2.7	1.0
Equipos					
Servidor se base de datos		1.7		1.8	
Equipos virtuales	2.2			1.0	
Router	2.9			1.2	
Switch	2.9			1.2	
Radios	2.9			1.2	
Firewall	2.9			1.2	
Computadoras de escritorio				1.2	
Computadoras portátiles				1.2	
Impresora laser	2.3			1.3	
Impresora matricial	3.0			1.3	

Continua ➡

Equipos de contingencia				1.2	
Comunicaciones					
Telefonía IP	3.2			2.2	
Red LAN	3.0			1.9	
Red WWAN	3.0			1.9	
Internet	1.9			2.0	
Elementos auxiliares					
Fuentes de alimentación					
Sistema de alimentación ininterrumpida	1.1				
Generador eléctrico	1.1				
Equipo de climatización	1.1				
Cableado de datos	3.8				
Robots	2.9				
Mobiliario	2.9				
Caja fuerte	2.9				
Otros equipamientos auxiliares	2.9				
Servicios subcontratados					
Ventanilla compartida	3.2	2.8	1.0	3.4	
Instalaciones					
Departamento de sistemas	2.6	1.9		2.0	

Continua

Personal					
Administración de base de datos	1.5	2.0		2.0	
Infraestructura y telecomunicaciones	1.5	2.0		2.0	
Desarrolladores/ programadores	1.5	2.0		2.0	
Ingeniería de software					
Soporte a usuarios					

3.10.7.Toma de Decisiones

3.10.7.1.Identificación de Riesgo Críticos

A continuación se indica lo anteriormente dicho:

Tabla No. 3.19 Nivel de Riesgo

	Bajo 1.9]	Medio [2 -]	Alto [3 -]	Muy 4.9]	Crítico [5 -]

Tabla No. 3.20 Riesgos Críticos

	D	I	C	A	T
Capa del negocio					
Cajero automático	3.2	2.8	1.0	3.4	
Servicios internos					
Portal WEB	3.3	2.9	1.1	3.5	
Equipamiento: aplicaciones					
Sistema Financiero	3.3	2.3	1.0	2.8	
Equipos					
Servidor se base de datos	2.9	1.7		1.8	
Comunicaciones					
Telefonía IP	3.2			2.2	
Red WWAN	3.0			1.9	
Elementos auxiliares					
Cableado de datos	3.8				
Servicios subcontratados					
Ventanilla compartida	3.2	2.8	1.0	3.4	
Instalaciones					
Departamento de sistemas	2.6	1.9		2.0	
Personal					
Administración de base de datos	1.5	2.0		2.0	
Infraestructura y telecomunicaciones	1.5	2.0		2.0	

Continua

Desarrolladores/ programadores	1.5	2.0		2.0	

3.10.7.2. Mitigación de los Riesgos Críticos

Es una tarea que tiene como objetivo principal elaborar un conjunto de programas de seguridad, fundamentados en las valoraciones de los riesgos, para implementar una serie de salvaguardas que mitiguen el impacto y/o riesgo a un nivel residual mínimo.

Los programas de seguridad tratan de implantar o mejorar la implantación de una serie de salvaguardas que lleven impacto y riesgo a niveles residuales asumidos por la Dirección. Los niveles residuales se mencionan luego de la gestión de los activos con riesgos críticos.

A continuación se gestionan los activos con riesgos críticos.

Capa del Negocio

Cajero automático._ Para este activo, una vez conocidas sus amenazas y salvaguardas existentes causantes del riesgo, se ha obtenido:

Un nivel de riesgo Alto (3.2) en cuanto a disponibilidad, teniendo la amenaza con mayor nivel de riesgo el acceso no autorizado; si esta llegase a materializarse el atacante podría acceder a los recursos del sistema burlando los sistemas de identificación y autorización.

La consecuencia de la amenaza en el cajero automático en cuanto a disponibilidad generaría que el servicio quede indispuesto, provocando que la imagen de la cooperativa sea mal vista por usuarios insatisfechos con un servicio que no se puede acceder a él.

Un nivel de riesgo Alto (3.4) en cuanto a autenticidad, teniendo la amenaza con mayor nivel de riesgo la suplantación de la identidad del usuario, pudiendo ser personal interno, personal ajeno a la Cooperativa o por personal contratado

temporalmente, si esta amenaza llegase a materializarse el atacante disfrutaría de los privilegios del usuario suplantado para sus fines propios.

La medida para reducir el riesgo actual de este activo,. es la siguiente:

- Mejorar la protección del equipo dentro de la organización, en lo que se refiere a la seguridad lógica, con una protección de acceso controlado donde se limite los intentos fallidos de acceso.

Servicios Internos

Portal web._ Para este activo. una vez conocidas sus amenazas y salvaguardas existentes causantes del riesgo, se ha obtenido:

Un nivel de riesgo Alto (3.3) en cuanto a disponibilidad, teniendo la amenaza con mayor nivel de riesgo el acceso no autorizado, si esta llegase a materializarse el atacante podría acceder a los recursos del sistema burlando los sistemas de identificación y autorización.

La consecuencia de la amenaza del servicio portal web en cuanto a disponibilidad generaría que el servicio quede inhabilitado. impidiendo quo los socios puedan realizar servicios en línea y obtener Información adicional.

Un nivel de riesgo Alto (3.5) en cuanto a autenticidad, teniendo la amenaza con mayor nivel de riesgo la suplantación de la identidad del usuario, pudiendo ser personal interno como externo a la cooperativa.

La consecuencia de la amenaza en cuanto a autenticidad provocaría que el atacante disfrute de los privilegios del usuario suplantado para sus fines propios.

Las medidas para reducir el riesgo actual de este activo, son las siguientes:

- Implementar medidas de control de acceso para aumentar la seguridad de los servicios en línea como: protección de acceso controlado donde se limite los intentos fallidos de acceso e implementación de tarjetas de coordenadas.

Equipamiento

Aplicaciones

Sistema Financiero._ Para este activo, una vez conocidas sus amenazas y salvaguardas existentes causantes del riesgo, se ha obtenido:

Un nivel de riesgo Alto (3.3) en cuanto a disponibilidad, teniendo las amenazas con mayor nivel de riesgo el acceso no autorizado, difusión de software dañino, errores de configuración y errores de los usuarios. Si estas llegasen a materializarse: el atacante podría acceder a los recursos del sistema burlando los sistemas de identificación y autorización, propagar virus, espías, gusanos, troyanos, bombas 1ogicas, etc.; en errores no intencionados el introducir datos de configuraci6n errónea provocaría la perdida de privilegios de acceso, fallo en el flujo de actividad, etc.; y los errores comunes de los usuarios (personal) al usar los servicios, datos, etc.; provocaría fallos de la información.

Las consecuencias de las amenazas en la disponibilidad generaría la perdida de la exactitud y completitud de la información ocasionando que la aplicación genere resultados erróneos.

Las medidas para reduce el riesgo actual de este activo, son las siguientes:

- Mejorar las medidas de control de acceso para aumentar la segundad de la información. como el control mediante firewall.

- Mejorar la protección de la aplicación: monitorear la proteca6n del código dañino.

- Implementar un registro de errores no intencionales.

Equipos

Servidor de base de datos._ Para este activo, una vez conocidas sus amenazas y salvaguardas existentes causantes del riesgo, se ha obtenido:

Un nivel de riesgo Medio (2.9) en cuanto a disponibilidad, teniendo las amenazas con mayor nivel de riesgo la condición inadecuada de temperatura o humedad y denegación del servicio, si la primera amenaza llegase a materializarse el servidor de base de datos trasladaría la información demasiado tarde a quien lo requiera, debido a la deficiencia de adaptación del local donde se encuentra, por exceso de calor, frio o humedad. La amenaza denegación de servicio provoca que el sistema caiga debido a una carencia de recursos suficientes.

Las consecuencias de las amenazas en la disponibilidad del servidor de base de datos provocarían que la información generada en los departamentos no ingrese ni salga de la base de datos de manera oportuna.

Las medidas para reducir el riesgo actual de este activo, son las siguientes.

- Implementar el Estándar TIA-942 (Telecomunications Industry Association) para Data Center, encaminado una atención al control periódico de los niveles de temperatura y control físico.

Comunicaciones

Telefonía IP._ Para este activo, una vez conocidas sus amenazas y salvaguardas existentes causantes del riesgo, se ha obtenido:

Un nivel de riesgo Alto (3.2) en cuanto a disponibilidad, teniendo las amenazas con mayor nivel de riesgo los errores de configuración, los errores de re-encaminarniento e interceptación de información (escucha); si existe un error en la configuración las comunicaciones podrían llegar a tener un error de re-encaminamiento provocando que la información no llegue a donde lo requiera o simplemente la comunicación no se realiza. Si la tercera amenaza llegase a materializarse el atacante. al interceptar la información emitida por la telefonía IP, podría utilizar toda esa información para sus fines propios.

Las consecuencias de las amenazas en la disponibilidad generarían que la comunicación IP falle y por ende no esté disponible el servicio.

Las medidas para reducir el riesgo actual de este activo, son las siguientes.

- Protección del equipo dentro de la organización, mejorar el control centralizado con revisiones periódicas de la configuración.

- Implementar una prohibición de establecimiento de conversaciones confidenciales en lugares públicos o sin adecuadas medidas de protección.

- Prohibición de dejar mensajes confidenciales en contestadoras automáticas.

Comunicaciones

Red WWAN ._ Para este activo. una vez conocidas sus amenazas y salvaguardas existentes causantes del riesgo, se ha obtenido.

Un nivel de riesgo Alto (3.0) en cuanto a disponibilidad, teniendo las amenazas con mayor nivel de riesgo los fallos de servicios de comunicaciones, errores del administrador y análisis de tráfico; si la primera amenaza llegase a materializarse generaría que se pierda la capacidad de trasmitir datos de un sitio a otro debido a la destrucción física de los medios físicos de transporte. Si la segunda amenaza se llegase a materializar a causa de unas equivocaciones de personas con responsabilidades de instalación y operación, la red WWAN no llegaría a los usuarios, impidiendo que puedan realizar sus labores oportunamente. Y si la tercera amenaza se materializa, el atacante sin necesidad de analizar el contenido de las comunicaciones es capaz de extraer conclusiones solamente conociendo el origen, destino, volumen y frecuencia de los intercambios.

Las consecuencias de las amenazas en la disponibilidad generarían que la red WWAN pierda la capacidad de trasmitir datos de un sitio a otro generando dificultad en la realización de trabajos.

Las medidas para reducir el riesgo actual de este activo, son las siguientes:

- Implementar un control de los medios físicos de transporte de comunicaciones.

- Protección del equipo dentro de la organización: mejorar las pruebas de operaciones.

- Mejorar la seguridad del filtrado de redes.

Elementos auxiliares

Cableado de Datos._ Para este activo, una vez conocidas sus amenazas y salvaguardas existentes causantes del riesgo, se ha obtenido:

Un nivel de riesgo Alto (3.8) en cuanto a disponibilidad, teniendo las amenazas con mayor nivel de riesgo la contaminación mecánica, contaminación electromagnética, condiciones inadecuadas de temperatura o humedad y deficiencias en la organización; si las amenazas se materializan debido a una deficiente instalación del cableado por parte de la organización, provocarían que el cableado y equipos interrelacionados sufran emanaciones electromagnéticas y daños físicos por el polvo, suciedad, cables expuestos a daños no intencionados por el personal.

Las consecuencias de las amenazas en la disponibilidad impedirían que, con un daño en el cableado, las conexiones entre redes dejen de funcionar y también podrían generar daños físicos a los equipos, generando dificultades para realizar los trabajos y poder enviar información.

Las medidas para reducir el riesgo actual de este activo, son las siguientes.

- Implementar planes actualizados del cableado

- Implementar procedimientos para la modificación del cableado

- Implementar la segregación de cableado de alimentación y de comunicación para evitar interferencias

- Implementar un control de todos los accesos al cableado

- Mejorar el monitoreo y gestión electrónica y fisca

Servicios subcontratados

Ventanilla compartida._ Para este servicio que presta la Cooperativa, una vez conocidas sus amenazas y salvaguardas existentes causantes del riesgo, se ha obtenido:

Un nivel de riesgo Alto (3.2) en cuanto a disponibilidad, teniendo las amenazas con mayor nivel de riesgo la caída del sistema por agotamiento de recursos y el acceso no autorizado. Si la primera amenaza llegase a materializarse provocarían que los socios no puedan realizar retiros en las ventanillas de la institución y si la segunda amenaza se materializa el atacante accedería al sistema burlando su autenticidad haciendo que el sistema funcione con fallas o simplemente no funcione.

Las consecuencias de las amenazas en la disponibilidad impedirían quo los socios dispongan del servicio de ventanilla compartida.

Un nivel de riesgo Alto (3.4) en cuanto a autenticidad, teniendo la amenaza con mayor nivel de riesgo la suplantación de la identidad del usuario. Si la amenaza llegase a materializarse, la consecuencia en la dimensión, provocaría quo el atacante disfrute de los privilegios para sus fines propios o para terceros.

Las medidas para reducir el riesgo actual de este servicio, son las siguientes:

- Implementar controles de monitorización y verificación del rendimiento.

- Implementar acuerdos para informar, notificar, investigar las incidencias y fallos de segundad.

Instalaciones

Departamento de Sistemas._ Para este activo, una vez conocidas sus amenazas y salvaguardas existentes causantes del riesgo, se ha obtenido:

Un nivel de riesgo Medio (2.6) en cuanto a disponibilidad, teniendo las amenazas con mayor nivel de riesgo el fuego, daños por agua y deficiencias en la

organización. Si las amenazas llegasen a materializarse el nivel de impacto sería alto, causando daños físicos y económicos.

Las consecuencias de las amenazas en la disponibilidad impedirían quo el personal disponga de las instalaciones para poder ejercer sus actividades, debido a los daños en sus activos.

Un nivel de riesgo Medio (2.0) en cuanto a autenticidad, teniendo la amenaza con mayor nivel el acceso no autorizado. Si la amenaza llegase a materializarse el atacante puede ser el causante de producir daños irreversibles.

La consecuencia de la amenaza en la autenticidad provocaría quo el atacante desconocido origine daños físicos y económicos.

Las medidas para reducir el riesgo actual de este activo, son las siguientes:

- Supervisar la normas de conducta (prohibición de fumar. beber. comer, etc.)
- Implementar un plan de protección frente a desastres
- Implementar una separación de aéreas de segundad y de acceso público
- implementar un control de las aéreas de carga y descarga
- Implementar un control de acceso mecanismo de huella dactilar
- Mejorar el control de visitas
- Implementar una protección de conductos y aberturas
- Implementar las medidas de seguridad de los sistemas de información

Personal

Personal. Los riesgos que abarcan: la administración de base de datos, infraestructura y telecomunicaciones, desarrolladores/programadores, ingeniería de

software y soporte a usuarios, son los siguientes: deficiencia de la organización, divulgación de información, extorción e ingeniería social.

Si la primera amenaza se materializa existiría información desorganizada e interpretaciones erróneas, cuando no estén claras las responsabilidades de quien tiene que hacer exactamente qué y cuándo. Si las demás amenazas llegan a materializarse, la información sustraída puede ser utilizada como extorción o como abuso de la buena fe para beneficios propios del atacante.

Las consecuencias de las amenazas causarían: cambios de conducta en el personal, inasistencia al trabajo, preocupaciones sin poder cumplir sus responsabilidades e inseguridad en el manejo de la información.

Las medidas para reducir el riesgo actual de este activo, son las siguientes:

- Implementar una política de gestión de personal (en materia de segundad)
- Mejorar la asignación de responsabilidades
- Implementar procedimientos para el cambio de puesto de trabajo
- Implementar comprobaciones de puestos de gran responsabilidad
- Implementar una normativa de desempeño del puesto-propiedad intelectual

Con la aplicación de las salvaguardas el nivel de riesgo actual disminuiría a un nivel de riesgo objetivo, como se indica en la siguiente tabla:

Tabla No. 3.21 Nivel de Riesgo

	Bajo 1.9]	Medio [2 -]	Alto [3 -]	Muy 4.9]	Crítico [5 -]

Tabla No. 3.22Riesgo Objetivo

	D	I	C	A	T
Capa del negocio					
Cajero automático	0.0	0.0	0.0	0.0	0.0
Servicios internos					
Portal WEB	0.0	0.0	0.0	0.0	0.0
Equipamiento: aplicaciones					
Sistema Financiero	0.0	0.0	0.0	0.0	0.0
Equipos					
Servidor se base de datos	0.8	0.0	0.0	0.0	0.0
Comunicaciones					
Telefonía IP	0.5	0.0	0.0	0.0	0.0
Red WWAN	0.6	0.0	0.0	0.0	0.0
Elementos auxiliares					
Cableado de datos	2.0	0.0	0.0	0.0	0.0
Servicios subcontratados					
Ventanilla compartida	0.0	0.0	0.0	0.0	0.0
Instalaciones					
Departamento de sistemas	0.0	0.0	0.0	0.0	0.0
Personal					
Administración de base de datos	0.0	0.0	0.0	0.0	0.0

Continua

Infraestructura y telecomunicaciones	0.0	0.0	0.0	0.0	0.0
Desarrolladores/ programadores	0.0	0.0	0.0	0.0	0.0

La aplicación de salvaguardas implica recurrir en costos, los cuales estarán en función de los materiales a emplearse, del recurso humano a disponer tanto interno como externo, y del tiempo que se extienda en la aplicación de dichas salvaguardas.

Se deberá tomar en cuenta antes de la aplicación de la salvaguarda, la variable costo-beneficio, con el fin de poder controlar que el costo de la aplicación de la salvaguarda no supere al costo de la amenaza en caso de que se materialice.

Para la Cooperativa de Ahorro y Crédito Textil 14 de Marzo a nuestro criterio analizaremos la factibilidad de la aplicación de las salvaguardas y el beneficio que estas aportaran con el fin de disminuir el riesgo: así también, a nuestro libre criterio seleccionaremos los recursos convenientes a utilizarse para la aplicación de las salvaguardas, con sus costos respectivos y el tiempo que estimen prudente.

3.11. Medición de la Rentabilidad de TI

Una adecuada gestión del valor generado por las iniciativas del negocio, es fundamental para asegurar la disponibilidad de los fondos para los procesos de TI. Esto es lo que VAL-IT enfatiza, un conjunto de prácticas para garantizar el gobierno de TI, la gestión activa de inversiones y la gestión activa de la cartera de inversiones posibilitadas por TI que nos permita preguntarnos continuamente:

Figura No. 3.11 Preguntas de los Responsables en Inversiones de TI

Fuente: VAL - IT

Basándonos en las características VAL-IT, se establece una escala de madurez que responda estas interrogantes, orientada a determinar la capacidad y madurez de los procesos y practicas definidos en el marco de referencia de VAL-IT. Ver tabla No. 3.23

Tabla No. 3.23 Nivel de Madurez de las Inversiones en TI en una Organización

2	Inicial	TI visto como costo e inversión.

Continua

4	Definido	Las funciones de negocio y TI comprenden los requerimientos para seleccionar y ejecutar inversiones.

Una vez definidos los niveles de madurez de las inversiones en TI, nos queda determinar si existe una adecuada gestión de las inversiones de TI en la organización. Para esto,los niveles de madurez deben ser evaluados sobre los 3 procesos de VAL-IT mediante indicadores que nos mostraran donde está la organización con respecto a sus inversiones en TI.

Gestión del Valor (VG –Value Governance)

Para este proceso hemos definido indicadores, que son mecanismo de diagnóstico y gestión, que nos permitirán tener una idea global del nivel de madurez en el que se encuentra la organización con respecto a la Gestión de Valor, además de mostrar los objetivos y metas que deben cumplirse con el propósito de obtener el nivel de madurez buscado, ver Tabla No. 3.24

Tabla No. 3.24 Nivel de Madurez para la Gestión de Valor

5	Gestionado	Se ha desarrollado un proceso de gestión del portafolio de inversiones de TI.	CALIDAD 
		Alineación de las inversiones de TI con las prioridades de negocio	
4	Definido	Existe un comité de arquitectura.	
		Existe un comité de inversiones en TI.	
		El CIO está a nivel de la dirección ejecutiva de la organización.	
3	Repetible	La estructura del gobierno de TI está desarrollada.	
		El consejo y dirección ejecutiva son conscientes y apoyan al gobierno de TI.	
		Plena comprensión del gobierno de TI.	
2	Inicial	Mejora la contribución de los TI al funcionamiento de la empresa.	
		Existe concientización sobre los objetivos del gobierno de TI.	
1	Ausencia	No se reconoce ningún proceso de gobierno de TI.	RIESGO

* Comité de inversiones: Revisar, aprueba y define prioridades para las inversiones en TI.

* Comité de arquitectura: Desarrolla, comunica e introduce una arquitectura de empresa y estándares de TI.

Gestión de Cartera (PM –Portfolio Management)

Para este proceso hemos definido indicadores, que son mecanismo de diagnóstico y gestión, que nos permitirán tener una idea global del nivel de madurez en el que se encuentra la organización con respecto a la Gestión de Cartera, además de mostrar los objetivos y metas que deben cumplirse con el propósito de obtener el nivel de madurez buscado, ver Tabla No. 3.25

Tabla No. 3.25 Nivel de Madurez para la Gestión de Cartera

5	Gestionado	El retorno de la inversión del portafolio de TI se calcula a nivel de empresa y unidades de negocio/niveles funcionales.	CALIDAD  RIESGO
		Se refina el catálogo de servicios para incluir los de terceros.	
4	Definido	Se realizan ajustes dinámicos del portafolio basado en los cambios en la estrategia.	
		Se estructura el catalogo de servicios	
		Se usa el portafolio en la priorización y gestión del valor.	
3	Repetible	Análisis del portafolio (estrategias, solapamientos, riesgos).	
		Definido el portafolio de proyectos de aplicaciones de TI (repositorio simple de proyectos y definición de servicios claves).	
2	Inicial	La aprobación de los proyectos se hace por presiones o mandatos. (Criterios basados en coste).	
		Existe un repositorio de proyectos no consolidado.	
1	Ausencia	No se reconoce ningún portafolio de inversiones de TI.	

Gestión de Inversiones (IM –Investment Management)

Para este proceso hemos definido indicadores, que son mecanismo de diagnóstico y gestión, que nos permitirán tener una idea global del nivel de madurez en el que se encuentra la organización con respecto a la Gestión de Inversiones, además de mostrar los objetivos y metas que deben cumplirse con el propósito de obtener el nivel de madurez buscado, ver Tabla No. 3.26

Tabla No. 3.26 Nivel de Madurez para la Gestión de Inversiones

5	Gestionado	El retorno de la inversión del portafolio de TI se calcula a nivel de empresa y unidades de negocio/niveles funcionales.	**CALIDAD** 
		Se refina el catálogo de servicios para incluir los de terceros.	
4	Definido	Se realizan ajustes dinámicos del portafolio basado en los cambios en la estrategia.	
		Se estructura el catalogo de servicios	
		Se usa el portafolio en la priorización y gestión del valor.	
3	Repetible	Análisis del portafolio (estrategias, solapamientos, riesgos).	
		Definido el portafolio de proyectos de aplicaciones de TI (repositorio simple de proyectos y definición de servicios claves).	
2	Inicial	La aprobación de los proyectos se hacen por presiones o mandatos. (Criterios basados en coste).	
		Existe un repositorio de proyectos no consolidado.	
1	Ausencia	No se reconoce ningún portafolio de proyectos de TI.	**RIESGO**

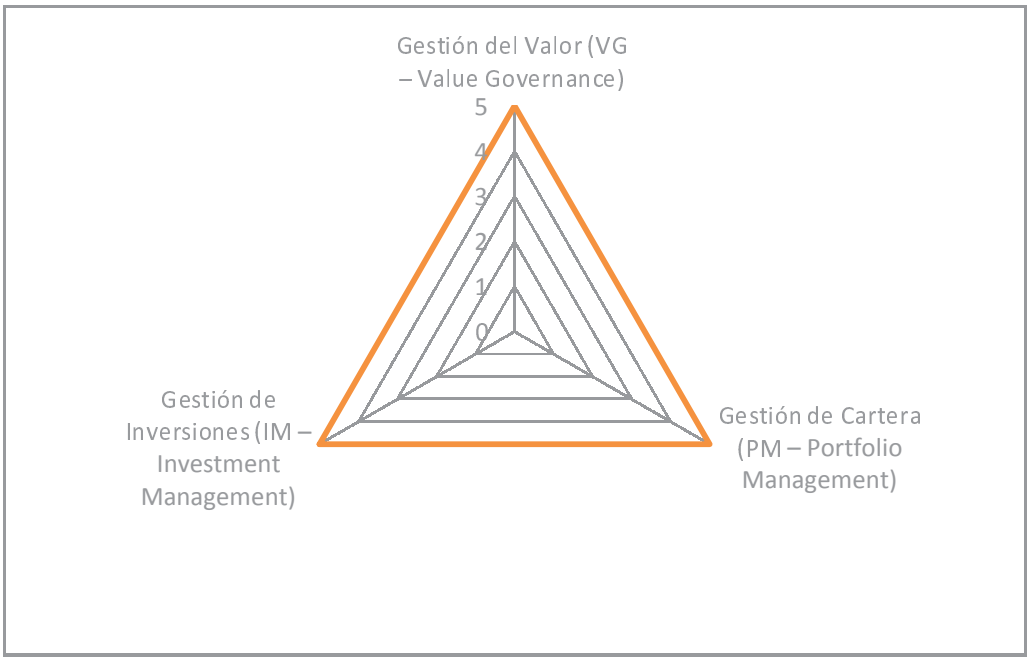


Figura No. 3.12 Nivel de Madurez Buscado

3.11.1. Medición de la Rentabilidad de TI en la COAC Textil 14 de Marzo

Para determinar si las inversiones en TI tienen impacto en la rentabilidad de la COAC Textil 14 de Marzo, se aplico la guía para determinar el Nivel de Madurez de las Inversiones en TI en una Organización, a través de entrevistas con los encargados del Departamento de Sistemas y en especial con la Ing.Verónica Suquillo Jefe del Departamento, obtenido los siguientes resultados.

Tabla No. 3.27 Madurez de las Inversiones de TI en la COAC Textil 14 de Marzo

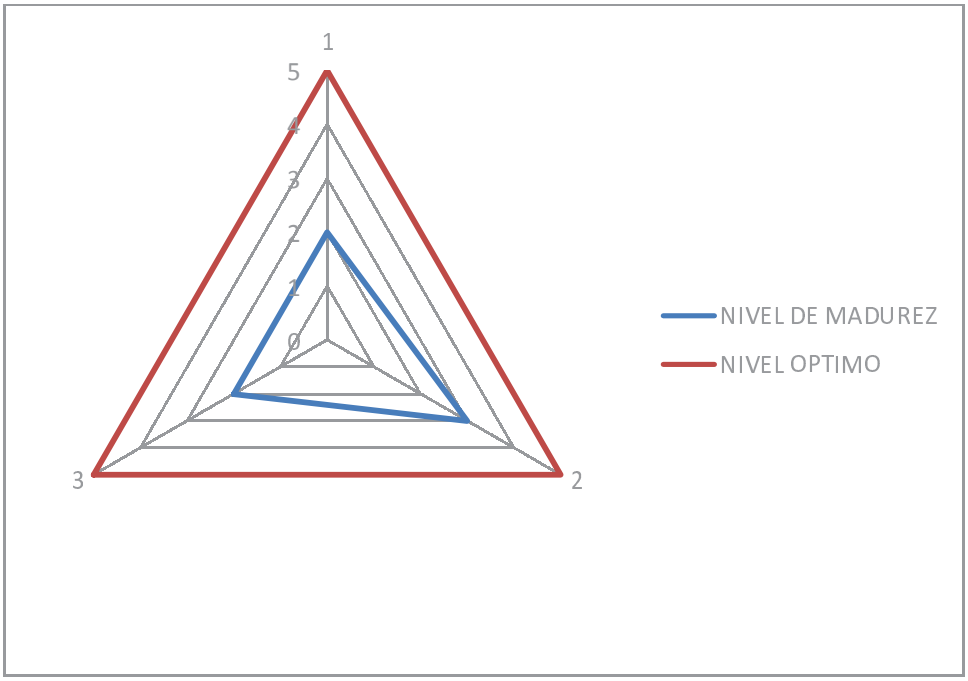


Figura No. 3.13 Nivel de Madurez de la COAC Textil 14 de Marzo

3.12. Medición del Nivel de Madurez de TI

En la actualidad las organizaciones se están preocupando en aplicar normas y estándares internacionales para la gestión de las TIC's como lo es ITIL. Las prácticas de ITIL son altamente complementarias en el momento de gestionar las TIC's desde el punto de vista del negocio. En lo que sea posible se debe tener una estrecha relación con el modelo de ITIL para garantizar la continua convergencia de los procesos de ITIL y las soluciones de gestión del servicio.

Los directivos de las empresas quieren que el departamento de TI no se limite a ayudar a su empresa a cumplir los objetivos de negocio. Esperan que introduzca elementos de innovación en el negocio. Por tanto, los esfuerzos de TI deberían centrarse en comprender hacia dónde se dirige la tecnología y saber aprovecharla, no sólo para mejorar la eficacia de los procesos operativos, sino para abrir nuevas oportunidades de negocio con servicios y productos innovadores. Esta nueva forma de plantear su misión, obliga a TI a dar un salto en el camino hacia una gestión de servicios madura. Pasa de centrar sus actividades en la simple puesta en marcha de una buena infraestructura, mecanismos de control rigurosos y procesos para una gestión de servicios efectiva, a convertirse en parte del negocio.

En la actualidad las pequeñas y medianas empresas experimentan problemas y desafíos que son diferentes a los que deben enfrentar las empresas más grandes. Por lo general se dispone de plantillas de empleados más reducida, presupuestos más bajos y entornos informáticos menos complejos que en las grandes empresas. Sin embargo se ven sometidas a las mismas demandas que se exige a las grandes empresas, deben optimizar sus niveles de servicio para apoyar a los objetivos del negocio, así como controlar costes y adaptar las actividades de sus departamentos de TI a las necesidades de la empresa.

Las pymes pueden alcanzar estos objetivos estructurando su gestión de servicios sobre los principales procesos del sector:

- Gestión de Incidentes

- Gestión de la Configuración
- Gestión de Cambios
- Gestión de Problemas

De manera similar en las grandes empresas enfrentar los procesos de ITIL requiere mucho tiempo alrededor de 3 años y es muy riesgoso tratar de hacerlo en forma integral de ahí que siguiendo la filosofía de ITIL para pymes, la implementación de una mesa de servicios también debe comenzar con Gestión de Incidentes, Gestión de Problemas, Gestión de Cambios y Gestión de Configuración.

3.12.1. Niveles de Madurez de ITIL

ITIL consta con 6 niveles de madurez, los mismos que se observan a continuación:

Figura No. 3.14 Niveles de Madurez de ITIL

Fuente: ITIL - ISACA

En particular para las Cooperativas de Ahorro y Crédito que es un importante sector financiero del medio, se pueden implementar las buenas prácticas de ITIL para mejorar la prestación y asistencia de servicios informáticos, para lo cual se debe tomar en cuenta los 4 procesos claves:

- **Gestión de Incidentes**

A continuación se tienen los niveles de madurez para la Gestión de Incidentes:

Tabla No. 3.28 Niveles de madurez para la Gestión de Incidentes

Nivel 5	Los incidentes se asignan al personal especialista.
	Se analiza la información del incidente entre la Gerencia de TI y los especialistas.
	Se lleva una clasificación de incidentes mediante una adecuada documentación.
	Se lleva un control de incidentes cerrados de forma satisfactoria de manera que tienda al 99%.
Nivel 4	Existe el personal capacitado para determinadas áreas.
	El incidente es documentado por el personal que se lo asignó.
	Se cuenta con un registro de los incidentes cerrados.
Nivel 3	El personal ha recibido capacitación en algunas áreas en que se desenvolvería adecuadamente por lo que no podría resolver varios incidentes al mismo tiempo.
	El personal cuenta con la información del incidente.

Continua ➡

Nivel 2	Se asigna el personal a los incidentes, de acuerdo a la experiencia que tengan en el área.
	El personal que se le asigno el incidente, cuenta con documentación si lo cree necesario.
Nivel 1	Los incidentes se asignan al personal que se encuentre disponible.
	El incidente no es documentado ni se lo clasifica.
	No se lleva un control de la cantidad de incidentes que se cerraron.
Nivel 0	El personal que recibe el incidente es el responsable.
	No se cuenta con una administración de incidentes.

Ejemplos de métricas:

- Porcentaje de incidencias resueltas.
- Tiempo medio de resolución.
- Porcentaje de incidencias reasignadas más de una vez.
- Porcentaje de SLAS cumplidos.

- **Gestión de Problemas**

A continuación se tienen los niveles de madurez para la Gestión de Problemas:

Tabla No. 3.29 Niveles de madurez para la Gestión de Problemas

Nivel 5	Se monitoriza la calidad de la infraestructura de TI con frecuencia.
	Se analiza la configuración de la infraestructura de TI periódicamente con el objetivo de prevenir incidentes incluso antes que ocurran.
	Se tiene definido al Jefe de Administración de Problemas que es la persona encargada de manejar los problemas.
	Todos los problemas son registrados y documentados durante todo su progreso por el asignado a la solución.
	Se cuenta con métricas para medir la solución del problema.
Nivel 4	Se tiene claramente identificados los problemas resueltos.
	Se realiza una sociabilización de los involucrados de los problemas presentados.
Nivel 3	Se lleva un registro de problemas con al menos: los elementos de configuración implicados, causas del problema, síntomas asociados, soluciones temporales, servicios involucrados, niveles de prioridad y estado (activo, error conocido, cerrado).
Nivel 2	No se lleva un adecuado registro de problemas.
	El encargado de un problema es quien cuenta con una mayor experiencia en el área.

Continua ➡

Nivel 1	Cada responsable lleva cuantificados los problemas resueltos individualmente.
	Los problemas no son documentados adecuadamente.
	La solución de los problemas no son sociabilizados a los involucrados.
	El problema se asigna a la persona que más experiencia tenga en el área.
Nivel 0	Los problemas no tienen documentación.
	El problema se asigna a la persona que lo detectó.

Ejemplos de métricas:

- Número de incidencias resueltas con trabajo documentado.
- Top 5 de categorías de incidencias reportadas en el periodo.
- Coste total de resolución por problema

- **Gestión de Cambios**

A continuación se tienen los niveles de madurez para la Gestión de Cambios:

TablaNo.3.30 Niveles de madurez para la Gestión de Cambios

Nivel 5	Se lleva una adecuada evaluación y planificación del proceso de cambio para asegurar que se lleva a cabo de una manera más eficiente siguiendo procedimientos establecidos y asegurando la calidad y continuidad del servicio de TI.
	Se realiza un análisis del porcentaje de cambios exitosos.
	Se documenta los cambios de una forma adecuada, de manera que pueda formar parte de una base de conocimientos para futuros cambios.
Nivel 4	La documentación de los cambios tiene un estándar definido.
	Se tiene diferenciados los cambios exitosos de los fallidos.
	Se cuenta con documentación y aprobación de los involucrados del cambio.
	La opinión de los usuarios es tomada en cuenta en caso de que se encuentren objeciones.
Nivel 3	Se tiene documentado el registro de cambios.
	Se cumplen con los calendarios previstos y la asignación de recursos es la adecuada.
Nivel 2	Se documentan los cambios por los involucrados y por separado.
	Se tiene definido el calendario previsto pero no se toma en consideración los recursos necesarios.
Nivel 1	La documentación de los cambios se encarga el responsable y no es obligatorio.
	Los cambios quedan sujetos a calendarios propios de cada cambio.
	El cronograma de cambios se lo deja a cargo de los involucrados.

Continua

Nivel 0	El cambio se lo realiza a criterio del involucrado.
	No se cuenta con documentación de cambios.
	No se cuenta con un procedimiento y cronograma.

Ejemplos de métricas:

- Número de peticiones realizadas sin autorización.
- Número de peticiones sin reverso previsto.
- Número de cambios de emergencia realzados.

- **Gestión de la Configuración**

A continuación se tienen los niveles de madurez para la Gestión de la Configuración:

Tabla No. 3.31 Niveles de madurez para la Gestión de Configuración

Nivel 5	Se tiene un claro conocimiento de la infraestructura con su respectiva documentación.
	Se tiene conocimiento claro del ciclo de vida de los activos, desde su inventario hasta la fase de retirada.
	Se lleva un control de todos los elementos de configuración de la infraestructura de TI con el adecuado nivel de detalle y se gestiona dicha información a través de la Base de Datos de Configuración.

Continua ➡

Nivel 4	La infraestructura es conocida por las personas involucradas.
	Se lleva un control regular del inventario de los activos.
Nivel 3	La infraestructura solo es conocida por determinados funcionarios.
	Cuando se realiza la adquisición y baja de activos, se actualiza en el inventario.
Nivel 2	Solo se tiene un conocimiento de las partes de infraestructura que se manipulan con frecuencia.
	El inventario se lo actualiza cuando se hace la adquisición de activos
Nivel 1	El conocimiento de la infraestructura es mínimo.
	El inventario no se encuentra actualizado.
Nivel 0	No existe conocimiento de la infraestructura de la institución.
	No existe un inventario de infraestructura.

Ejemplos de métricas:

- Número de errores debido a datos incorrectos en BD.
- Porcentaje de identificaciones incorrectas en la BD.

Además es recomendable evaluar los procesos existentes usando una serie de criterios dados en el modelo de evaluación de la gestión de las TIC's para identificar los puntos débiles y oportunidades sin hacer un mayor esfuerzo de documentación de procesos.

Para medir se debe realizar un análisis de la situación actual de la gestión de TI y compararla con un marco de referencia que en este caso es ITIL para de esta forma tener una visión clara del nivel de madurez en que se encuentra la organización en la gestión de las TIC's.

Al realizar la medición se debe decidir lo que se va a evaluar para lo cual se debe definir cómo se lo va a hacer. Existen mediciones que se las pueden realizar de forma intuitiva con solo observar las actividades de la gestión de TI de la organización,

pero en algunos casos esto no es posible como por ejemplo en el cumplimiento de ciertas políticas internas, etc.

Se debe encontrar claramente definido el funcionario responsable asignado a la medición del proceso, que tenga a su disposición las herramientas necesarias para mencionada actividad y que se disponga claramente del procedimiento a utilizarse.

Las actividades habituales en el proceso de medición incluyen:

- Definición del calendario o frecuencia de toma de datos (en el caso automático este proceso puede ser continuo).
- Análisis de las herramientas necesarias para el proceso de medición y registro.
- Instalación, configuración, personalización y pruebas de funcionamiento de dichas herramientas.
- Analizar la disponibilidad y capacidad de la infraestructura necesaria.
- Monitorizar la calidad y adecuación al propósito de los datos recogidos, estableciendo métricas.
- Preparar los datos para que sean accesibles y útiles.
- Documentar todo el proceso.

En el siguiente gráfico se muestran los niveles de madurez. Una organización debe tratar de llegar a un nivel 5 de madurez para poder decir que se encuentra en un nivel óptimo.

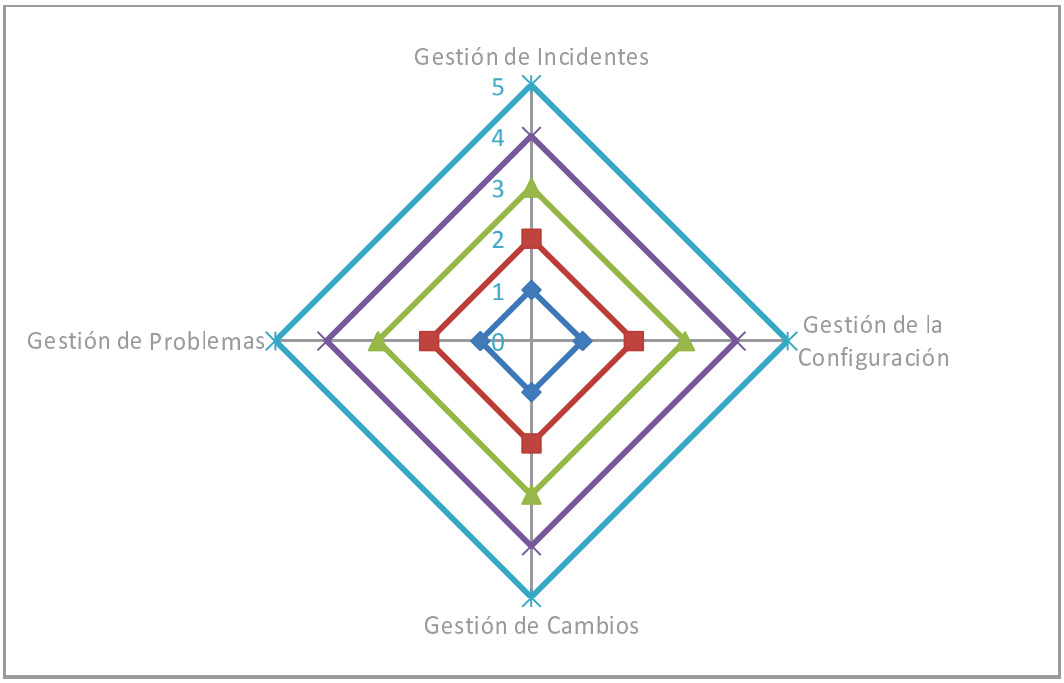


Figura No. 3.15 Nivel de Madurez de TI

3.12.1.1.Nivel de Madurez de la COAC Textil 14 de Marzo

Para una mejor comprensión del nivel de madurez de los procesos de ITIL para pymes, a continuación se presentan los resultados que se obtuvieron al aplicar a la COAC Textil 14 de Marzo.

Resultados:

- Los incidentes son asignados al personal que se encuentra encargado del área en que se presentó.
- El personal del departamento de TI tiene conocimiento únicamente de la infraestructura que maneja el personal con frecuencia. Existen áreas que no tienen conocimiento de la infraestructura debido a que el personal que se encargaba, ya no labora en la institución.
- Se cuenta con procedimientos establecidos pero no se encuentran documentados.

- El registro de problemas lo lleva el personal que fue asignado si lo considera adecuado. Además el personal no tiene conocimiento del problema presentado en distintas áreas.

Se realiza un análisis de los resultados obtenidos y se los ubica en el nivel que corresponde. A continuación se puede ver los niveles de madurez que se obtuvieron en cada proceso.

Tabla No. 3.32 Resultados del Nivel de Madurez en la COAC Textil 14 de Marzo

Nivel 0				
Nivel 1	✔			✔
Nivel 2		✔	✔	
Nivel 3				
Nivel 4				
Nivel 5				

Para mayor compresión, a continuación se muestra el gráfico del resultado obtenido.

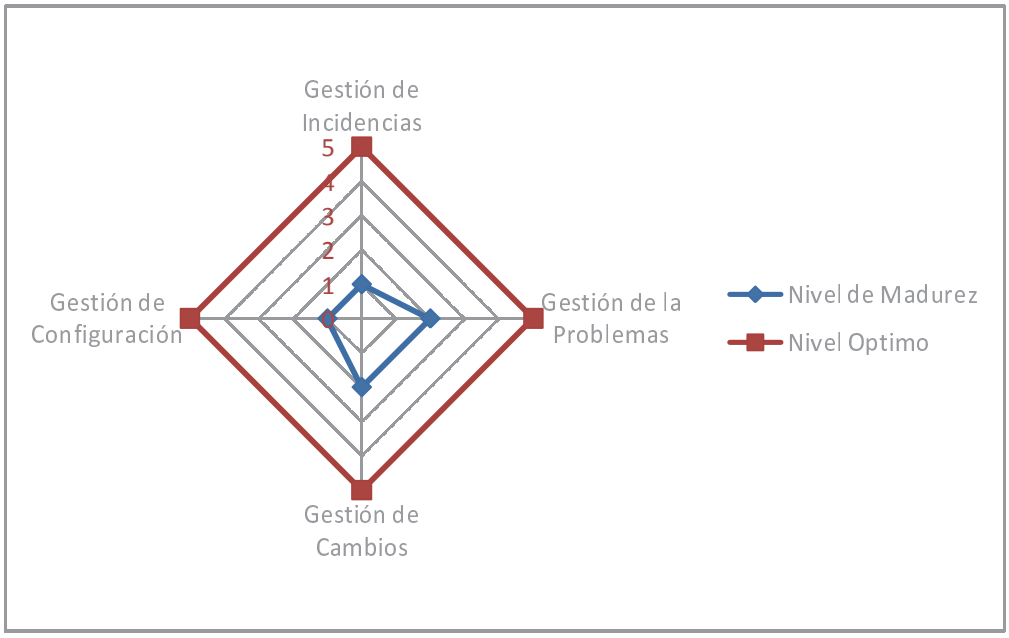


Figura No. 3.16 Nivel de Madurez de TI de la COAC Textil 14 de Marzo

Las organizaciones que desean ser exitosas comprenden y administran los riesgos asociados con la implementación de normas y mejores prácticas, como acabamos de ver en este capítulo, COBIT ayuda a reducir las brechas entre los riesgos del negocio, las necesidades de control y los aspectos propiamente técnicos. Provee de buenas prácticas, gracias al marco de dominios con que cuenta. Para brindar una visión clara a la directiva de la inversión que se hace en tecnología, se utilizó Val-IT ya que se puede verificar que el valor obtenido, sea al costo más conveniente para la empresa y a un nivel de riesgo adecuado. ITIL provee a la organización más eficiencia y efectividad alineadas con los objetivos del negocio, por lo que para organizaciones como las Cooperativas de Ahorro y Crédito se tomó en cuenta cuatro procesos fundamentales: la Gestión de Incidentes, Gestión de

Problemas, Gestión de Cambios y Gestión de Configuración, que son con lo que se debe empezar para una adecuada administración de tecnología.

CAPITULO IV

4.1. Conclusiones

1. El modelo propuesto es el resultado del estudio, análisis y adopción de marcos de referencia y metodologías (COBIT, ITIL, VAL-IT y la Norma de Riesgo Operativo) para la Gestión de TIC's, de los cuales se ha tomado lo pertinente para proporcionar una guía de mejores prácticas a fin de lograr un producto que satisfaga las necesidades del sector de las Cooperativas de Ahorro y Crédito, bajo un enfoque sistemático y profesional para la Gestión de TIC's.

2. En la elaboración del modelo propuesto, COBIT se utilizo como un marco general de control basado en un modelo de procesos de Gestión de TI, que debería adaptarse a cada organización. Los estándares, las prácticas específicas y las normas, tales como ITIL, VAL-IT y la Norma de Riesgo Operativo abarcan áreas discretas y pueden ser mapeadas en el marco COBIT, estructurando una jerarquía de materiales de orientación. Así se logra que las mejores prácticas de Gestión de TIC's se ajusten a los requisitos del negocio y se integren entre sí y con los procedimientos internos.

3. Con la finalidad de validar el modelo propuesto, se aplico el mismo en la COAC Textil 14 de Marzo y se pudo comprobar la pertinencia de la propuesta con los procesos y procedimientos reales y en producción, siendo coherente el modelo de Gestión de TIC's con las necesidades específicas del área financiera y la integración de las metas de TI y las metas del negocio, mediante un proceso detallado paso a paso pero con la posibilidad de ser adaptado a cada situación particular.

4. El presente trabajo cuenta con una aplicación de la metodología MAGERIT, para la ejecución del Análisis y Gestión de Riesgos, que es una guía que permite prevenir, detectar y mitigar los riesgos; extendida hacia cualquier institución pública o privada que posee activos de TI.

5. Se desarrollo un procedimiento basado en el modelo del VAL-IT que permite determinar si una organización hace un adecuado uso de las inversiones en TI,

determinando el estado actual de la instituciones, además de proporcionar las metas y objetivos que le permitan gestionar de forma apropiada las inversiones de tecnología en caso de que no lo estén haciendo, para así optimizar las inversiones en TIC, para asegurar que el portafolio global de inversiones en TIC está alineada con los objetivos de negocio.

6. Se estableció un modelo de madurez que nos muestra y explica el camino de una organización para alcanzar un buen nivel de madurez en los principales procesos de gestión de servicios aplicando ITIL (ITIL para PYMES), a través de diversos niveles de madurez. El mismo, ofrece una estructura para comparar el grado de desarrollo de la capacidad de gestión de los servicios de TI existentes en la organización.

4.2. Recomendaciones

1. Se plantea la necesidad de aplicar una Auditoria en cualquier Cooperativa de Ahorro y Crédito, donde se desglose el modelo propuesto. A partir de los resultados obtenidos se puede realizar la afinación del modelo y una propuesta de mejora o incorporación de estándares relacionados.

2. El presente modelo abarca la Gobernabilidad de TI, la Gestión de Servicios y la valoración de la rentabilidad de la TI en el negocio, el modelo se puede ampliar para una visión global del análisis de riesgos, usando la ISO 31500 y NGOSS para evaluación de los niveles de madurez de procesos bajo la filosofía BPM.

3. Se recomienda a las organizaciones realicen el Análisis y Gestión de Riesgos de los Sistemas de Información, por lo menos, una vez al año, con lo cual podrán conocer sus fortalezas y debilidades e implementar salvaguardas para reducir las debilidades encontradas. Aplicando la metodología MAGERIT, complementada con la herramienta PILAR Basic.

4. Planificar la implementación de ITIL estableciendo un alcance acorde a la situación actual de la empresa que se determina con el Nivel de Madurez de TI, aplicando los procesos de ITIL para PYMES que representaran la línea base del ciclo de vida de los servicios de TI.

4.3. Recomendaciones Adicionales

A continuación se presentan algunas sugerencias, basadas en la experiencia propia al haber cursado la Maestría en Evaluación y Auditoria de Sistemas Tecnológicos, que ayuden a mejorar el programa:

1. Formación pedagógica para el personal docente que sea complementaria a los procesos de conocimiento debido a que muchos profesores no saben transmitir el conocimiento.

2. Revisión de la malla curricular y los contenidos de las asignaturas que permitan presentar una mejor oferta académica.

3. Incentivar la presentación de proyectos de investigación por parte de los estudiantes para la adquisición de experiencia y mejoramiento de la calidad del programa de maestría.

4. Promover grupos de investigación con el fin de mejorar el conocimiento y el aprendizaje por parte de los estudiantes.

5. Que la Universidad de las Fuerzas Armadas genere una beca para los mejores estudiantes de los posgrados devolviéndole la matricula o parte de ella.

Bibliografía

ArriantoMukti, Wibowo (s.f.). Enterprise Value: Governance of IT Investments The Val IT Framework 2.0.Recuperado de http://www.itgov.cs.ui.ac.id/itgov/Val%20IT%202.0.pdf.

(ISACA), Information Technology Governance Institute. (s.f.). Recuperado el 15 de Noviembre de 2013, de http://www.isaca.org/cobit/pages/default.aspx

AENOR. (2009). *ISO/IEC 20000 Guía completa de aplicación para la gestión de los servicios de tecnologías de la información.* AENOR ediciones .

Arrianto Mukti, W. (s.f.). *Governance of IT Investments The Val IT Framework 2.0*. Obtenido de http://www.itgov.cs.ui.ac.id/itgov/Val%20IT%202.0.pdf

Ballester Fernández, J. M. (s.f.). *GOBIERNO CORPORATIVO TIC*. Obtenido de http://www.isacamty.org.mx/archivo/Standard_ISO38500.pdf

Coronel Hoyos, K. d. (2008). *Metodología de Evaluación del Riesgo Tecnológico en las Instituciones del Sistema Financiero Ecuatoriano, Utilizando COBIT 4.1.* Sangolqui.

Davila, L. (2007). *La Reforma de las Instituciones Financieras y la Regulación Bancaria en el Ecuador a partir de Basilea II*. Obtenido de http://repositorio.uasb.edu.ec/bitstream/10644/523/1/T-

El Comercio. (13 de Junio de 2013). *Cronología de los Problemas en Cooperativas de Ahorro y Crédito*. Obtenido de http://www.elcomercio.ec.

IAPC. (2002). *Norma Internacional de Auditoría N° 6 Evaluación del Riesgo y Control Interno.* Corporación Edi-Ábaco Cía. Ltda.

ISACA. (2012). *COBIT 5.*

ISACA, I. T. *Control Objectives for Information and Related Technologies (COBIT).*

Lopez, F., Amutiol, M., & Candau, J. (2006). *MAGERIT.*

Mordecki, D. (03 de Octubre de 2004). *¿Qué es diseñar?* Obtenido de Mordecki: http://www.mordecki.com/html/que_es_disenar.php

osiatis. (s.f.). Obtenido de http://itilv3.osiatis.es/proceso_mejora_continua_servicios_TI/proceso_mejora_csi/recopilacion_datos.php

osiatis. (s.f.). ITIL-Gestión de Servicios TI. *Curso ITIL* .

PNUD. (2002). *Informe sobre Desarrollo Humano.*

Repositorio digital de Tesis PUCP. (s.f.). Recuperado el 15 de Noviembre de 2013, de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/1433/GOMEZ_ALVAREZ_JESUS_GESTION_INCIDENTES.pdf?sequence=1

Riesgo operativo en el Ecuador. (s.f.). Recuperado el 15 de Noviembre de 2013, de http://riesgooperativo.blogspot.com/

SBS. (2012). *Norma de Riesgo Operativo Resolución JB-2012-2148.*

Universidad ICESI. (s.f.). Recuperado el 15 de Noviembre de 2013, de http://bibliotecadigital.icesi.edu.co/biblioteca_digital/bitstream/10906/68861/1/metodologia_gestionar_inversiones.pdf