ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE POSGRADO EN TECNOLOGIAS DE LA INFORMACION

MODELO DE AUDITORÍA INFORMÁTICA BASADA EN RIESGOS EN ÁMBITOS FINANCIEROS. APLICACIÓN DE UN CASO DE ESTUDIO A UNA COOPERATIVA DE AHORRO Y CRÉDITO.

TESIS PREVIA A LA OBTENCIÓN DEL GRADO DE MÁSTER (Msc.) EN GESTION DE TECNOLOGIAS DE INFORMACION

BETY ELIZABETH QUISHPE GOYES
bety_quishpe@hotmail.com

MARJORI SILVANA VARGAS CISNEROS
marjori12vc@yahoo.com

DIRECTOR: ING. CARLOS MONTENEGRO
carlos.montenegro@epn.edu.ec

2013

DECLARACIÓN

Nosotras, Bety Quishpe y Marjori Vargas, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Bety Quishpe	**Marjori Vargas**

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Bety Quishpe y Marjori Vargas, bajo mi supervisión.

Ing. Carlos Montenegro

DIRECTOR DE PROYECTO

AGRADECIMIENTOS

A Dios por ser mi luz, mi guía y mi fortaleza en todo momento, a mi esposo, padres y hermanos por todo el apoyo recibido.

BETY

A Dios creador del universo y dueño de mi vida que me permite concluir con esta meta, a Iván, Carlitos, David e Isaac por su comprensión, paciencia y apoyo, los amo.

MARJORI

DEDICATORIAS

A mi esposo y mis padres por el apoyo incondicional durante toda la carrera, por haber forjado en mí, la idea de obtener un grado de cuarto nivel.

BETY

A mi esposo, hijos y padres porque son lo más importante en mi vida.

MARJORI

CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

El presente trabajo tiene como objetivo elaborar un modelo que permita efectuar auditorías informáticas basadas en riesgos en ámbitos financieros, en este caso aplicado a una Cooperativa de Ahorro y Crédito. El modelo propuesto se basa en normas y estándares nacionales e internacionales relacionados con la auditoría informática basada en riesgos, que permiten al auditor informático obtener las referencias necesarias para efectuar el examen de auditoría.

A continuación se presenta el detalle del trabajo en mención:

El Capítulo I, **MARCO CONCEPTUAL, PROCESOS Y PROCEDIMIENTOS DE LA AUDITORÍA INFORMÁTICA BASADA EN RIESGOS**, contiene el marco teórico de la auditoría de sistemas, los estándares internacionales, las regulaciones ecuatorianas que deben cumplir las entidades financieras, así como un extracto del proceso actual de auditoría informática y los procedimientos relacionados en la institución financiera tomada como caso de estudio para el presente trabajo.

El Capítulo II**, DESARROLLO DEL MODELO PARA EFECTUAR AUDITORÍAS INFORMÁTICAS BASADAS EN RIESGOS**, plantea el modelo que permitirá llevar a cabo los exámenes de auditoría, el cual se ejecuta en tres fases principales que son: planificación, definición de alcance y objetivos; ejecución, y una fase de apoyo que es la de Monitoreo, la cual permitirá dar un seguimiento adecuado de los hallazgos de auditoría encontrados relacionados con falencias o debilidades de un objetivo de control no cumplido que incide en el nivel de madurez del proceso evaluado.

El Capítulo III, **VALIDACIÓN DE LA APLICABILIDAD DEL MODELO A TRAVÉS DE UN CASO DE ESTUDIO EN UNA ENTIDAD FINANCIERA**, es la aplicación del modelo propuesto en el presente trabajo, para lo cual se tomó como caso de estudio una Cooperativa de Ahorro y Crédito. En cada una de las fases del modelo se elaboraron formatos y esquemas necesarios, a la medida de la Institución financiera.

Finalmente, el Capítulo IV, **CONCLUSIONES Y RECOMENDACIONES**, plantea las conclusiones en base a la evidencia obtenida de la aplicación del modelo a un caso de estudio utilizando el enfoque basado en riesgos, así como las recomendaciones que pueden generar un valor agregado al hacer uso del modelo.

PRESENTACION

Como antecedente para el desarrollo del presente trabajo es importante mencionar que la Superintendencia de Bancos y Seguros emitió la resolución JB-2010-1549 [1], la cual debe ser cumplida por todas las instituciones financieras controladas por este organismo; la normativa indica que se deberá efectuar las auditorías basadas en riesgos al igual que los programas anuales de auditoría, por tal razón dichas entidades requieren realizar las auditorías, así como los seguimientos trimestrales sobre el avance de las recomendaciones de los hallazgos de los exámenes de auditoría, bajo un modelo que les permita dar cumplimiento a la exigencia del Organismo de Control y a la vez mejorar la productividad de los funcionarios del área de Auditoría Interna.

En la actualidad, no existe un modelo de uso generalizado utilizado por las entidades financieras el cual les permita efectuar sus auditorías basadas en riesgos, sino que cada una de ellas ha desarrollado metodologías a la medida a fin de llevar a cabo auditorías tradicionales, es decir, verificaciones de cumplimiento y cálculos.

Con el fin de dar solución a la problemática planteada en el párrafo anterior, el presente trabajo propone un modelo que sirva como guía para la ejecución de las auditorías informáticas basadas en riesgos. El modelo permitirá dar cumplimiento a la resolución emitida por la Superintendencia de Bancos y Seguros.

El modelo propuesto se apoya en el marco de trabajo COBIT 4.1 [2], ITAF^{TF} [3], PROCESS ASSESSMENT MODEL (PAM) [4], Prácticas de Control y Guías de aseguramiento de ISACA [5].

CAPÍTULO 1. MARCO CONCEPTUAL, PROCESOS Y PROCEDIMIENTOS DE LA AUDITORÍA INFORMÁTICA BASADA EN RIESGOS.

Todo modelo de auditoría debe tener como fundamento un marco teórico conceptual, así como un proceso que organice los procedimientos relacionados con el desarrollo de los exámenes de auditoría informática, por lo que las autoras consideran vincular estos tres aspectos relevantes a fin de lograr el sustento necesario que servirá como punto de partida para el desarrollo del modelo que en el presente trabajo se propone. A continuación se muestra un esquema general:

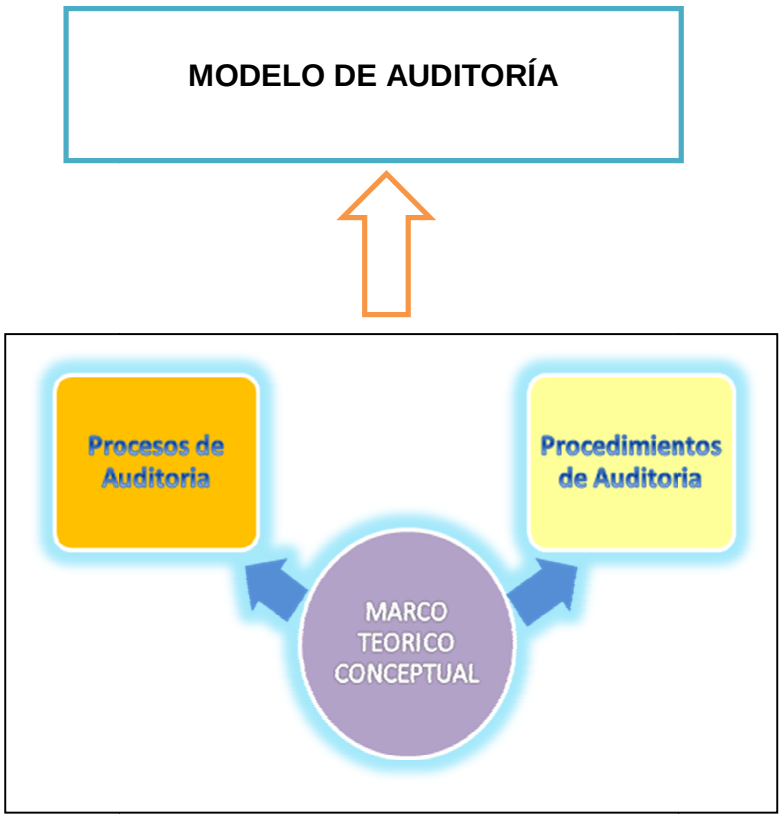


Figura 1 Relación marco teórico, procesos y procedimientos con modelo de auditoría

1.1 MARCO CONCEPTUAL DE AUDITORÍA INFORMATICA

El Marco conceptual que se expone a continuación permitirá tener una visión general de todas las normativas, estándares nacionales e internacionales actuales relativas al enfoque de auditoría basada en riesgos, aspecto que constituye el sustento para el desarrollo del modelo; así como obtener un entendimiento general sobre la necesidad del control sobre la Tecnología de Información, el rol del departamento de Auditoría Interna y el papel que juega la Auditoría informática dentro de una organización que a criterio de las autoras es importante debido a que es el fundamento del desarrollo del modelo.

Con el siguiente esquema se presenta los elementos teórico-conceptuales debidamente vinculados al modelo que se propondrá.

Figura 2 Marco conceptual vinculado a modelo propuesto

1.1.1 LA NECESIDAD DE CONTROL EN TECNOLOGÍA DE INFORMACIÓN

En los últimos años, ha sido cada vez más evidente la necesidad de un Marco Referencial para el control de tecnología de información. Las organizaciones exitosas requieren una apreciación y un entendimiento básico de los riesgos y limitaciones de TI a todos los niveles dentro de la empresa con el fin de obtener una efectiva dirección y controles adecuados. La Administración debe decidir cuál es la inversión razonable en el control en TI y cómo lograr un balance entre riesgos e inversiones en control en un ambiente de TI frecuentemente impredecible. Los controles en los sistemas de información ayudan a administrar los riesgos, no los eliminan. Adicionalmente, el exacto nivel de riesgo nunca puede ser conocido ya que siempre existe un grado de incertidumbre. Finalmente, la Administración debe decidir el nivel de riesgo que está dispuesta a aceptar. Juzgar cual puede ser el nivel tolerable, particularmente cuando se tiene en cuenta el costo, puede ser una decisión difícil para la Administración. Por esta razón, la Administración necesita un marco de referencia de las prácticas generalmente aceptadas de control de TI para compararlos contra el ambiente de TI existente y planificado. Existe una creciente necesidad entre los usuarios de los servicios de TI, de estar protegidos a través de la acreditación y la auditoría de servicios de TI proporcionados internamente o por terceras partes, que aseguren la existencia de controles y seguridades adecuadas.

1.1.2 EL ROL DE AUDITORÍA INTERNA

El rol fundamental de la Auditoría Interna es proveer un aseguramiento razonable sobre la efectividad de las actividades de la gestión de riesgos corporativa, verificar si los riesgos claves del negocio se gestionan apropiadamente y validar que la función del control interno sea efectiva.

A Auditoría Interna no le compete efectuar:

- Establecer el apetito de riesgo
- Imponer procesos de gestión de riesgo
- Manejar el aseguramiento sobre los riesgos
- Tomar decisiones en respuesta a los riesgos
- Implementar respuestas a riesgos a favor de la administración
- Tener responsabilidad de la gestión de riesgo

1.1.3 LA AUDITORÍA INFORMÁTICA

La Auditoría Informática es el conjunto de técnicas, procedimientos para evaluar y controlar un sistema informático, cuyo fin es validar si sus actividades son correctas y están enmarcadas dentro de los lineamientos establecidos en una Organización.

La Auditoría Informática no solo comprende la evaluación de los equipos de cómputo de un sistema o procedimiento específico, sino que además, considera la evaluación de sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La Auditoría Informática es el pilar para el buen desempeño de los sistemas de información, debido a que proporciona los controles necesarios para que los sistemas sean confiables, garanticen la seguridad de los activos de información, aseguren la eficacia de los procesos.

1.1.4 RESOLUCIÓN JB-2005-834 [6]

La resolución JB-2005-834 fue emitida en Octubre del 2005, misma que establece un conjunto de principios que proporcionan a las Entidades financieras un marco para la gestión y supervisión efectiva del riesgo operativo, también es de uso para entidades de supervisión al momento de evaluar políticas y prácticas de gestión del riesgo operativo. Además, el alcance de la norma depende de factores tales como el tamaño, la sofisticación y complejidad de las entidades financieras para las que aplica. La

resolución imparte una serie de disposiciones aplicables al sistema financiero a fin de contar con un sistema de gestión efectivo para la administración del riesgo operativo que permita identificar, medir, controlar/mitigar los riesgos derivados de fallas o insuficiencias en los procesos, personas, tecnologías de información y eventos externos, incluyendo el riesgo legal.

La resolución recomienda que se cumpla con sus directrices respecto a la administración de los procesos, personas, tecnología de la información y eventos externos, agrupando sus procesos por línea de negocio, identificando para cada una de estas sus eventos de riesgo, las mismas que están agrupadas de la siguiente manera: Fraude Interno, Fraude Externo, Prácticas laborales y seguridad del ambiente de trabajo, prácticas relacionadas con los clientes, productos y negocios, daños a los activos físicos, fallas de tecnología de información; y, deficiencias en la ejecución de procesos, operaciones y relaciones con proveedores y terceros.

Figura 3 Resolución JB-2005-834 [6] – Eventos de riesgos

1.1.4.1 Riesgo de Procesos

Para este factor primero se deben identificar los procesos del gobierno corporativo o procesos estratégicos, productivos, operativos y los de apoyo. Esta actividad exige contar con un mapa de procesos y la cadena de valor de la institución.

El siguiente paso consiste en elaborar un diagnóstico de los procesos con respecto a riesgos que pueden ocasionar pérdidas, para lo cual es necesario analizar todo el flujo de cada proceso, especialmente los críticos, poniendo énfasis en los controles y riesgos, es decir, ubicando debilidades de control que podrían generar un riesgo en el proceso. La flujodiagramación, políticas y procedimientos de los procesos, son importantes para validar su cumplimiento e identificar oportunidades de mejoramiento.

Un tercer paso, corresponde al diseño e implantación de los controles faltantes o a mejorar la efectividad de los controles existentes y evaluar el nivel de riesgo residual a fin de decidir la incorporación de controles adicionales o la aceptación del riesgo. Finalmente, se documentan las políticas y procedimientos de cada proceso rediseñado, se prepara un inventario de procesos de la institución con información básica de los mismos y se procede a su difusión y entrenamiento.

1.1.4.2 Riesgo de Personas

Para cubrir este ámbito, se debe identificar fallas o insuficiencias asociadas al factor humano, también conocido como ingeniería social, en los procesos de incorporación, permanencia y desvinculación.

Además, debe validarse que estos procesos se ajusten a las disposiciones legales vigentes y garanticen condiciones laborales idóneas. Es conveniente revisar estos procesos de forma minuciosa a fin de identificar riesgos y oportunidades de mejoramiento. También se debe evaluar la definición y

cumplimiento de competencias, valores, actitudes y habilidades del personal. Finalmente, disponer de una base de datos con toda la información relativa al personal y su trayectoria en la organización.

1.1.4.3 Riesgos de Eventos Externos

Consiste en identificar, analizar y cuantificar riesgos derivados de fallas en servicios públicos, desastres naturales, atentados y otros actos delictivos que pudieran afectar la operación normal de la institución. Debe revisarse que estos eventos estén considerados en los planes de contingencia y recuperación de desastres, en caso de tenerlos, de lo contrario, se procede a elaborarlos.

1.1.4.4 Riesgos de Tecnologías de Información

Este factor es quizás el que tiene mayor alcance y complejidad de todos los que integran el riesgo operativo, esto se debe a dos causas principales: las tecnologías de información se extienden por todos los procesos y niveles de decisión de la Institución, además, las tecnologías de información siguen siendo un tema muy complejo y técnico, las cuales son manejadas por especialistas, quienes son presionados cada vez más en la entrega de servicios oportunos y de calidad.

Se debe considerar que para contar con una apropiada gestión del riesgo, las instituciones deben disponer de políticas, procesos y procedimientos que aseguren una adecuada planificación y administración de las tecnologías de información para garantizar lo siguiente:

- La administración de tecnología de información debe soportar adecuadamente los requerimientos de operación actuales y futuros de la entidad;
- Las operaciones de tecnología de información deben satisfacer los requerimientos de la entidad;

- Los recursos y servicios provistos por terceros se deben administrar adecuadamente y se debe monitorear la efectividad y eficiencia del servicio
- El proceso de adquisición, desarrollo, implementación y mantenimiento de aplicaciones debe satisfacer los objetivos del negocio.
- La infraestructura tecnológica que soporta las operaciones debe ser administrada y monitoreada de manera adecuada.

En materia de Seguridad de la Información, la Resolución JB-2005-834 [6] abarca otras disposiciones, donde se señala que las instituciones deben disponer de políticas, procesos y procedimientos que aseguren:

- Que el sistema de administración de seguridad de la información satisfaga las necesidades de la entidad para salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas.
- Que exista continuidad en la operación de la institución frente a eventos imprevistos en las tecnologías de información.
- Que los planes de contingencia y continuidad garanticen la capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción severa del negocio, implementando además un proceso de administración de la continuidad del negocio.

A continuación se muestra un diagrama que muestra en detalle el universo de la resolución JB-2005-834. [6]

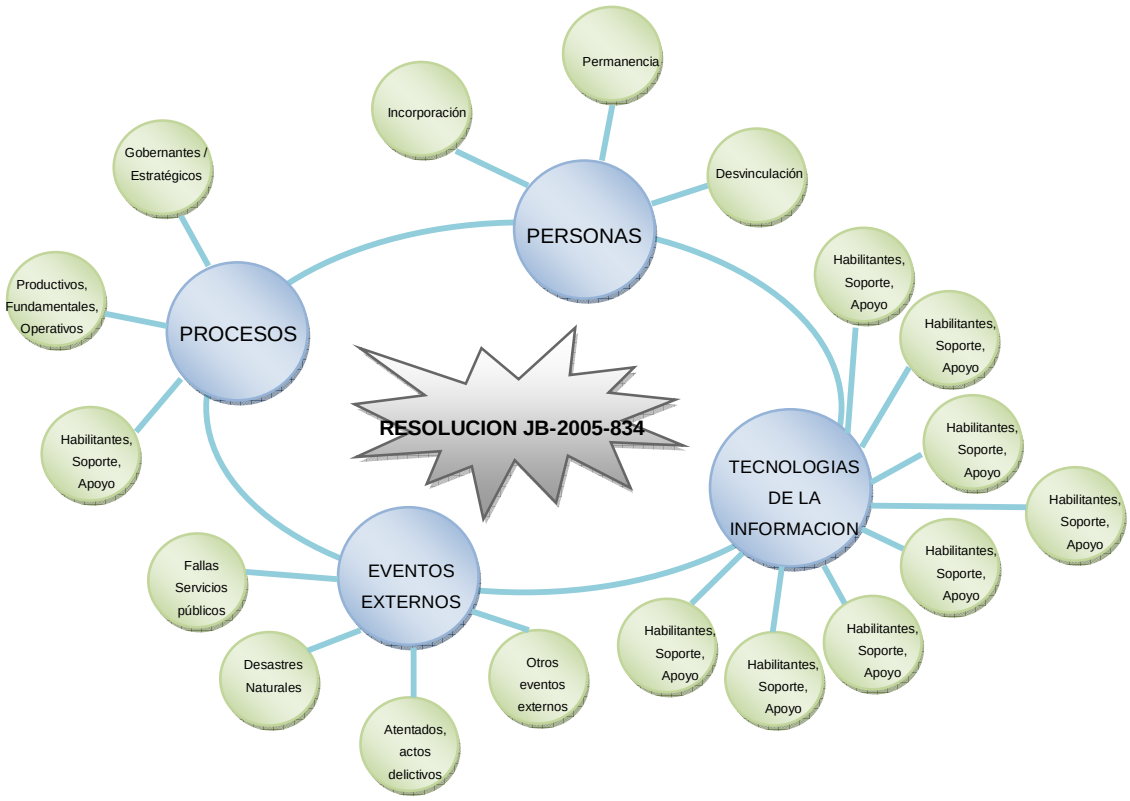


Figura 4 Universo de Resolución JB-2005-834 [6]

Debido a que en ésta resolución uno de los factores de riesgos que afectan las operaciones normales del negocio está inmerso las tecnologías de información, es una de las normas base para la ejecución de los exámenes de auditoría de sistemas. Esta resolución está basada en COBIT 4.1 [2], ITIL 3.0 [7] e ISO 27002:2005 [8].

1.1.5 NORMA TÉCNICA COLOMBIANA NTC 5254 (APLICACIÓN DE AZ-NZS:4360) [9]

La norma técnica Colombiana de gestión del riesgo 5254 es una traducción idéntica de la norma técnica Australiana AS/NZ 4360:2004 de amplia aceptación y reconocimiento a nivel mundial para la gestión de riesgos independiente de la industria o el negocio que desee emplearla. Esta norma establece la recomendación a los administradores de negocios: “La Gestión

de riesgos debe formar parte de la cultura organizacional…quienes gestionan el riesgo de forma eficaz y eficiente tienen más probabilidad de alcanzar sus objetivos y hacerlo a menor costo".

Este Estándar provee una guía genérica para el establecimiento e implementación el proceso de administración de riesgos involucrando el establecimiento del contexto y la identificación, análisis, evaluación, tratamiento, comunicación y el monitoreo en curso de los riesgos.

Esta norma tiene como objeto proporcionar una guía para permitir a cualquier empresa:

- Mejorar la identificación de oportunidades y amenazas
- Tener una base rigurosa para la toma de decisiones y la planificación
- Gestionar de forma proactiva y no reactiva
- Mejorar la conformidad con la legislación pertinente
- Mejorar la gestión de incidentes y la reducción de las pérdidas y el costo del riesgo.

Los principales elementos del proceso de gestión de riesgo, se ilustra en la siguiente figura:

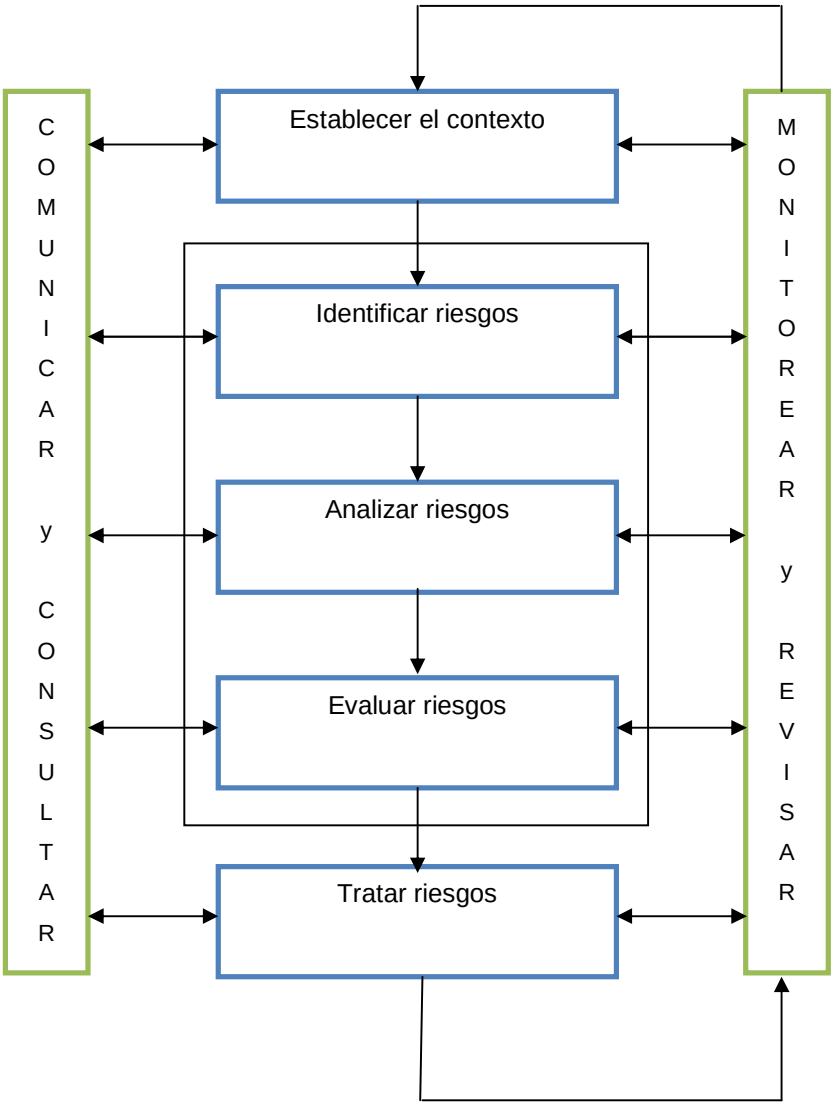


Figura 5 Elementos que conforman el proceso de gestión del riesgo [9]

Comunicación y consulta: Se refiere a comunicar y consultar con interesados internos y externos según corresponda en cada etapa del proceso de administración de riesgos y concerniendo al proceso como un todo.

Establecer el contexto: Se refiere a establecer el contexto interno y externo de la gestión del riesgo en el cual tendrá lugar el resto del proceso.

Identificar riesgos: Establece como identificar el qué, por qué y cómo pueden surgir las cosas como base para análisis posterior.

Analizar riesgos: Determina los controles existentes y así como el análisis de riesgos en términos de consecuencias y probabilidades en el contexto de esos controles. El análisis debe considerar el rango de consecuencias potenciales y cuán probable es que ocurran esas consecuencias. Las consecuencias y probabilidades pueden ser combinadas para producir un nivel estimado de riesgo.

Evaluar riesgos: Significa comparar niveles estimados de riesgos contra los criterios prestablecidos.

1.1.6 RESOLUCIÓN JB-2010-1549 [1]

La resolución JB-2010-1549 fue emitida en Enero del 2010, misma que establece que es necesario reformar las disposiciones para la labor de los auditores internos sobre un enfoque basado en riesgos, empezando con:

“La auditoría basada en riesgos consiste en un conjunto de procesos mediante los cuales la auditoría provee aseguramiento independiente al directorio u organismo que haga sus veces, acerca de:

8.1 Si los procesos y medidas de gestión del riesgo que se encuentran implementadas están funcionando de acuerdo a lo esperado;

8.2 Si los procesos de gestión de riesgos son apropiados y están bien diseñados; y,

8.3 Si las medidas de control de riesgos que la gerencia ha implementado son adecuadas y efectivas, y reducen el riesgo al nivel de tolerancia aceptado por el directorio u organismo que haga sus veces.

La auditoría basada en riesgos depende del nivel de desarrollo que la propia institución del sistema financiero ha alcanzado en la gestión de riesgos en el área objeto de examen, y el grado en que han sido definidos objetivos determinados por la gerencia contra los cuales pueden medirse los riesgos asociados.

Cuando la institución del sistema financiero cuenta con un sistema de gestión del riesgo adecuado en las área bajo examen, sin perjuicio de la necesidad de verificaciones adicionales propias del debido cuidado profesional, la auditoría basada en riesgos puede confiar en mayor grado en la evaluación del riesgo que la propia institución ha realizado, y desarrollar un plan basado en riesgos que complemente las acciones realizadas por la entidad y aumente el valor de las actividades de la auditoría interna.

Cuando la institución del sistema financiero cuenta con un sistema de gestión de riesgos menos desarrollado, la auditoría basada en riesgos requiere descansar más en la evaluación del riesgo que hace la propia auditoría.”

De ésta forma, todas las entidades financieras controladas por la Superintendencia de Bancos deberán efectuar sus revisiones de auditoría interna sobre un enfoque basado en riesgos.

1.1.7 NORMAS ISO 31000 [10]

Todas las actividades de una organización están sometidas de forma permanente a una serie de amenazas, lo cual las hace altamente vulnerables, comprometiendo su estabilidad. Accidentes operacionales, enfermedades, incendios u otras catástrofes naturales, son una muestra de este panorama, sin olvidar las amenazas propias del negocio.

Tradicionalmente, las organizaciones han tratado estos riesgos mediante estrategias de reacción y soluciones puntuales, no obstante, la experiencia ha demostrado que los elementos que conforman los riesgos y los factores que determinan el impacto de sus consecuencias sobre un sistema, son los mismos que intervienen para todos los riesgos en una organización. Por ello, la tendencia moderna es utilizar un enfoque integral de manejo de los mismos conocido como “Enterprise Risk Management” (ERM), con el fin de evaluar, administrar y comunicar estos riesgos de una manera integral, basados en los objetivos estratégicos de la organización.

La gestión integral de riesgos ha ganado impulso en los últimos años, especialmente a partir de la década de los noventa, lo que ha conllevado la aparición de “Modelos de Gestión de Riesgos”, algunos de ellos de carácter más específico, como por ejemplo: COSO ERM II [11] , y otros de carácter más global como la norma AS/NZS 4630 (NTC 5254) [9] o la norma ISO 31000 [10].

El estándar IS0 31000 [10], desarrollado por la ISO (International Organization for Standarization) propone guías genéricas para gestionar los riesgos de forma sistemática y transparente.

El diseño y la implantación de la gestión de riesgos dependen de las necesidades de cada organización de sus objetivos, contexto, estructura, operaciones, procesos operativos, proyectos, servicios, entre otros.

El enfoque se estructura con los siguientes tres elementos:

a. Los principios para la gestión de riesgos.
b. La estructura de soporte.
c. El proceso de gestión de riesgos.

La siguiente figura muestra la relación entre principios de gestión, estructura de soporte y gestión del riesgo.

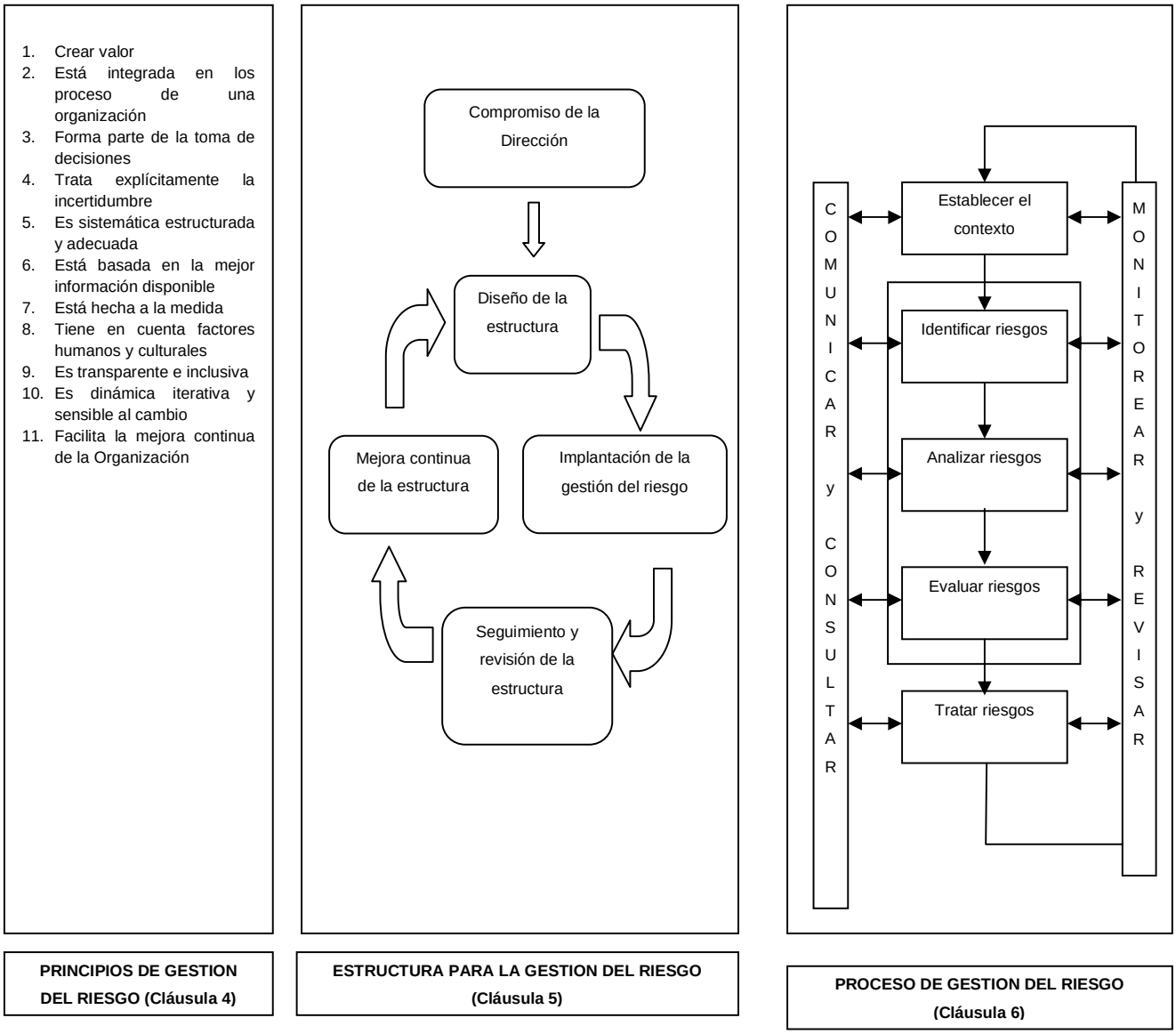


Figura 6 Relación entre principios de gestión, estructura de soporte y gestión del riesgo [14]

1.1.8 COSO ERM II [11]

COSO ERM II ha desarrollado una estructura conceptual para la administración del riesgo empresarial denominada E.R.M. para el entendimiento de la formulación y seguimiento de un proceso básico en la administración del riesgo como apoyo al buen gobierno corporativo y mejores medidas de control en una organización.

La gestión de riesgos corporativos permite a la dirección tratar eficazmente la incertidumbre y sus riesgos y oportunidades asociados, mejorando así la capacidad de generar valor.

El Marco de referencia establece que, maximiza el valor cuando la dirección determina una estrategia y objetivos para encontrar un equilibrio óptimo entre los objetivos de crecimiento y rentabilidad y los riesgos asociados, además, de desplegar recursos de forma eficaz y eficiente a fin de lograr los objetivos de la entidad.

La gestión de riesgos corporativos incluye las siguientes capacidades:

a. Alinear el riesgo aceptado y la estrategia

En la evaluación de alternativas estratégicas, la dirección considera el riesgo aceptado por la entidad, estableciendo los objetivos correspondientes y desarrollando mecanismos para gestionar los riesgos asociados.

b. Mejorar las decisiones de respuesta a los riesgos

La gestión de riesgos corporativos proporciona rigor para identificar los riesgos y seleccionar entre las posibles alternativas de respuesta a ellos: evitar, reducir, compartir o aceptar.

c. Reducir las sorpresas y pérdidas operativas

Las entidades consiguen mejorar su capacidad para identificar los eventos potenciales y establecer respuestas, reduciendo las sorpresas y los costes o pérdidas asociados.

d. Identificar y gestionar la diversidad de riesgos para toda la entidad

Cada entidad se enfrenta a múltiples riesgos que afectan a las distintas partes de la organización y la gestión de riesgos corporativos facilita respuestas eficaces e integradas a los impactos interrelacionados de dichos riesgos.

e. Aprovechar las oportunidades

Mediante la consideración de una amplia gama de potenciales eventos, la dirección está en posición de identificar y aprovechar las oportunidades de modo proactivo.

f. Mejorar la dotación de capital

La obtención de información sólida sobre el riesgo permite a la dirección evaluar eficazmente las necesidades globales de capital y mejorar su asignación.

Estas capacidades, inherentes en la gestión de riesgos corporativos, ayudan a la dirección a alcanzar los objetivos de rendimiento y rentabilidad de la entidad y prevenir la pérdida de recursos. La gestión de riesgos corporativos permite asegurar una información eficaz y el cumplimiento de leyes y normas, además de ayudar a evitar daños a la reputación de la entidad y sus consecuencias derivadas. En suma, la gestión de riesgos corporativos ayuda a una entidad a llegar al destino deseado, evitando baches y sorpresas por el camino.

La siguiente figura muestra los componentes de la Gestión de Riesgos Corporativos:

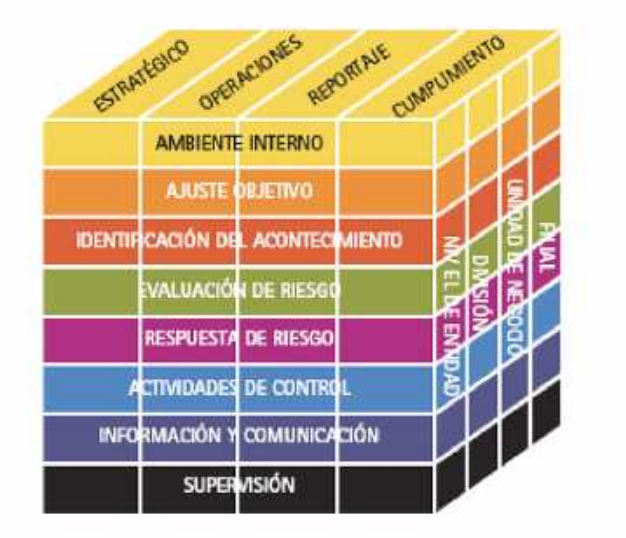


Figura 7 Cubo COSO – ERM II [11]

La gestión de riesgos corporativos consta de ocho componentes relacionados entre sí, que se derivan de la manera en que la dirección conduce la empresa y cómo están integrados en el proceso de gestión. A continuación, se describen estos componentes:

- ✓ Ambiente interno

  Abarca el talante de una organización y establece la base de cómo el personal de la entidad percibe y trata los riesgos, incluyendo la filosofía para su gestión, el riesgo aceptado, la integridad y valores éticos y el entorno en que se actúa.

- ✓ Establecimiento de objetivos

  Los objetivos deben existir antes de que la dirección pueda identificar potenciales eventos que afecten a su consecución. La gestión de riesgos corporativos asegura que la dirección ha establecido un proceso para fijar objetivos y que los objetivos seleccionados apoyan la misión de la entidad y están en línea con ella, además de ser consecuentes con el riesgo aceptado.

- ✓ Identificación de eventos

  Los acontecimientos internos y externos que afectan a los objetivos de la entidad deben ser identificados, diferenciando entre riesgos y oportunidades. Estas últimas revierten hacia la estrategia de la dirección o los procesos para fijar objetivos.

- ✓ Evaluación de riesgos

  Los riesgos se analizan considerando su probabilidad e impacto como base para determinar cómo deben ser gestionados y se evalúan desde una doble perspectiva, inherente y residual.

- ✓ Respuesta al riesgo

  La dirección selecciona las posibles respuestas - evitar, aceptar, reducir o compartir los riesgos - desarrollando una serie de acciones para alinearlos con el riesgo aceptado y las tolerancias al riesgo de la entidad.

- ✓ Actividades de control

  Las políticas y procedimientos se establecen e implantan para ayudar a asegurar que las respuestas a los riesgos se llevan a cabo eficazmente.

- ✓ Información y comunicación

  La información relevante se identifica, capta y comunica en forma y plazo adecuado para permitir al personal afrontar sus responsabilidades. Una comunicación eficaz debe producirse en un sentido amplio, fluyendo en todas direcciones dentro de la entidad.

- ✓ Supervisión

  La totalidad de la gestión de riesgos corporativos se supervisa, realizando modificaciones oportunas cuando se necesiten. Esta supervisión se lleva a

cabo mediante actividades permanentes de la dirección, evaluaciones independientes o ambas actuaciones a la vez.

La gestión de riesgos corporativos no constituye estrictamente un proceso en serie, donde cada componente afecta sólo al siguiente, sino un proceso multidireccional e iterativo en que casi cualquier componente puede influir en otro.

1.1.9 BASILEA II [12]

El Comité de Basilea es un organismo Internacional, conformado por la alta gerencia de los bancos centrales de: Alemania, Bélgica, Canadá, EEUU., Francia, Italia, Japón, Holanda, Reino Unido, Suecia, Suiza, Luxemburgo y España, el que ha emitido acuerdos y directrices para el funcionamiento de entidades financieras.

En 1988 se publicó el primer acuerdo de Basilea que se centraba en varias directrices que regulaba el capital mínimo que debía disponer una entidad financiera frente a los riesgos asociados.

Desde el año 2007 está vigente el acuerdo de Basilea II el cual se enfoca en los siguientes tres pilares fundamentales:

Mínimos requerimientos de capital: establece los requerimientos de capital basados en los riesgos de mercado, crédito y operacional.

Revisión de Supervisor: se enfoca en la auditabilidad y transparencia de una entidad financiera a través de la supervisión cualitativa del proceso interno del control de riesgos a través de organismos de control Internos y Externos.

Disciplina de Mercado: establece que debe ser asumida por la entidad financiera, mediante la publicación de reportes al público respecto a su situación financiera y control de riesgos.

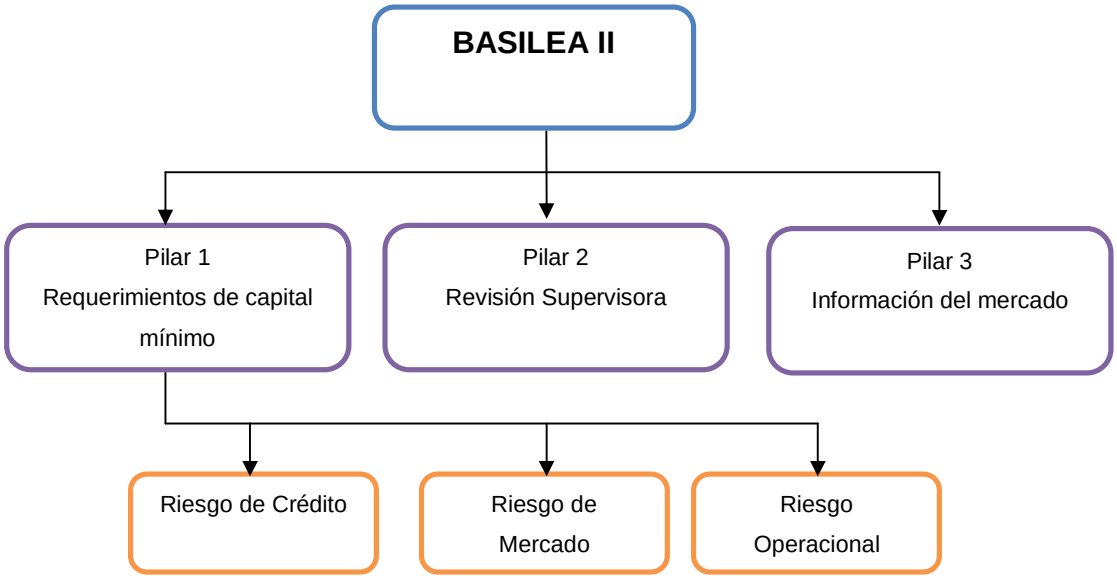


Figura 8 Pilares BASILEA II [12]

1.1.10 COBIT 4.1 [2]

COBIT 4.1, fue lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de TI. COBIT 4.1 vincula la tecnología informática y prácticas de control, consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

El marco de trabajo COBIT 4.1 se aplica a todos los sistemas de información, está basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

La misión de COBIT 4.1 es investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes y auditores.

Los usuarios del sistema COBIT 4.1 son:

La Gerencia: para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.

Los Usuarios Finales: quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.

Los Auditores: para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido.

Los Responsables de TI: para identificar los controles que requieren en sus áreas.

También puede ser utilizado dentro de las empresas por el responsable de un proceso de negocio en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de la TI en las empresas.

El estándar tiene las siguientes características:

- ✓ Orientado al negocio
- ✓ Alineado con estándares y regulaciones "de facto"
- ✓ Basado en una revisión crítica y analítica de las tareas y actividades en TI
- ✓ Alineado con estándares de control y auditoría (COSO ERM II, IFAC, IIA, ISACA, AICPA)

La estructura conceptual se puede enfocar desde tres puntos de vista:

a. Los criterios empresariales que deben satisfacer la información
b. Los recursos de las TI
c. Los procesos de TI

Los criterios deben considerar los requerimientos de información: de Calidad, fiduciarios y de seguridad.

Requerimientos de Calidad: Calidad, Costo y Entrega.

Requerimientos Fiduciarios: Efectividad y Eficiencia operacional, Confiabilidad de los reportes financieros y Cumplimiento le leyes y regulaciones.

Efectividad: La información debe ser relevante y pertinente para los procesos del negocio y debe ser proporcionada en forma oportuna, correcta, consistente y utilizable.

Eficiencia: Se debe proveer información mediante el empleo óptimo de los recursos (la forma más productiva y económica).

Confiabilidad: proveer la información apropiada para que la administración tome las decisiones adecuadas para manejar la empresa y cumplir con sus responsabilidades.

Cumplimiento: de las leyes, regulaciones y compromisos contractuales con los cuales está comprometida la empresa.

Requerimientos de Seguridad: Confidencialidad, Integridad y Disponibilidad

Confidencialidad: Protección de la información sensible contra divulgación no autorizada

Integridad: Refiere a lo exacto y completo de la información así como a su validez de acuerdo con las expectativas de la empresa.

Disponibilidad: accesibilidad a la información cuando sea requerida por los procesos del negocio y la salvaguarda de los recursos y capacidades asociadas a la misma.

En COBIT 4.1 se establecen los siguientes recursos en TI necesarios para alcanzar los objetivos de negocio:

Aplicaciones: Incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.

Información: Son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.

Infraestructura: es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.

Personas: son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.

La estructura de COBIT 4.1 se define a partir de una premisa simple y pragmática: "Los recursos de las Tecnologías de la Información (TI) se han de gestionar mediante un conjunto de procesos agrupados de forma natural para que proporcionen la información que la empresa necesita para alcanzar sus objetivos".

COBIT 4.1 se divide en tres niveles:

1. **Dominios:** Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.
2. **Procesos:** Conjuntos o series de actividades unidas con delimitación o cortes de control.
3. **Actividades:** Acciones requeridas para lograr un resultado medible.

La siguiente figura muestra la relación entre procesos de TI, Criterios de información y recursos requeridos:

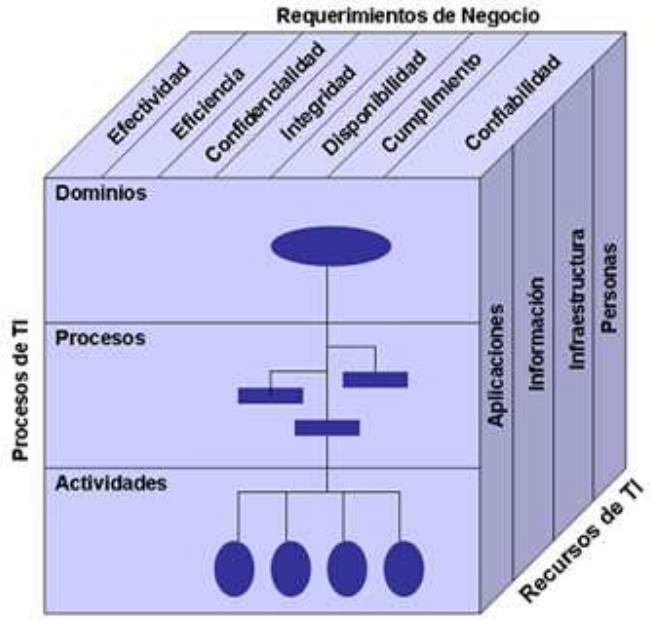


Figura 9 Cubo COBIT 4.1 [2]

COBIT 4.1 define las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios: Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar. Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear.

La figura siguiente consolida los 4 dominios de COBIT 4.1:

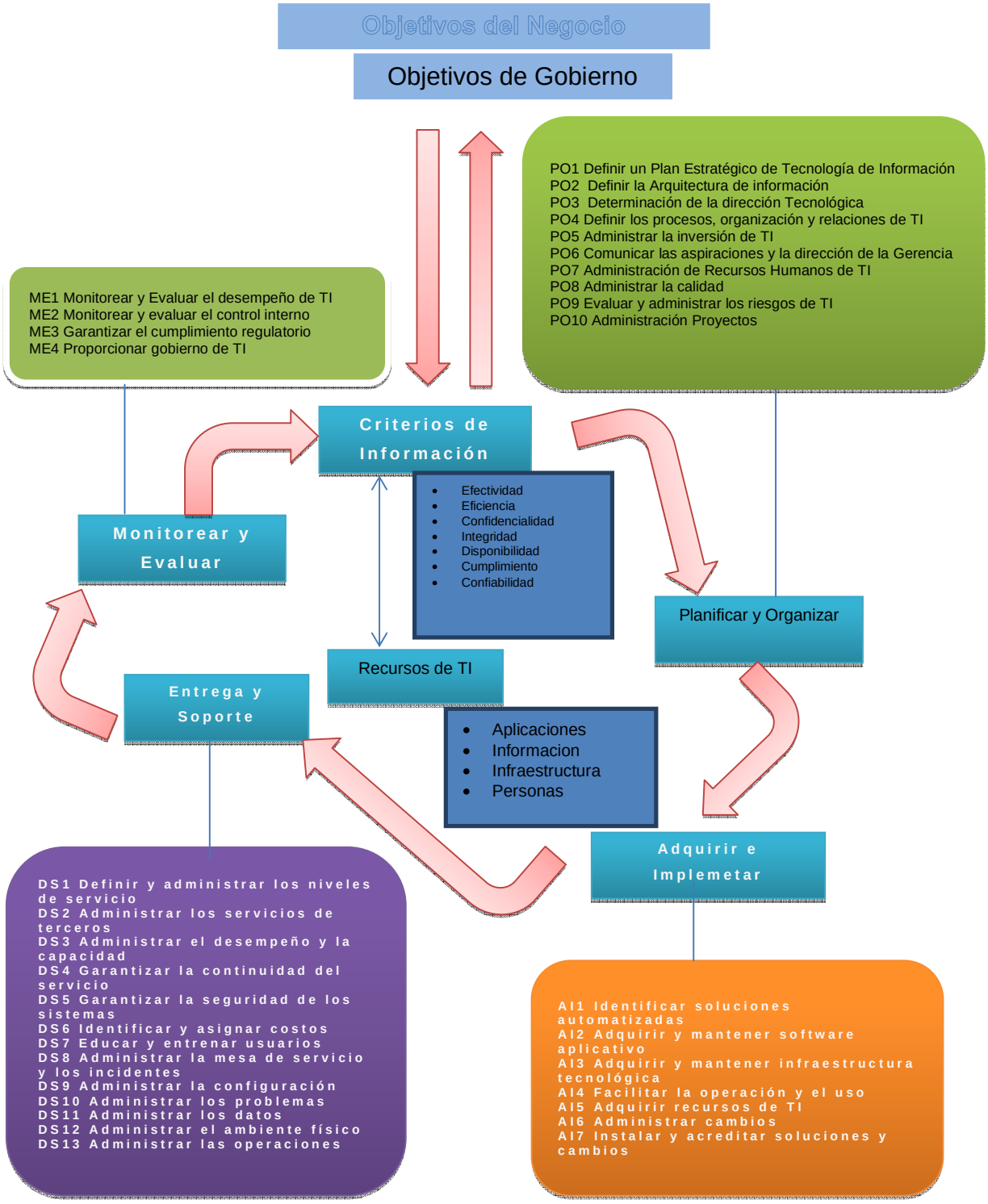


Figura 10 Marco de trabajo COBIT 4.1 [2]

A continuación se describen los 4 dominios del estándar COBIT 4.1.

1.1.10.1 Planificación y organización

Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos de negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas. Para este dominio se considera 11 procesos.

1.1.10.2 Adquisición e implementación

Para llevar a cabo la estrategia de TI, las soluciones de Ti deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes. Para este dominio se considera 7 procesos.

1.1.10.3 Prestación y soporte

En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación. Para este dominio se considera 13 procesos.

1.1.10.4 Monitoreo y Evaluación

Todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad. Este es,

precisamente, el ámbito de este dominio. Para este dominio se considera 4 procesos.

1.1.11 GUÍAS DE AUDITORÍA (IT ASSURANCE GUIDE) [13]

Las guías de Auditoría o aseguramiento permiten la revisión de los procesos establecidos en COBIT 4.1 [2] como guía de mejores prácticas de TI, a fin de garantizar su cumplimiento y efectuar recomendaciones para el mejoramiento continuo si la Institución ha decidido su implementación. Los Auditores de S.I. deben tener como base las guías de auditoría al determinar cómo se va a lograr la implementación de los estándares por parte de la Administración de TI, además, debe utilizar un buen juicio profesional con respecto a su utilización y estar dispuesto a justificar algún tipo de desviación en el cumplimiento de estos estándares.

Las guías de aseguramiento proporcionan una guía detallada de actividades que pueden ser efectuadas por los profesionales de TI para cada uno de los 34 procesos de TI, las cuales proporcionan controles genéricos que se aplican a todos los procesos, de aplicación y específicos; medidas de garantía y directrices para probar el diseño y control de los objetivos de control, el resultado del objetivo de control (eficacia de las operaciones), deficiencia en la documentación y su impacto.

Los usuarios deben estar familiarizados con los conceptos del COBIT 4.1 [2] a fin de entender la aplicación de las guías, así como tener un buen nivel de conocimiento en tecnologías de información y seguridad informática.

Las guías de aseguramiento de TI proporciona consejos de garantía en diferentes niveles, a nivel de procesos, a nivel de procesos específicos, además, proporcionan asesoramiento sobre la forma de comprobar si los objetivos de control se están cumpliendo y la forma de documentar las deficiencias del control.

En el ámbito de los objetivos de control, las guías de aseguramiento ofrecen medidas de garantía para probar el diseño de control para cada objetivo de control basado en las prácticas de control interno de TI.

Para los pasos de prueba de la fase de ejecución, esta guía ofrece una orientación de carácter general, así como de carácter específico.

Una visión general del marco de referencia en el que se basa este proceso se muestra en la siguiente figura:

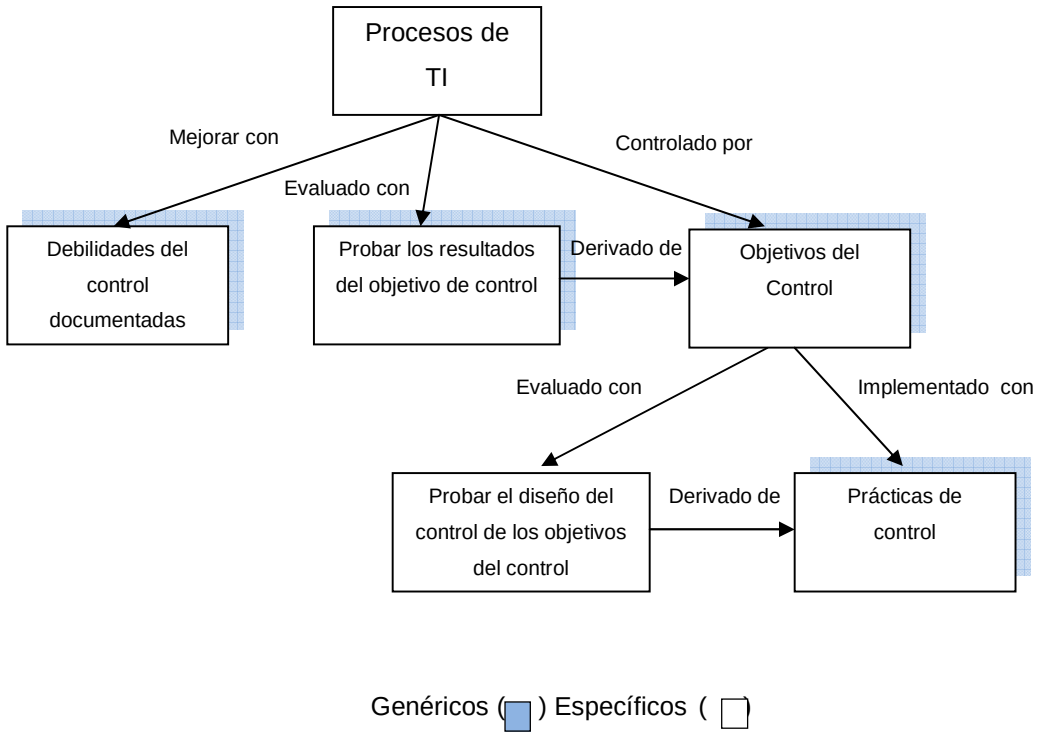


Figura 11 Consejos de Aseguramiento provistos por las guías [13]

1.1.11.1 Relación con las prácticas de control COBIT 4.1 [2]

Las guías de Aseguramiento de TI es parte de la familia de productos COBIT 4.1.

Los procesos de TI de COBIT 4.1, los requerimientos del negocio y los objetivos de control definen lo que hay que hacer para implementar una estructura de control eficaz.

Las prácticas de control de COBIT 4.1 ofrecen una guía más detallada a nivel de objetivo de control sobre la manera de alcanzar los objetivos.

Para cada uno de los objetivos de control, se ha establecido una lista de prácticas específicas a efectuarse, mismas que sirven para lograr el objetivo de control.

También proporcionan orientación de alto nivel genérico, en un nivel más detallado a fin de evaluar la madurez del proceso, teniendo en cuenta las posibles mejoras e implementación de los controles.

Hoja de ruta

Las principales secciones o títulos de la hoja de ruta son:

- Planificación
- Alcance
- Ejecución, que incluye:
  - Perfeccionamiento de la comprensión del tema seguridad de TI
  - Refinación del alcance de los objetivos de control clave
  - Prueba de la efectividad del diseño de control
  - Prueba de los resultados de los objetivos de control clave
  - Documentar el impacto de las debilidades de control
  - Desarrollar / comunicar las conclusiones y recomendaciones

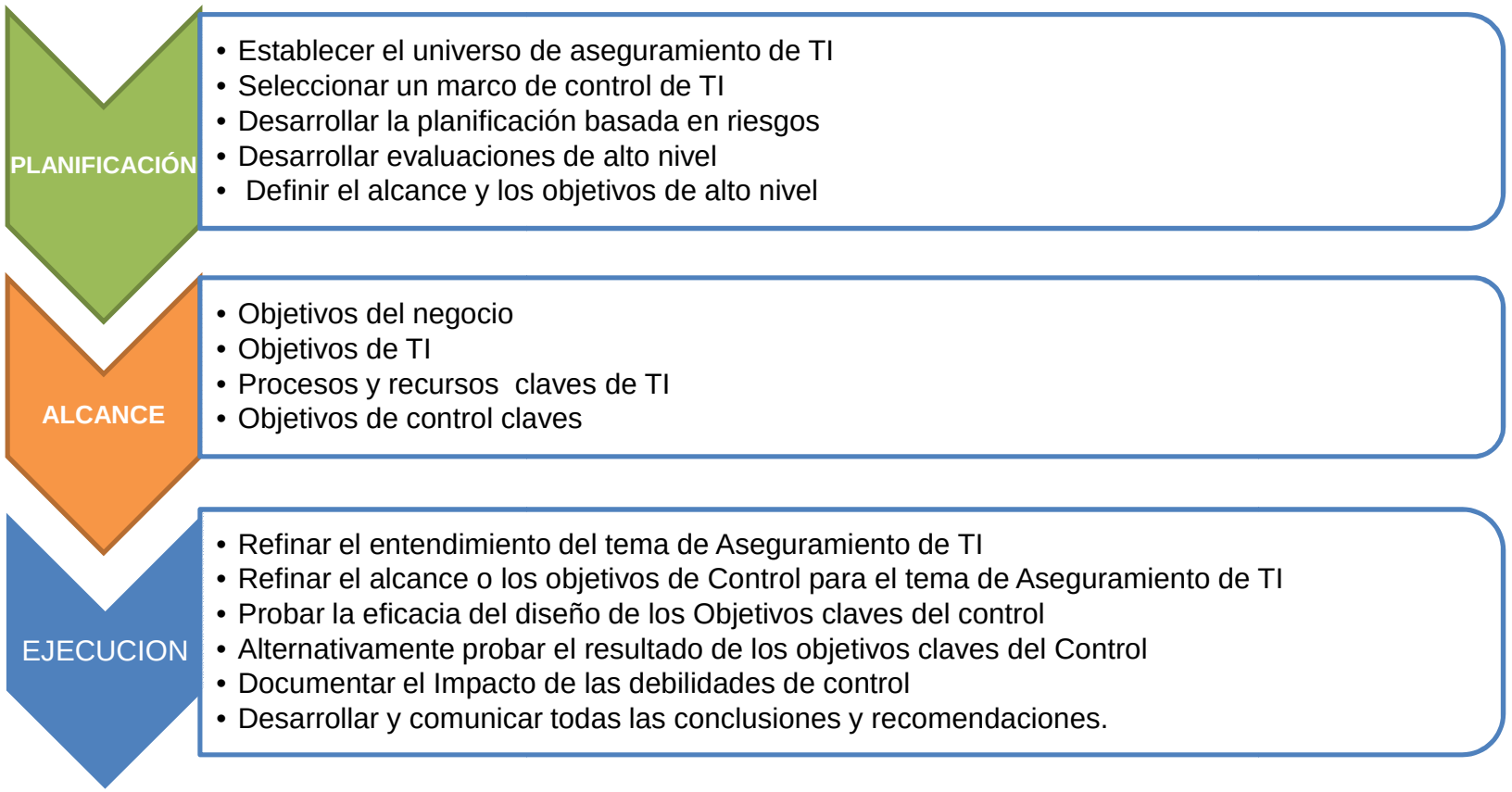


Figura 12 Hoja de ruta – Aseguramiento de TI

✓ **Planificación**

La creación del universo de auditoría de TI, es el inicio de todas las iniciativas de aseguramiento. Al crear un plan integral, el profesional de aseguramiento debe combinar una comprensión del universo y aseguramiento de TI, a través de la selección de un marco de control adecuado de TI, tal como COBIT 4.1. La suma de estos dos criterios permite la adecuada planificación basada en riesgos.

Para establecer los objetivos de garantía correcta, en primer lugar se debe realizar una evaluación de alto nivel, como resultado de esta etapa se entrega el plan anual de auditoría.

✓ **Alcance**

La determinación del alcance se puede realizar de tres formas diferentes:

- El enfoque de alcance más detallado se inicia desde la definición de los objetivos de negocio y de TI para el medio ambiente bajo análisis y la identificación de un conjunto de procesos y recursos de TI, necesarios para apoyar estos objetivos. Los objetivos que están sujetos a las iniciativas de TI puede establecerse hasta un nivel específico.
- Un enfoque de alto nivel de evaluación puede partir de la investigación de referencia ejecutado por ITGI (Instituto de Gobierno de TI), quien ha proporcionado directrices genéricas sobre la relación de los objetivos de negocio, los objetivos de TI y procesos de TI, como se describe en COBIT 4.1. [2] Esta cascada genérica de los objetivos y los procesos pueden ser utilizados como una base de información más detallada del alcance, como se requiere para el entorno específico que se está evaluando.
- Un enfoque híbrido combina los métodos de determinación del alcance detallado y de alto nivel. Este enfoque parte de la cascada

de los objetivos genéricos y procesos, pero se adapta y modifica el medio específico donde se desarrolla, antes de continuar con la definición del alcance de los niveles más detallados.

- ✓ **Ejecución**

  La tercera etapa de la hoja de ruta es la ejecución, aquí se describen todas las actividades que el profesional de auditoría debe seguir como medidas de control. A continuación la descripción:

  - Refinar el entendimiento del sujeto del aseguramiento de TI
  - Refinar el alcance de los objetivos claves de control para el aseguramiento de TI
  - Probar la eficacia del diseño del control de los objetivos claves de control
  - Adicionalmente, probar los resultados de los objetivos claves de control
  - Documentar el impacto de las debilidades del control
  - Desarrollar y comunicar todas las conclusiones y recomendaciones.

1.1.12 AUDIT & ASSURANCE GUIDANCE [14]

El propósito de las guías de auditoría es especificar las normas que un Auditor de Sistemas debe seguir a fin de efectuar los exámenes de auditoría basándose en los siguientes factores:

- ✓ Estatuto regulatorio,
- ✓ Independencia profesional,
- ✓ Ética y estándares profesionales,
- ✓ Competencia profesional,
- ✓ Planeación,
- ✓ Ejecución de la auditoría,

- ✓ Reporte,
- ✓ Actividades de seguimiento,
- ✓ Irregularidades y acciones legales,
- ✓ Gobernabilidad de TI,
- ✓ Uso de la evaluación de riesgos en la planeación de auditoría,
- ✓ Materialidad de la auditoría,
- ✓ Uso del trabajo de otros expertos,
- ✓ Evidencia de auditoría,
- ✓ Controles de TI,
- ✓ Comercio electrónico.

1.1.13 PROCESS ASSESSMENT MODEL , USING COBIT 4.1 (PAM) [4]

El modelo PAM está basado en COBIT 4.1[2] y en el estándar ISO/IEC 15504 [15], el cual está orientado a la evaluación de procesos de desarrollo de software basado en el antigua Modelo de Capacidad de Madurez (CMM–Capability Maturity Model/SPICE). El PAM fue desarrollado por la necesidad de mejorar la fiabilidad de la evaluación de los procesos de Tecnología de información.

El modelo sirve como una referencia de base para la realización de evaluaciones de la capacidad de los procesos actuales de Tecnología, además permite:

- ✓ Definir el conjunto mínimo de requisitos para llevar a cabo una evaluación para asegurar que los resultados de los procesos evaluados sean consistentes, repetibles y representativos.

- ✓ Definir la capacidad del proceso en dos dimensiones, desempeño y capacidad de los procesos, utilizando material definido en COBIT 4.1, niveles de capacidad de evaluación y atributos de proceso, definidos en la

norma ISO / IEC 15504-2, la capacidad del proceso e indicadores de desempeño determinan si los atributos del proceso se han logrado o no.

- ✓ Medir el desempeño del proceso a través de un conjunto de prácticas comunes y actividades necesarias para cumplir con los resultados del proceso, así como entradas y salidas del proceso.

- ✓ Medir la capacidad del proceso en base a la evaluación del atributo a través de la evidencia de prácticas específicas y genéricas.

- ✓ Reconocer que la evaluación del proceso puede ser un motor fuerte y eficaz para la mejora de los procesos.

El modelo puede ser utilizado para evaluar los niveles de capacidad de procesos de TI y efectuar mejoras en estos, además, para que auditores y consultores de TI realicen auditorías o evaluaciones de la capacidad de determinados procesos.

La siguiente figura muestra los niveles de madurez a evaluar:

	Nivel 1 Realizado	Nivel 2 Gestionad	Nivel 3 Establecid	Nivel 4 Predecible	Nivel 5 Optimizado
PA 5.2 OPTIMIZACIÓN PA 5.1 INNOVACIÓN					L / F
PA 4.2 CONTROL PA 4.1 MEDIDA				L / F	F
PA 3.2 DESPLIEGUE PA 3.1 DEFINICIÓN				F	F
PA 2.2 GESTION DEL PRODUCTO DE TRABAJO PA 2.1 GESTION DEL DESEMPEÑO		L / F	F	F	F
PA 1.1 DESEMPEÑO DEL PROCESO	L / F	F	F	F	F

Figura 13 Niveles de Madurez – ISO 15504 [17]

Los valores derivados de las evaluaciones que utiliza este modelo incluyen resultados fiables que centran a la empresa en el riesgo, beneficios, recursos, consecuencias que se derivan de la ejecución y proporcionan una base sólida para la evaluación comparativa y mejora, priorización y planificación de los proceso de TI.

1.1.14 ITAF™ – A PROFESSIONAL PRACTICES FRAMEWORK FOR IT ASSURANCE [3]

El marco de referencia ITAF™ es un modelo de buenas prácticas, el cual:

- ✓ Proporciona orientación sobre el diseño, realización y presentación de informes de auditorías de TI.

- ✓ Define los términos y conceptos específicos para las evaluaciones de los procesos de TI.
- ✓ Establece las normas que se ocupan de las auditorías de los procesos de TI, así como la evaluación de los roles y responsabilidades, conocimientos y habilidades de los profesionales de TI.

ITAF [3]se centra en el material de ISACA, así como el contenido y la orientación desarrollada por el IT Governance Institute ® (ITGI™) y otras organizaciones, y como tal, ofrece un sola fuente a través del cual, los profesionales de auditoría y aseguramiento pueden buscar orientación, sobre políticas de investigación y procedimientos, de cómo obtener programas de auditoría y aseguramiento, y elaborar informes eficaces.

1.2 PROCESO DE AUDITORÍA

Actualmente el proceso de auditoría Informática sigue un enfoque tradicional, es decir, valida el cumplimiento de normas políticas y procedimientos con en apoyo de marcos de referencia de manera aislada, sin tener un sustento que haga relación entre ellos a través de un modelo particular, a continuación se muestra el proceso actual de la Auditoría Informática:

Figura 14 Proceso actual Auditoría Informática

1.2.1 ANÁLISIS ESTRATÉGICO

El análisis estratégico le permite al Auditor determinar el alcance de la auditoría a realizarse por lo tanto, es importante, considerar todos los aspectos a evaluar en el examen a efectuarse. A continuación los pasos a seguir:

1. Revisar todos los aspectos relacionados con el tema:

- Disposiciones legales y normativas
- Procedimientos internos, políticas y controles
- Flujos o documento narrativo del proceso

2. Revisar los comentarios de las auditorías anteriores realizadas por auditoría interna y externa y organismos de control (Superintendencia de Bancos y Seguros).

3. Listar de forma general todos los aspectos, actividades, procesos o tareas que comprende el área a auditarse. Luego agrupar en subtemas utilizando el programa de auditoría.

4. Solicitar todos los instructivos y normativa interna y externa sobre el tema a revisar.

5. Elaborar la plantilla de control que detalla las actividades inmersas en el proceso, los controles existentes, mismos que deben ser evaluados considerando la importancia de cada actividad frente al impacto que tendría de no cumplirse. También debe incluir la muestra considerada con la identificación del número tareas cumplidas adecuadamente y el número de no cumplidas. Se debe valorar el nivel de control existente, obteniendo de riesgo existente.

1.2.2 ANÁLISIS DE LOS PROCESOS

Para iniciar el análisis de los proceso a evaluarse, se debe informar a la jefatura de todas las áreas que intervienen en el proceso a auditarse sobre la revisión a realizar, indicando el enfoque y los objetivos que se ha planteado, además se deberá requerir otros aspectos de interés que la jefatura considere deben ser revisados. A continuación los pasos a seguir:

1. Coordinar con la jefatura para que direccione al personal a quien solicitar

la información requerida.

2. Evaluar la información entregada por los responsables
3. Evaluar los controles existentes y que afectan directamente al proceso que están siendo auditado
4. Realizar las pruebas contempladas en el programa, de ser necesario y dependiendo del tamaño de la muestra y del alcance de las pruebas, elaborar papeles de trabajo específicos.
5. Si los procesos son automatizados, evalúe los controles establecidos frente a riesgos de accesos indebidos, seguridad, integridad y confiabilidad en los procesos de la información, respaldos, existencia de pistas de auditoría, segregación de funciones, transacciones acordes al nivel que aprueba, segregación entre registro, ejecución y autorización, existencia de respaldos especialmente si se trata de transacciones en cuentas de clientes, etc.
6. Evaluar la productividad del proceso, determinando si no existen reprocesos, pasos innecesarios o que toman demasiado tiempo su ejecución y que pueden estar afectando al servicio y por ende al costo.
7. En la medida que vaya determinando hallazgos y recomendaciones, preparar y presentar los reportes correspondientes.
8. Obtener las respuestas de los auditados.

En esta fase, el Auditor debe aplicar las técnicas de auditoría que le permitan al auditor obtener evidencias necesarias y suficientes, con el objeto de formarse un juicio profesional y objetivo de la materia que se examina.

1.3 PROCEDIMIENTOS ACTUALES DE LA AUDITORÍA INFORMATICA

Los temas desarrollados a continuación fueron tomados del Manual de Auditoría informática perteneciente a la Institución financiera que servirá como caso de estudio para el presente trabajo.

1.3.1 ALCANCE DEL TRABAJO DE AUDITORÍA

La auditoría informática se enfoca a las siguientes áreas:

- Auditoría a sistemas de información
- Auditoría de redes y telecomunicaciones
- Auditoría de la seguridad de la información
- Auditoría de la continuidad de las operaciones
- Auditoría de adquisición e implementación de infraestructura
- Auditoría de planeación y organización de TI
- Auditoría de servicios de terceros
- Auditoría de entrega de servicios

1.3.2 METODOLOGÍA DE AUDITORÍA INFORMÁTICA

La auditoría informática puede ser general o específica. Si se examina temas complejos resulta evidente mayor cantidad de esfuerzo y tiempo destinados para la revisión. Cuando el tema es específico, se contempla solo los particulares que afectan a la revisión y se obtiene más rápidamente los resultados.

La metodología que se utiliza actualmente en las auditorías informáticas TI están basadas en el marco de referencia COBIT 4.1 [2] a un nivel básico tomando en cuenta únicamente el uso de las mejores prácticas de tecnología de información que pueden contribuir al correcto desempeño de los procesos relacionados.

1.3.3 TÉCNICAS

- Análisis de la información recopilada a través de entrevistas o encuestas
- Análisis de la información obtenida de los auditados
- Cruce de la información recopilada vs. La obtenida
- Simulación de procesos auditados
- Muestreo

1.3.4 HERRAMIENTAS

- Cuestionarios
- Checklist’s
- ACL (herramienta de evaluación de datos).
- Excel
- SQL (consultas)

1.3.5 METODOLÓGIA ACTUAL

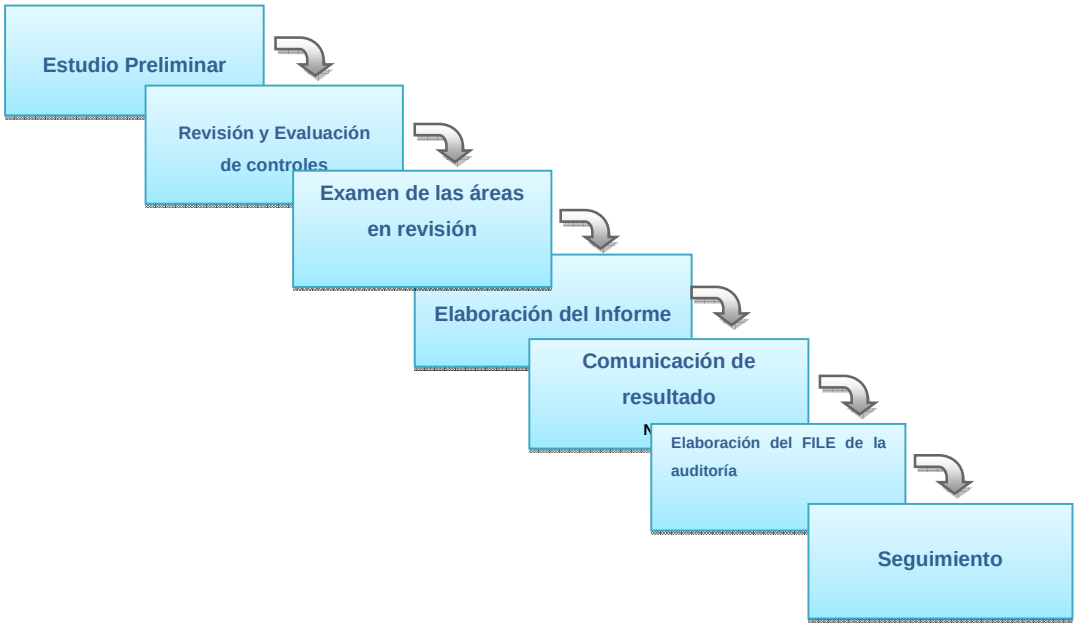


Figura 15 Metodología Auditoría de Sistemas

1.3.5.1 Estudio preliminar

- Comunicar a los funcionarios involucrados sobre el inicio del examen
- Entrevistar a los funcionarios involucrados
- Obtener información básica en base a la entrevista
- Obtener manuales, instructivos, reglamentos, actas y documentación relacionada a la revisión.
- Solicitar plan de actividades y verificar el cumplimiento
- Solicitar el detalle de la configuración del hw o sw relacionado con la revisión

- Solicitar el detalle de todo el personal involucrado en el proceso bajo revisión
- Solicitar contratos relacionados

1.3.5.2 Revisión y evaluación de controles y seguridades

- Revisar la documentación obtenida (manuales, normas, instructivos, metodologías) y verificar su cumplimiento y su vigencia.
- Analizar procedimientos, políticas y manuales y comprobar que se hayan elaborado en base a normas y estándares internacionales.

1.3.5.3 Examen de las áreas bajo revisión

- Efectuar el análisis de problemas encontrados de forma cualitativa y cuantitativa, a través de, pruebas de cumplimiento y pruebas sustantivas.
- Tomar muestras y analizar el cumplimiento. El tamaño de las muestras depende del volumen y la complejidad de la información, si la población es pequeña se debe analizar sobre toda la muestra, si es mediana se tomará el 50% de la población total, y si es grande en volumen se analizará el 10% de la población total.
- Obtener copias de reportes, formatos de pantallas
- Elaborar papeles de trabajo para evidenciar los errores encontrados
- Usar normas y estándares, como referencia de las mejores prácticas de TI.

1.3.5.4 Elaboración del informe

Elaborar el informe de la revisión, el cual debe contener:

a. Objetivos

b. Alcance

c. Resultados de la revisión

d. Recomendaciones

e. Conclusiones

1.3.5.5 Comunicación de resultados

Dar lectura del informe a los ejecutivos de la Cooperativa a fin de poner en conocimiento los hallazgos y recomendaciones del examen.

1.3.5.6 Elaboración del file de auditoría

Consolidar toda la información recopilada durante el examen en un file, el cual debe contener: índice, programa de auditoría, informe final, informe borrador, papeles de trabajo, evidencia, procedimientos relacionados.

1.3.5.7 Seguimiento

Examinar la revisión previa para adquirir un claro conocimiento del tema que se va a dar seguimiento a fin de retomar conceptos e información que en un determinado momento fueron factores de análisis y revisión y de esta forma determinar si el grado de cumplimiento es satisfactorio o requiere atención para su ejecución.

1.3.5.8 Criterio para el mejoramiento

De lo expuesto sobre el procedimiento actual de la auditoría informática se observa que está orientado sobre el enfoque tradicional de cumplimiento, por

lo tanto, como la normativa de la Superintendencia de Bancos resuelve que los exámenes de auditoría deben efectuarse sobre un enfoque basado en riesgos, como se propone en el siguiente capítulo.

CAPÍTULO 2. DESARROLLO DEL MODELO PARA EFECTUAR AUDITORÍAS INFORMÁTICAS BASADAS EN RIESGOS

2.1 ENFOQUE DEL MODELO

El enfoque aplicado por una Institución es diferente a otra, y depende de la iniciativa o necesidad del Auditor. El presente trabajo se fundamenta en normas, estándares, marcos de referencia nacionales e internacionales que rigen la gestión de las TIC's, todos ellos descritos en el capítulo I de este documento, además, se soporta en guías de aseguramiento y auditoría de sistemas de información, modelos de evaluación de procesos y buenas prácticas para el diseño, realización y elaboración de informes, sin las cuales no fuese posible el desarrollo del modelo, objeto del presente trabajo.

El modelo que se propone contiene cuatro fases: Planificación, Definición del Alcance, Ejecución y Monitoreo; este enfoque agrupa las actividades de la auditoría basada en riesgos, aspecto que permite el desarrollo ordenado de los exámenes de auditoría.

Las actividades contenidas en cada una de las fases mencionadas fueron elaboradas específicamente para construir un modelo a la medida en el que se incluye el diseño de formularios, esquemas, informes, y otros documentos necesarios para la ejecución de las auditorías.

A continuación se muestra un esquema completo del modelo, objetivo principal del presente trabajo:

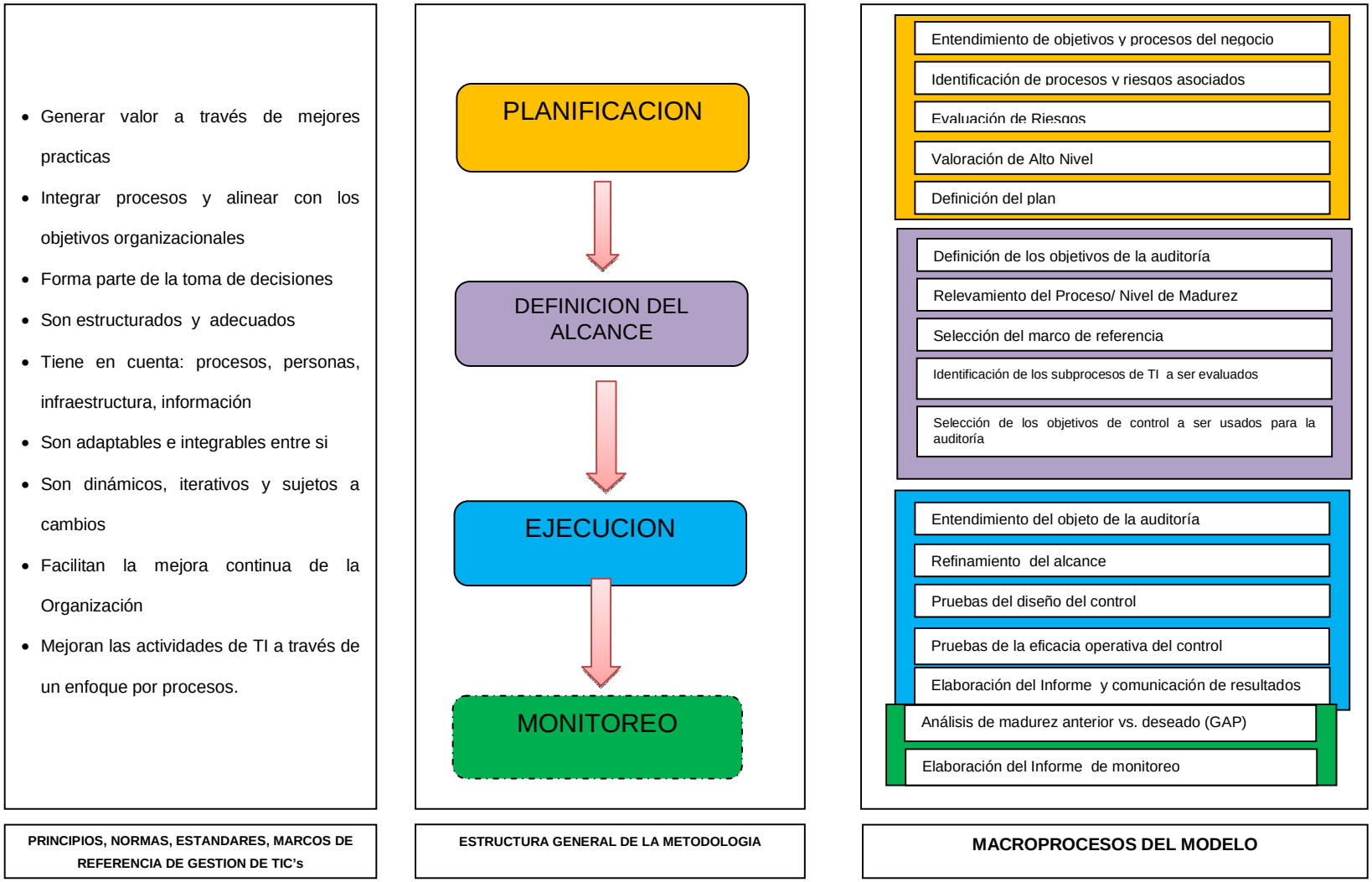


Figura 16 Enfoque del Modelo

2.1.1 PLANIFICACIÓN

Para crear un plan de auditoría basada en riesgos, el Auditor requiere un entendimiento completo del ambiente de TI que contempla: plan estratégico, procesos, recursos, información, aplicaciones, infraestructura, personas y los riesgos asociados.

Una vez adquirido el conocimiento general del ambiente de TI, se efectúa la valoración de alto nivel, la cual se basa en criterios de riesgos debidamente formulados y ponderados por la Alta Gerencia.

A continuación se exponen detalladamente los pasos para la elaboración de la planificación basada en riesgos, cuyo entregable es el plan anual de auditoría.

2.1.1.1 Entendimiento de objetivos y procesos del negocio

La planificación de la auditoría basada en riesgos requiere una comprensión completa sobre la cadena de valor, los objetivos y procesos del negocio, mismos que están relacionados estrechamente y sobre los cuales la Institución ha establecido su modelo de negocio, por lo tanto, su comprensión integral es básica.

El conocimiento del modelo del negocio puede ser efectuado de arriba hacia abajo (top-down) o desde abajo hacia arriba (botton-up), dependiendo del criterio del auditor.

Además, del conocimiento del modelo del negocio se requiere un conocimiento sobre la misión, visión, valores, estrategias, planes operativos, productos y servicios, entre otros, es decir, el plan estratégico institucional.

Los procesos del negocio deben ser identificados, considerando la cadena de valor a nivel de la Institución, por lo tanto, con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, se debe contar con procesos definidos en conformidad con la estrategia y las políticas

adoptadas, que deberán ser agrupados, conforme lo establecido en la resolución de riesgo operativo. [6]

Procesos gobernantes o estratégicos: Se considerarán a aquellos que proporcionan directrices a los demás procesos y son realizados por el Directorio y la alta Gerencia para poder cumplir con los objetivos y políticas institucionales. Se refieren a la planificación estratégica, lineamientos de acción básicos, estructura organizacional, administración integral de riesgos, entre otros;

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

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

En una organización el Control Interno juega un papel importante, el cual proporciona una garantía razonable para el logro de los objetivos institucionales clasificados en las siguientes categorías:

Estrategia: Objetivos a alto nivel, alineados con la misión de la entidad y dándole apoyo

Operaciones: Objetivos vinculados al uso eficaz y eficiente de recursos

Información: Objetivos de fiabilidad de la información suministrada

Cumplimiento: Objetivos relativos al cumplimiento de leyes y normas aplicables

Esta clasificación permite a la Institución centrarse en aspectos diferenciadores para una adecuada gestión de riesgos; enfocarse en necesidades que pueden ser de responsabilidad directa de diferentes ejecutivos, además, establecer las diferencias de lo que se espera de cada una de ellas.

La fiabilidad de la información y el cumplimiento de leyes y normas están enmarcados dentro del control interno de una Institución, aspecto que permite que la gestión de riesgos corporativos facilite la seguridad razonable para la consecución de los objetivos institucionales.

La cultura organizacional permitirá conocer los valores corporativos, creencias, costumbres, ideales, criterios, etc. que los integrantes de una organización tienen en común.

El conocimiento de la capacidad instalada de la Institución es un factor preponderante para el conocimiento de la organización, en esta se contempla infraestructura, tecnología, instalaciones, recursos con lo que la empresa cuenta para lograr sus objetivos.

Los aspectos mencionados anteriormente tales como objetivos, metas, estrategias, modelo del negocio, control interno, cultura organizacional y capacidad instalada pueden verse afectados por factores de riesgo internos que probablemente incidan el logro de los objetivos organizacionales, los cuales pueden ser minimizados o mitigados a través de una adecuada gestión; la siguiente figura muestra el esquema relacionado:

Figura 17 Conocimiento de la organización sobre factores internos de riesgo [18]

Además, el conocimiento de la organización abarca varias consideraciones, las cuales no deben ser relegadas, sino más bien tomadas en cuenta como se indica en la figura siguiente:

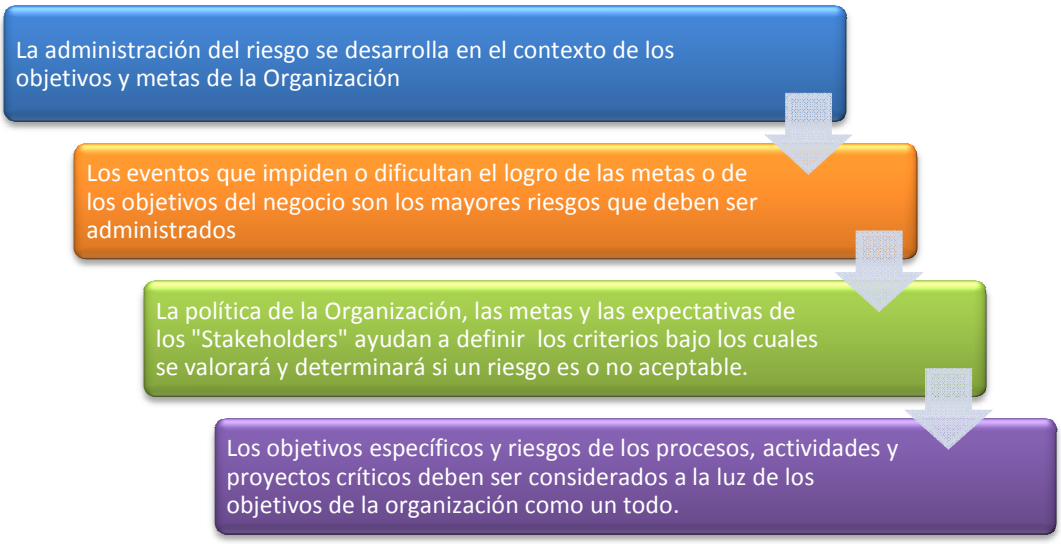


Figura 18 Criterios de riesgos [16]

2.1.1.2 Identificación de procesos y riesgos asociados

Una vez entendidos los objetivos y procesos del negocio se procede con la identificación de los riesgos asociados los cuales pueden impedir el logro de los objetivos institucionales. La adecuada comprensión de los riesgos del negocio es un factor determinante que le permitirá al Auditor Interno agregar valor a la organización a través de los exámenes de auditoría aplicados a los diferentes subprocesos institucionales. A continuación, se muestra un ejemplo en la siguiente figura:

DESCRIPCION PROCESO				
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	Incremento de la productividad del área por retrasos en las entregas de equipos y servidores que dilatan otras actividades del personal del IT. debido a actividades ya establecidas o calendarizadas al personal de IT que no cumplen con los tiempos establecidos
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	Incremento en los costos de operación por los equipos que deben ser retornados al área de IT para su revisión por preparación errónea o instalaciones no adecuadas que no dan el funcionamiento que el usuario requiere, además, se preparan equipos y servidores sin tomar en cuenta la funcion que va a desempeñar el mismo
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	Incremento en los costos de operación. Por Los equipos no funcionan adecuadamente . por las fallas en el Sistema Operativo. los sistemas operativos se corrompen o han sido instalados o manipulados de forma errónea

Figura 19 Relación entre objetivos y riesgos

2.1.1.3 Evaluación de Riesgos

La evaluación de riesgos, para fines de la elaboración del plan de auditoría, debe ser en base a lo establecido por una unidad gestora de la Institución que se encargue específicamente de la administración de riesgos, de ser necesario y conforme lo considere el Auditor la evaluación de riesgos deberá complementarse con su opinión. Por ejemplo, la definición de un esquema de mapa de riesgos donde se reflejen los riesgos identificados por la Institución en base a su impacto y probabilidad. Además, se puede considerar el siguiente esquema para la valoración de riesgos tomando en cuenta la relación con los atributos de los objetos involucrados: activos, amenazas, agente de amenaza, evento de amenaza, vulnerabilidad, contramedidas, riesgo residual.

A continuación, se muestra la relación entre los diferentes componentes del análisis de riesgos y los atributos principales, en la siguiente figura:

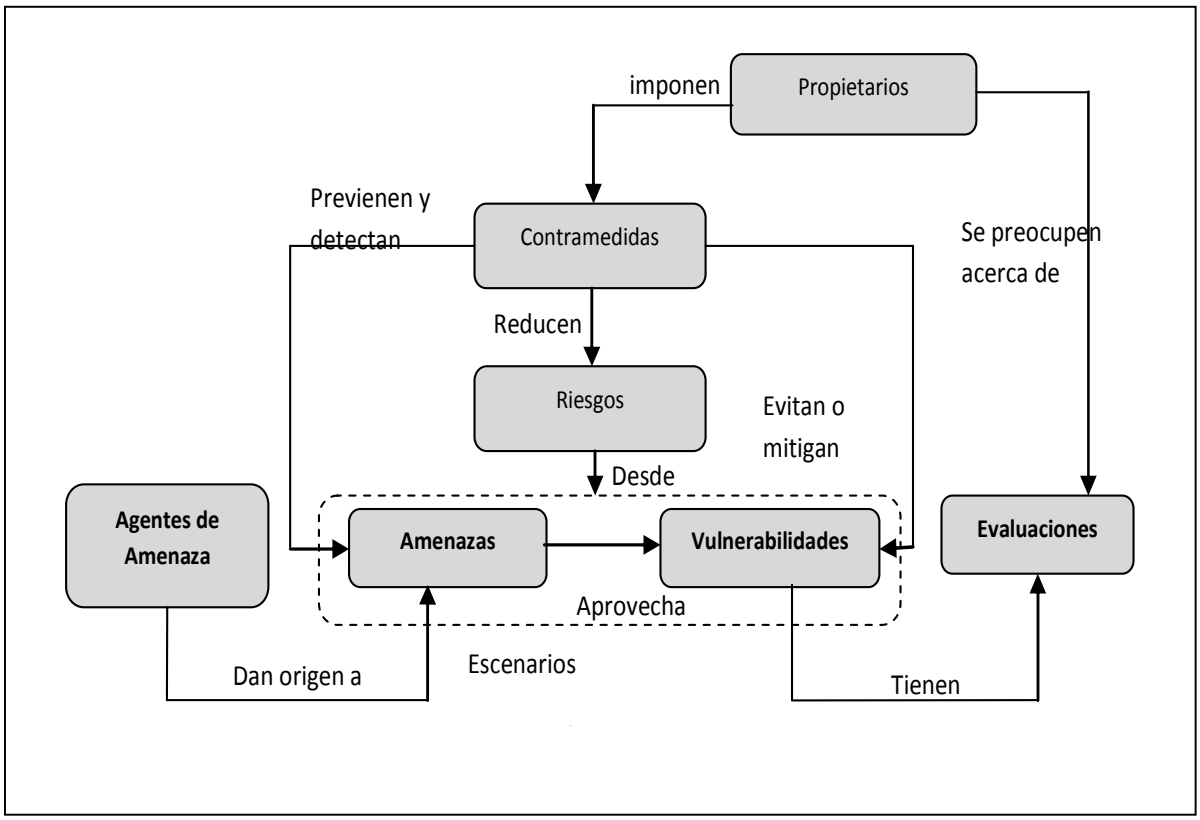


Figura 20 Atributos y Componentes de riesgos [14]

A continuación se muestra un esquema general de la evaluación de riesgos en base a impacto y probabilidad, como observamos en la siguiente figura:

DESCRIPCION PROCESO					IMPACTO	PROBABILIDAD	RIESGO	No. de Controles	CONTROL
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo					
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	Incremento de la productividad del área por retrasos en las entregas de equipos y servidores que dilatan otras actividades del personal del IT. debido a actividades ya establecidas o calendarizadas al personal de IT que no cumplen con los tiempos establecidos	2	2	4	1	Solicitud de preparación de equipos y servidores en el F11
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	Incremento en los costos de operación por los equipos que deben ser retornados al área de IT para su revisión por preparación errónea o instalaciones no adecuadas que no dan el funcionamiento que el usuario requiere, además, se preparan equipos y servidores sin tomar en cuenta la funcion que va a desempeñar el mismo	2	2	4	1	Acta de entrega recepción de equipos con el destinatario y función a cumplir

Figura 21 Ejemplo de Evaluación de riesgos

2.1.1.4 Valoración de Alto Nivel

Una valoración de alto nivel proporciona un apoyo a la planificación mediante la identificación de los procesos y el nivel de riesgo asociado. Para lograr determinar la valoración de alto nivel es necesario la participación de la Alta Gerencia, la cual proporcionará los factores de riesgo y su respectiva ponderación.

Para el levantamiento de los criterios o factores de riesgos es importante considerar ciertas características que permitan reconocerlos dentro de la organización, tales como:

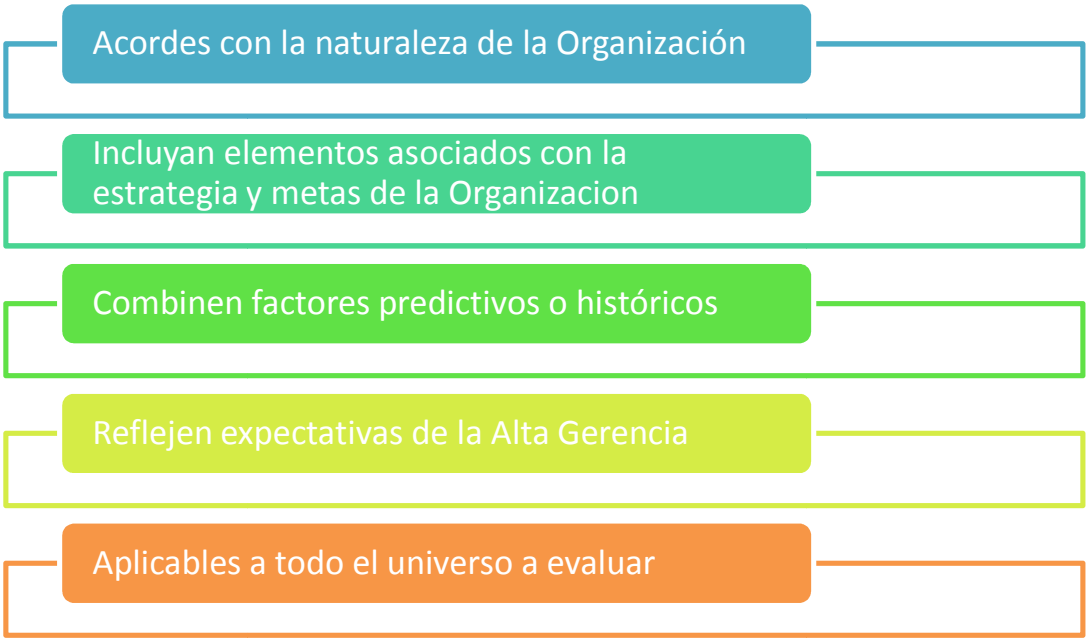


Figura 22 Características de los Factores / Criterios de Riesgo

También se debe determinar e identificar los rangos y puntajes para cada criterio, utilizando una mínima valoración semi-cuantitativa y asignando un peso para cada uno de ellos.

Los factores de riesgos pueden considerar aspectos tales como: insatisfacción de los empleados, restructuraciones, complejidad y volumen de las transacciones, tamaño del proceso, requisitos legales, estabilidad y eficacia del control interno, cambios en la Organización, fraudes, entre otros. Ver la figura siguiente:

CRITERIO 1	1
Insatisfacción de los empleados	
Baja	1
Media	2
Alta	3

CRITERIO 2	1
Reestructuraciones	
No hubo cambios	1
Cambios moderados	2
Cambios Significativos	3

CRITERIO 3	1
Fraudes	
No hubo fraudes	1
Fraudes pequeños	2
Fraudes moderados	3
Fraudes significativos	4

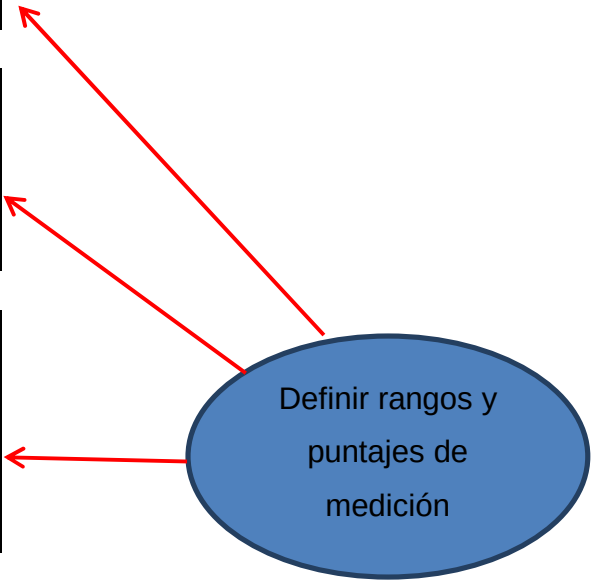


Figura 23 Ejemplo de Factores de Riesgos I [19]

CRITERIO 1	1
Insatisfacción de los empleados	
Baja	1
Media	2
Alta	3

CRITERIO 2	1
Reestructuraciones	
No hubo cambios	1
Cambios moderados	2
Cambios Significativos	3

CRITERIO 3	1
Fraudes	
No hubo fraudes	1
Fraudes pequeños	2
Fraudes moderados	3
Fraudes significativos	4

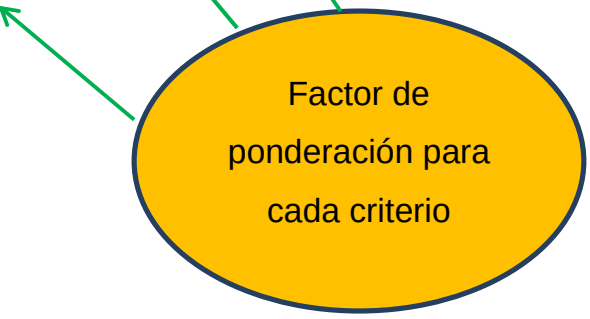


Figura 24 Ejemplo de Factores de Riesgos II [19]

La ponderación de esta valoración permitirá la priorización de los procesos que deberán incluirse en el plan de auditoría.

Los resultados de la evaluación de alto nivel son el fundamento para el plan de auditoría que permite dar prioridad al trabajo de auditoría de TI.

2.1.1.5 Definición del plan

Para definir el plan de auditoría se debe considerar el análisis entre procesos y riesgos priorizando los que obtuvieron mayor valoración, esto permitirá generar las actividades de auditoría a considerarse en el plan anual, para finalmente asignar el tiempo y los recursos disponibles. Además, se tomará en cuenta la carga de trabajo de los auditores para efectuar las siguientes asignaciones de actividades de auditoría, es decir, actividades predecesoras.

El plan de auditoría basado en riesgos debe ser actualizado anualmente y estar alineado con la gestión de riesgos institucionales. A continuación una muestra del plan de auditoría anual en la figura siguiente:

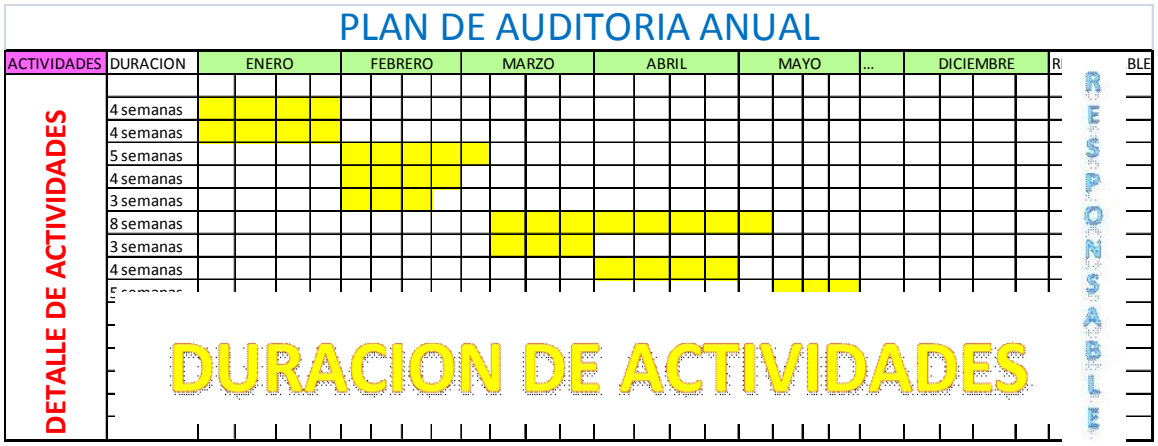


Figura 25 Ejemplo 1 Plan de Auditoría Anual

Otra forma de presentar el plan de auditoría anual, es con el apoyo de herramientas de gestion de proyectos tal como Microsoft Project o Open Proj, ejemplo se muestra en la siguiente figura:

Actividades	Duración	Inicio	Fin	Predecesoras	Recursos
Definic. Plan Estrategico y Operativo	20 días	02/01/2012 9:00	27/01/2012 19:00		Ing. Juan Pérez
Estructura y Responsabilidades TI	20 días	02/01/2012 9:00	27/01/2012 19:00		Ing. María López
Gestión de Proyectos	30 días	30/01/2012 9:00	09/03/2012 19:00	1	Ing. Juan Pérez
Inventario de Harware y Software	20 días	30/01/2012 9:00	24/02/2012 19:00	2	Ing. María López
Gestión de Cambios	30 días	12/03/2012 9:00	20/04/2012 19:00	3	Ing. Juan Pérez
Enlaces y comunicaciones	25 días	27/02/2012 9:00	30/03/2012 19:00	4	Ing. María López
Help Desk	16 días	23/04/2012 9:00	14/05/2012 19:00	5	Ing. Juan Pérez
Respaldos	16 días	02/04/2012 9:00	23/04/2012 19:00	6	Ing. María López
Base de Datos	40 días	15/05/2012 9:00	09/07/2012 19:00	7	Ing. Juan Pérez
Seguridades Físicas y Lógicas	30 días	24/04/2012 9:00	04/06/2012 19:00	8	Ing. María López
Aplicaciones de Operaciones	25 días	10/07/2012 9:00	13/08/2012 19:00	9	Ing. Juan Pérez
Monitoreo y Evaluación de TI	20 días	05/06/2012 9:00	02/07/2012 19:00	10	Ing. María López
Gestión de Adquisiciones	25 días	14/08/2012 9:00	17/09/2012 19:00	11	Ing. Juan Pérez
Administrac. y Mantenim. de Infraestruct. y Activos Fijos	25 días	03/07/2012 9:00	06/08/2012 19:00	12	Ing. María López
Manejo y Administración de Archivos	20 días	18/09/2012 9:00	15/10/2012 19:00	13	Ing. Juan Pérez
Gestión de Seguridad Administrativa	30 días	07/08/2012 9:00	17/09/2012 19:00	14	Ing. María López
Adquisición y mantenimiento de Infraestructura	35 días	16/10/2012 9:00	03/12/2012 19:00	15	Ing. Juan Pérez
Estructura y Responsabilidades de TI	30 días	18/09/2012 9:00	29/10/2012 19:00	16	Ing. María López
Seguimientos	25 días	30/10/2012 9:00	03/12/2012 19:00	18	Ing. María López
Vacaciones Ing. María López	20 días	04/12/2012 9:00	31/12/2012 19:00	19	Ing. María López
Vacaciones Ing. Juan Pérez	20 días	04/12/2012 9:00	31/12/2012 19:00	17	Ing. Juan López

Figura 26 Ejemplo 2 Plan de Auditoría Anual

2.1.2 DEFINICIÓN DEL ALCANCE

La definición del alcance y los objetivos de la auditoría son de suma importancia, porque a través de esto se establece hasta qué punto el Auditor efectuará el examen de auditoría, es decir, establece los límites de la auditoría a fin de evitar exceder las expectativas de los auditados. En los párrafos siguientes se detallan las actividades que permitan lograr una adecuada definición del alcance, reflejado en el siguiente esquema:

Plan Anual de Auditoría

Figura 27 Definición del alcance

2.1.2.1 Definición de los objetivos de la auditoría

De acuerdo a las asignaciones de las actividades de auditoría, el Auditor responsable debe establecer claramente los objetivos y alcance del examen, además, debe realizar una evaluación preliminar del objeto de revisión, con el fin de ofrecer una seguridad razonable de que todos los componentes serán adecuadamente cubiertos durante el proceso de auditoría. El auditor debe apoyarse en el marco de referencia de prácticas profesionales para el aseguramiento de TI (ITAF™) [3], además de las Guías de Aseguramiento y las Prácticas de Control de ISACA [5].

2.1.2.2 Relevamiento del Proceso

Una vez definidos los objetivos y alcance de la auditoría, el Auditor debe tener un acercamiento inicial con el dueño del proceso, a fin de obtener un conocimiento claro del proceso a evaluarse, por lo que deberá coordinar una reunión en la cual se releven todas las actividades ligadas a este proceso, producto de esta tarea, el auditor obtiene un conocimiento general del proceso de TI a evaluarse.

Además, es importante obtener el nivel de madurez del proceso a fin de valorar los objetivos de control asociados, basados en el modelo PAM [4].

Obtención del Nivel de Madurez

Para obtener el nivel de madurez del proceso a ser evaluado, el Auditor debe considerar el Modelo de Evaluación de un Proceso (PAM – Process Assessment Model), el cual permite valorar la madurez actual del proceso a través de varios criterios que debe cumplir y apoyándose en evidencias que aseguran que la capacidad del proceso sea confiable y consistente.

El modelo es bidimensional, en la primera se definen y clasifican por categorías los procesos, es la dimensión de los procesos (basado en COBIT 4.1 [2]) y en la segunda se define la dimensión de la capacidad, basada en

atributos del proceso cuyo cumplimiento establece el nivel de capacidad en el que se encuentra el proceso evaluado, como se indica en la siguiente figura:

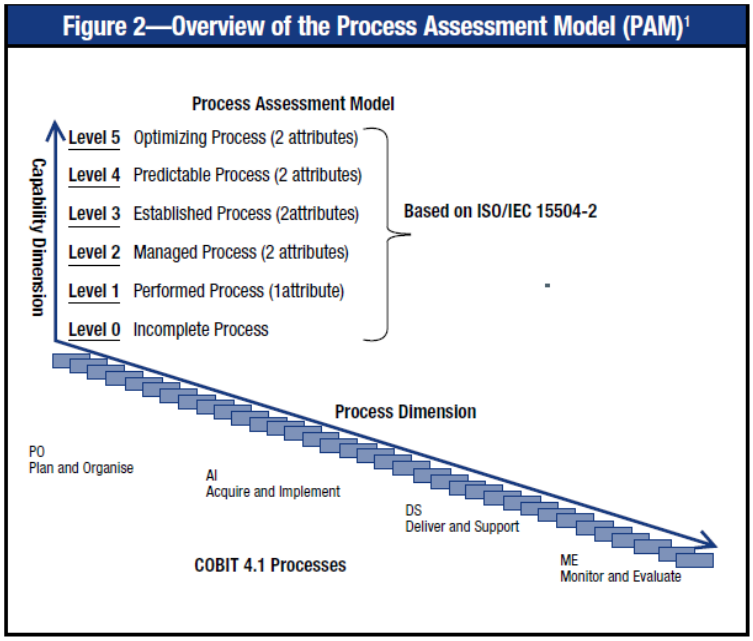


Figura 28 Modelo PAM [4]

En la dimensión del proceso el modelo usa COBIT 4.1 [2] como referencia, el cual provee definiciones de los procesos en un ciclo de vida, organizados en 4 dominios: Planificación y Organización (PO), Adquisición e Implementación (AI), Entrega y Soporte (DS), y Monitoreo y Evaluación (ME). Para mayor información sobre este marco de referencia referirse al Capítulo I.

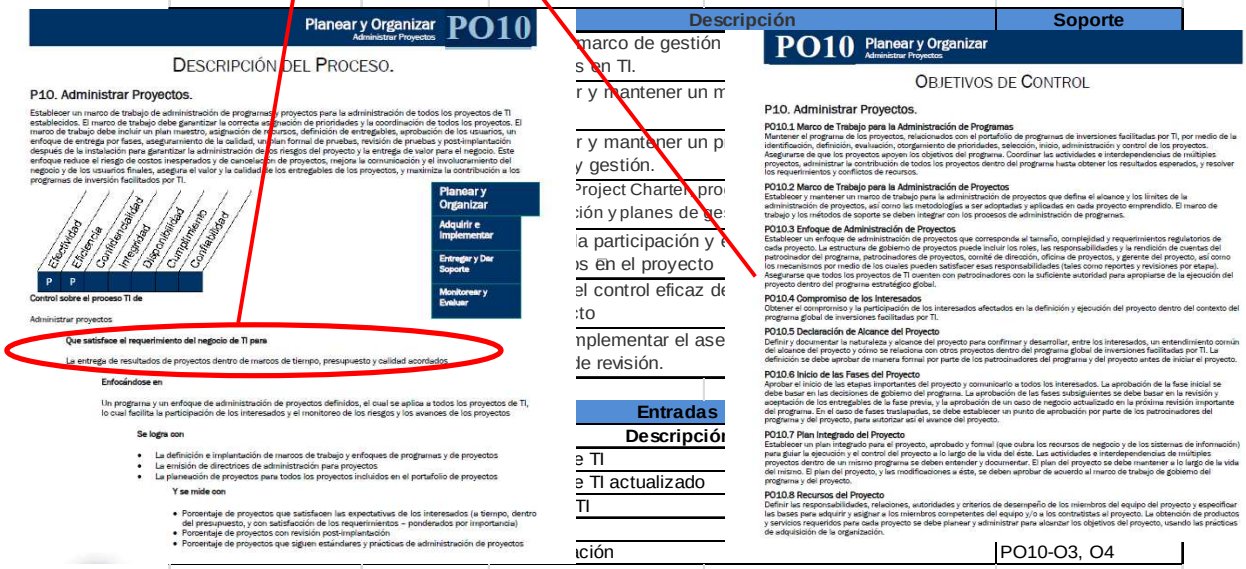
La dimensión de la capacidad provee una medida de la madurez del proceso evaluado. La capacidad se expresa en términos de atributos agrupados en niveles de capacidad, los cuales abarcan dos tipos de indicadores:

- **De Desempeño del proceso:** Proveen un valor de referencia a partir de cual se puede establecer una comparación; son específicos para cada proceso y se utiliza para determinar si un proceso está en el nivel 1.

Para evaluar este tipo de indicadores, los procesos evaluados se describen en términos de: nombre del proceso, propósito y resultados (Os), basados en COBIT 4.1 [2]; prácticas base (PBs) que son tareas y actividades necesarias para llevar a cabo el proceso y obtener resultados; productos de trabajo de entrada y salida (WPs) asociado con cada proceso.

A continuación la explicación de los términos mencionados en el párrafo anterior:

Nombre del Proceso	Administración de Proyectos	
Propósito	Cumplir con los requisitos de negocio para asegurar la entrega de los resultados del proyecto dentro plazos acordados, presupuesto y calidad.	
Resultados (Os)	Número	Descripción
	PO10-O1a	Esta definido un marco de gestión del programa?
	PO10-O1b	Se sigue un marco de gestión del programa?
	PO10-O1c	Se logró los resultados esperados con las contribuciones de los proyectos dentro del programa?
	PO10-O1d	Se gestionan actividades, interdependencias, necesidades de recursos y conflictos de varios proyectos?
	PO10-O2a	Se ha definido un marco de gestión de proyectos?
	PO10-O2b	Los proyectos siguen un proceso de gestión de proyectos que requieren aprobaciones adecuadas, gestión, gestión de calidad y la supervisión?
	PO10-O3	La planificación del proyecto se realiza para cada proyecto y se detalla en la cartera de proyecto?
	PO10-O4	Existe compromiso y participación del negocio y usuarios finales en los proyectos?

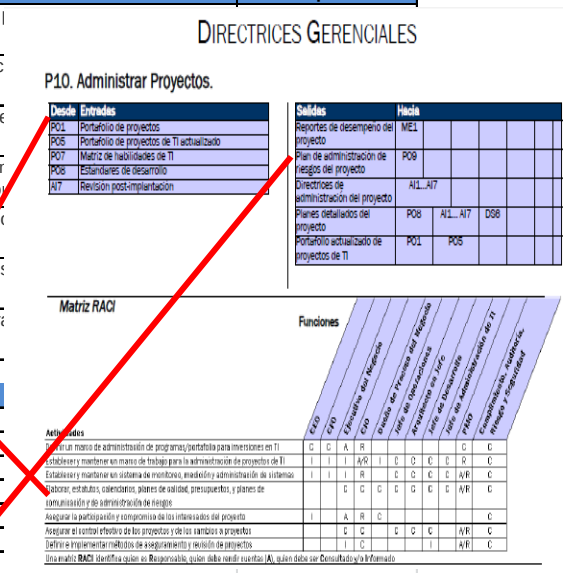


Salidas			
Número	Descripción	Entrada al	Soporte
PO10-WP1	Reportes de desempeño del proyecto	ME1	PO10-O1b, O1d, O4
PO10-WP2	Plan de gestión de riesgos de proyectos	PO9, AI3	PO10-O1c, O1d, O3
PO10-WP3	Guias de gestion de proyectos	AI1 al AI7	PO10-02, 03
PO10-WP4	Planes de proyectos detallados	PO8, AI1 al AI7, DS6	PO10-O1c, O3
PO10-WP5	Portafolio de proyectos de TI actualizados	PO1, PO5	PO10-01, O3

Figura 29 Esquema de evaluación del desempeño de un proceso parte I [4]

Nombre del Proceso	Administración de Proyectos	
Propósito	Cumplir con los requisitos de negocio para asegurar la entrega de los resultados del proyecto dentro plazos acordados, presupuesto y calidad.	
Resultados (Os)	Número	Descripción
	PO10-O1a	Esta definido un marco de gestión del programa?
	PO10-O1b	Se sigue un marco de gestión del programa?
	PO10-O1c	Se logró los resultados esperados con las contribuciones de los proyectos dentro del programa?
	PO10-O1d	Se gestionan actividades, interdependencias, necesidades de recursos y conflictos de varios proyectos?
	PO10-O2a	Se ha definido un marco de gestión de proyectos?
	PO10-O2b	Los proyectos siguen un proceso de gestión de proyectos que requieren aprobaciones adecuadas, gestión, gestión de calidad y la supervisión?
	PO10-O3	La planificación del proyecto se realiza para cada proyecto y se detalla en la cartera de proyecto?
	PO10-O4	Existe compromiso y participación del negocio y usuarios finales en los proyectos?

Prácticas Base (BPs)	Número	Descripción	Soporte
	PO10-BP1	Definir un marco de gestión de inversiones en TI.	
	PO10-BP2	Establecer y mantener un marc TI.	
	PO10-BP3	Establecer y mantener un proye medición y gestión.	
	PO10-BP4	Construir Project Charter, prograr comunicación y planes de gestió	
	PO10-BP5	Asegurar la participación y el c interesados en el proyecto	
	PO10-BP6	Asegurar el control eficaz de los del proyecto	
	PO10-BP7	Definir e implementar el asegura métodos de revisión	



Entradas	
Número	Descripción
PO1-WP3	Portafolio de proyectos de TI
PO5-WP4	Portafolio de proyectos de TI actualizado
PO7-WP2	Matriz de habilidades de TI
PO8-WP2	Estandares de desarrollo
AI7-WP5	Revisión post-implementación

Salidas			
Número	Descripción	Entrada al	Soporte
PO10-WP1	Reportes de desempeño del proyecto	ME1	PO10-O1b, O1d, O4
PO10-WP2	Plan de gestión de riesgos de proyectos	PO9, AI3	PO10-O1c, O1d, O3
PO10-WP3	Guias de gestion de proyectos	AI1 al AI7	PO10-02, 03
PO10-WP4	Planes de proyectos detallados	PO8, AI1 al AI7, DS6	PO10-O1c, O3
PO10-WP5	Portafolio de proyectos de TI actualizados	PO1, PO5	PO10-01, O3

Figura 30 Esquema de evaluación del desempeño de un proceso parte II [4]

El esquema mostrado anteriormente será el utilizado para valorar este tipo de indicadores en el caso de estudio.

- **De Valoración de la capacidad del Proceso:** Se aplica a niveles de capacidad del 1 al 5: son genéricos para cada atributo del proceso para los niveles de capacidad del 1 al 5.
  La siguiente figura muestra los niveles de capacidad y sus atributos conforme lo propone el modelo PAM.

Figura 31 Atributos y Niveles de Capacidad [4]

La siguiente figura muestra como valorar la capacidad del proceso evaluado, través de los atributos asignados a cada nivel de madurez, apoyado en prácticas base, entradas, salidas que se toman del marco de trabajo COBIT 4.1 [2], estos criterios están organizados en el modelo PAM, a través de un formato genérico, los mismos que son específicos para cada proceso que se evalúa.

PA 2.1 Gestión del Rendimiento, una medida del grado en que se gestiona el rendimiento del proceso. Como resultado del logro pleno de este atributo: una.
Se identifican los siguientes objetivos para el rendimiento del proceso:
a. Fueron identificados objetivos para el desempeño del proceso?
b. Se Organizó y se controló el rendimiento del proceso.
c. Se ajusta el rendimiento del proceso para cumplir los planes.
d. Se definen, asignan y comunican las responsabilidades y autoridades para la realización del proceso.
e. Se identifica, pone a disposición, distribución y uso de recursos e información necesaria para realizar el proceso.
f. Se gestionan las interfaces entre las partes involucradas se gestionan para garantizar una comunicación eficaz y una clara asignación de responsabilidades.

Resultado de la plena realización de los atributos	Prácticas Genéricas (GPs)	Productos de Trabajo genéricos (GWPs)
a. El proceso alcanza sus resultados definidos.	GP 2.1.1 Identificar los objetivos del rendimiento del proceso. Los objetivos del desempeño, el ámbito junto con las hipótesis y limitaciones, están definidas y son comunicadas.	GWP 1.0 La documentación de procesos debe describir el alcance del proceso. GWP 2.0 El plan de trabajo debería proporcionar los detalles de los objetivos de rendimiento del proceso
b. Se Organizó y se controló el rendimiento del proceso.	GP 2.1.2 Planificar y controlar el rendimiento del proceso para cumplir con los objetivos identificados. Las medidas básicas de rendimiento de los procesos vinculados a objetivos empresariales se han establecido y monitoreado. Se incluyen los principales hitos, actividades requeridas, estimaciones y horarios.	GWP 2.0 El plan de trabajo debería proporcionar los detalles de los objetivos de rendimiento del proceso GWP 9.0 Los registros del rendimiento de proceso deben proporcionar detalles de los resultados. Nota: En este nivel, el registro de proceso el rendimiento puede ser: informes,resgistro de resultados o cualquier registro informal.
c. Se ajusta el rendimiento del proceso se ajusta para cumplir los planes.	GP 2.1.3 Ajuste el rendimiento del proceso. Se toman medidas cuando el desempeño previsto no se alcanzado. Las acciones incluyen la identificación de problemas de rendimiento del proceso y el ajuste de los planes y horarios, según corresponda	GWP 4.0 Registro Calidad debería informar de la acción tomada cuando el rendimiento no se consigue.
d. Se definen, asignan y comunican las responsabilidades y autoridades para la realización del proceso.	GP 2.1.4 Definir las responsabilidades y autorizaciones para realizar el proceso. Las principales responsabilidades y autorizaciones de ejecución de las actividades clave delproceso se definen, se asignan y se comunican. La necesidad de la experiencia del rendimiento del proceso, conocimientos y habilidades están definidas.	GWP 1.0 La documentación del proceso debe proporcionar la identificación del propietario del proceso y quién es el responsable, rendición de cuentas, consulta y / o informado (RACI). GWP 2.0 El plan de trabajo debe incluir detalles del plan de comunicación del proceso, así como la experiencia del rendimiento del proceso y las habilidades requeridas.
e. Se identifica, pone a disposición, distribución y uso de recursos e información necesaria para realizar el proceso.	GP 2.1.5 Identificar y poner los recursos a disposición de realizar el proceso de acuerdo con el plan. Los recursos y la información necesaria para realizar las actividades clave del proceso se identifican, asignan y utilizan	GWP 2.0 El Plan de trabajo deberían proporcionar los detalles del plan de capacitación del proceso y plan del recursos del proceso.
f. Se gestionan las interfaces entre las partes involucradas se gestionan para garantizar una comunicación eficaz y una clara asignación de responsabilidades.	GP 2.1.6 Gestionar las interfaces entre las partes involucradas. Los individuos y grupos involucrados con el proceso se identifican, las responsabilidades se definen y mecanismos eficaces de comunicación están bien ubicados.	GWP 1.0 La documentación del proceso debe proporcionar los detalles de las personas y grupos involucrados (proveedores, clientes y RACI). GWP 2.0 El plan de trabajo 2.0 deberían proporcionar los detalles del plan de comunicación del proceso.

Figura 32 Esquema de Evaluación de la Madurez del proceso [4]

Con el formato del modelo PAM, el auditor validará el cumplimiento de cada atributo correspondiente al proceso evaluado, el cual permitirá generar una valoración que refleje la madurez del proceso.

El modelo PAM propone un esquema de valoración para el logro de los atributos de cada nivel de madurez, el cual se presenta en la siguiente figura:

N	No Logrado	0% - 15%
P	Parcialmente Logrado	15%-50%
L	En gran parte Logrado	50%-85%
F	Completamente Logrado	85%-100%

Figura 33 Escala de Valoración [4]

Los niveles de capacidad contienen atributos que permiten medir la madurez del proceso evaluado como se muestra en la siguiente figura:

	Nivel 0 Incompleto	Nivel 1 Realizado	Nivel 2 Gestionado	Nivel 3 Establecido	Nivel 4 Predecible	Nivel 5 Optimizado
PA 5.2 OPTIMIZACIÓN PA 5.1 INNOVACIÓN						L / F
PA 4.2 CONTROL PA 4.1 MEDIDA					L / F	F
PA 3.2 DESPLIEGUE PA 3.1 DEFINICIÓN				L / F	F	F
PA 2.2 GESTION DEL PRODUCTO DE TRABAJO PA 2.1 GESTION DEL DESEMPEÑO			L / F	F	F	F
PA 1.1 DESEMPEÑO DEL PROCESO		L / F	F	F	F	F

Figura 34 Atributos de los Niveles de Madurez PAM [4]

A partir de este enfoque se obtiene la madurez del proceso, mismo que será el punto de partida para de la evaluación, también será de utilidad para la fase de monitoreo a fin de determinar si se han efectuado las acciones correctivas para mitigar el riesgo asociado y de esta forma subir un escalón más en el modelo de madurez.

2.1.2.3 Selección del marco de referencia

Cuando el Auditor obtiene el conocimiento necesario del proceso a revisar, deberá seleccionar un método normalizado y estructurado que sea útil para la iniciativa de auditoría tal como es COBIT 4.1, [2] además puede apoyarse en normas de gestión de Tecnologías de la Información por ejemplo: ITIL 3.0 [7], ISO / IEC 27002:2005 [8], PMBOK, MOF, etc., esto le permitirá efectuar formalmente el examen en curso, además, un marco de referencia provee una seguridad razonable de que todos los componentes del proceso sean considerados en la evaluación y ninguno se quede fuera.

Por ejemplo referirse a la siguiente figura:

SUBPROCESO A REVISARSE	MARCO DE REFERENCIA				
			Dominio	*Objetivo de Control*	*Controles*
GESTION DEL GOBIERNO DE TI	COBIT 4.1	ISO 38500	Monitoreo y Evaluación	**ME4 Proporcionar Gobierno de TI**	ME4.1 Establecimiento de un Marco de Gobierno de TI ME4.2 Alineamiento Estratégico ME4.3 Entrega de Valor ME4.4 Administración de Recursos ME4.5 Administración de Riesgos ME4.6 Medición del Desempeño ME4.7 Aseguramiento Independiente
GESTION DE CAMBIOS		ITIL 3.0	Transición del Servicio	**Gestión del cambio**	CMDB Gestión de problemas Gestión de incidentes Gestión de versiones Gestión de capacidad Gestión de disponibilidad Niveles de Servicio
SEGURIDAD FISICA Y DEL ENTORNO		ISO 27000 - 27001	Seguridad física y del entorno	**8.1 Áreas Seguras** **8.2 Seguridad de los Equipos**	8.1.1 Perímetro de seguridad física 8.1.2 Controles físicos de Entrada 8.1.3 Seguridad de oficinas, despachos e instalaciones 8.2.1 Protección contra las amenazas externas y de origen ambiental 8.2.2 Trabajo en áreas seguras 8.2.3 Áreas de acceso público y de carga y descarga 8.2.4 Emplazamiento y protección de equipos 8.2.5 Instalaciones de suministro 8.2.6 Seguridad del cableado 8.2.7 Mantenimiento de los equipos 8.2.8 Seguridad de los equipos fuera de las instalaciones 8.2.9 Reutilización o retirada segura de equipos 8.2.10 Retirada de materiales propiedad de la empresa

Figura 35 Selección de un marco de referencia

2.1.2.4 Identificación de los subprocesos de TI a ser evaluados

Luego de efectuar el relevamiento del proceso de TI a ser evaluado, el Auditor debe identificar los subprocesos que serán considerados para la auditoría, debido a que un proceso es un universo complejo compuesto por varios subprocesos, el cual requeriría mayor tiempo y más recursos para lograr evaluarlo en su totalidad. Por ejemplo si el Auditor está revisando el proceso de Seguridad de la Información, deberá abarcar únicamente 2 ó 3 subprocesos, considerando el nivel de riesgo que puede afectar al negocio, como se indica en la siguiente figura:

Figura 36 Subprocesos a ser evaluados

2.1.2.5 Selección de los objetivos de control a ser usados para la auditoría

Dependiendo del proceso seleccionado para la auditoría, el Auditor debe seleccionar los objetivos de control, del marco de referencia previamente seleccionado, los cuales no necesariamente deben ser todos los establecidos en el Marco de Referencia elegido por el Auditor, sino los que se ajustan a las necesidades de la Institución y su aplicación genera un valor agregado.

Como ejemplo para el subproceso de seguridad de la información, el Auditor podría seleccionar los objetivos de control que se muestra en la siguiente figura:

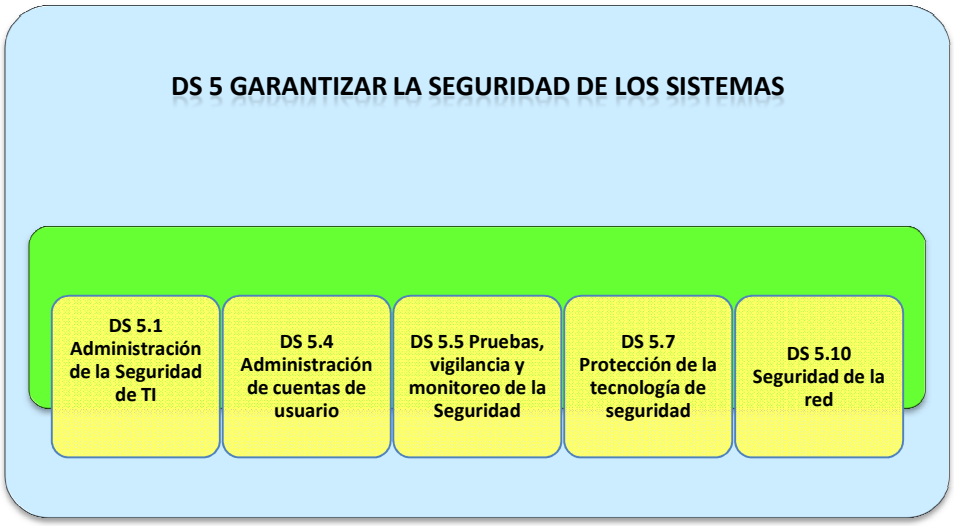


Figura 37 Selección de objetivos de control

Aplicados todos los pasos para la determinación del alcance, el Auditor obtendrá un documento como el que se muestra en la siguiente figura:

DEFINICION DE ALCANCE Y OBJETIVOS

Revisión: Seguridad de la Información
Responsable: Ing. Juan Pérez

Objetivos:

1. Analizar la planificación y administración de S.I.
2. Analizar la entrega y soporte de S.I.
3. Analizar el control y monitoreo de S.I.

Arquitectura de TI
El área de Seguridad de la Información efectúa la planificación de TI de forma anual en el plan estratégico y operativo que está alineado con las necesidades de la organización, esto a partir del plan de seguridad elaborado cuando se levantó el área. Para el proceso de entrega y soporte los funcionarios se encargan de ofrecer todos los servicios relacionados con la creación, eliminación, cambio de funciones, bloqueo, actualización de cuentas de usuario, controles de accesos a los sistemas de información y aplicaciones. El monitoreo y control se realiza todo el tiempo controlando que los usuarios con cuentas de mayor riesgo especialmente, no efectúen transacciones no autorizadas lo cual podría provocar robo o fraude.

Nivel de Madurez
Nivel 2: Gestionado

Marco de Referencia de Control
• COBIT 4.1 • ISO 27000:2005

Subprocesos a ser evaluados
Planificación Estratégica Entrega y Soporte Monitoreo y Control

Objetivos de control a ser usados
DS 5.1 Administración de la Seguridad de TI DS 5.4 Administración de cuentas de usuario DS 5.5 Pruebas, vigilancia y monitoreo de la Seguridad DS 5.7 Protección de la tecnología de seguridad DS 5.10 Seguridad de la red

Figura 38 Definición de Alcance y Objetivos

2.1.3 EJECUCIÓN

La fase de ejecución, se enfoca en la evaluación del diseño y la eficacia operativa de los controles, es decir, si existen los controles, si están funcionando adecuadamente y si estos mitigan los riesgos asociados.

Es importante considerar la evaluación de riesgos del área responsable sobre el riesgo inherente asociado al subproceso a ser evaluado, porque puede ser un factor que provoque materialidad, así como los riesgos residuales que permiten evaluar que tan efectivo es el control.

El resultado de esta fase es un documento con el detalle de los hallazgos, las recomendaciones y las conclusiones de la auditoría. El siguiente gráfico muestra la fase de ejecución.

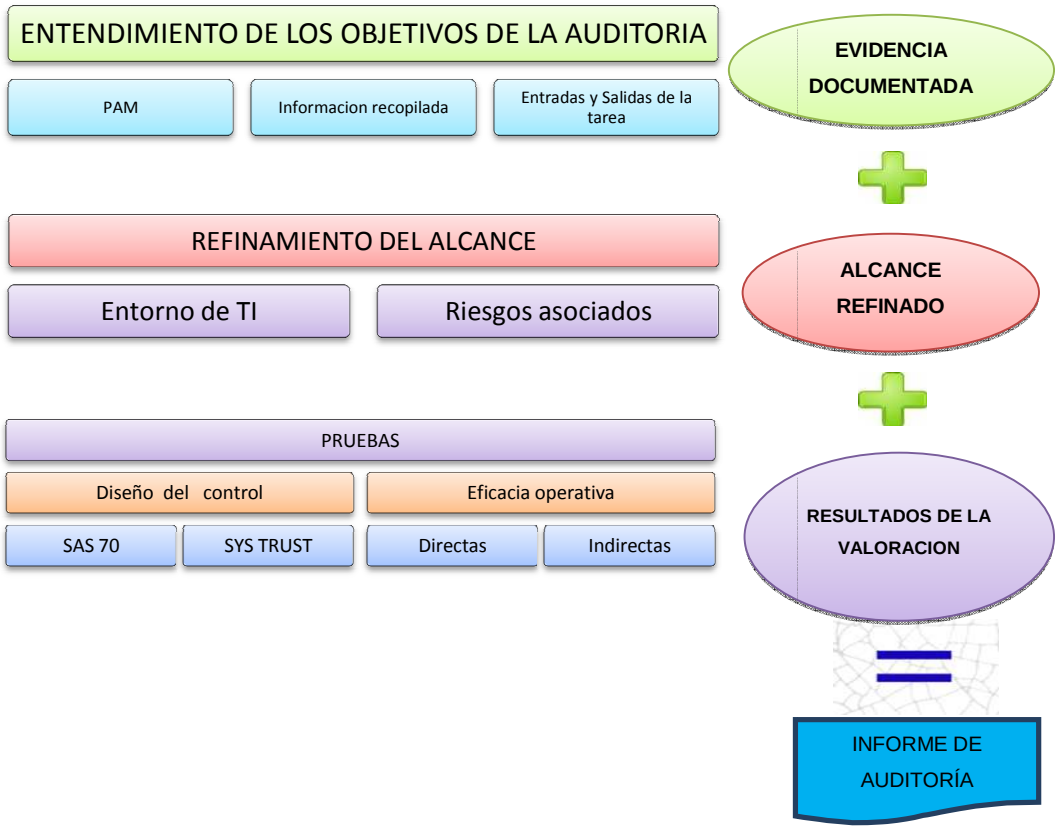


Figura 39 Fase de Ejecución

2.1.3.1 Entendimiento del objeto de la auditoría

El primer paso de la fase de ejecución es refinar la comprensión del entorno en el que se realiza la prueba, esto implica la comprensión correcta de los objetivos y procesos del área auditada. Tanto el alcance como los objetivos deben ser comunicados a los auditados y a las partes interesadas.

El entregable de esta fase consiste en la evidencia documentada respecto a:

- Quién, dónde y cuándo se realiza una tarea en particular.
- Las entradas y las salidas de la tarea.
- Los procedimientos establecidos para la realización de la tarea.

Para efectuar la revisión de los ítems mencionados anteriormente, el Auditor puede utilizar las siguientes técnicas de evaluación:

- Entrevistar y utilizar listas de actividades, tales como la matriz RACI.
- Recopilar y leer políticas, procedimientos, estándares, reportes, informes, actas, informes de auditoría anteriores respecto al proceso bajo revisión.

Como resultado de esta actividad se obtiene el plan detallado del proceso auditado, mismo que contiene: los objetivos definitivos y el contenido de la auditoría, las entradas y salidas a revisarse y el procedimiento a seguir.

2.1.3.2 Refinamiento del alcance

Siempre es aconsejable ajustar el alcance en base al conocimiento actual y detallado del entorno de TI, logrado en el relevamiento del proceso a ser revisado, así como, el conocimiento obtenido de auditorías anteriores, considerando los siguientes aspectos:

- ✓ Analizar los objetivos del negocio y de TI
- ✓ Seleccionar procesos y controles
- ✓ Analizar los riesgos clave inherentes y residuales

Para concluir con la definición final del alcance, la estrategia de la auditoría debe estar muy bien establecida, es decir, la comprensión de los objetivos, el enfoque de la prueba a efectuarse y la evaluación adecuada del riesgo debe ser clara, tal como se describió anteriormente.

Como resultado de esta actividad se obtiene un documento que contiene el alcance refinado, los subprocesos con sus riesgos asociados, los objetivos de control, el procedimiento a efectuar y el nivel de riesgo.

2.1.3.3 Pruebas del diseño del control

Para efectuar las pruebas del diseño del control el Auditor puede utilizar varias técnicas las cuales abarcan los siguientes objetivos principales establecidos en SAS 70 y seguridad SysTrust ™ :

- Evaluar el diseño de los controles
- Confirmar que los controles estén operativos.
- Evaluar la eficacia operativa de los controles.

En la fase de pruebas, se pueden aplicar los siguientes métodos genéricos de prueba que incluyen:

1. Preguntar y confirmar, se refiere a:
   - ✓ Buscar excepciones, desviaciones y examinarlas.
   - ✓ Investigar transacciones, eventos inusuales o no rutinarios.
   - ✓ Comprobar y determinar si está ocurriendo algo inusual.
   - ✓ Corroborar la gestión las declaraciones de fuentes independientes.
   - ✓ Entrevistar al personal y evaluar el conocimiento del proceso.
   - ✓ Conciliar las transacciones (por ejemplo, la conciliación de las transacciones a cuentas bancarias).
   - ✓ Hacer preguntas y obtener respuestas para confirmar resultados.

2. Inspeccionar, se refiere a:
   - ✓ Revisar planes, políticas y procedimientos.
   - ✓ Buscar pistas de auditoría, logs, etc.
   - ✓ Dar seguimiento a las transacciones, a través, de los procesos del sistema.
   - ✓ Inspeccionar documentación física
   - ✓ Recorrer instalaciones
   - ✓ Realizar un diseño o código
   - ✓ Comparar los resultados reales con los esperados

3. Observar, se refiere a:
   - ✓ Observar y describir procesos
   - ✓ Observar y describir procedimientos
   - ✓ Comparar el comportamiento real con el esperado

4. Volver a practicar y/o volver a calcular, se refiere a:
   - ✓ Desarrollar y estimar el resultado esperado de forma independiente
   - ✓ Probar que no se presente lo que se asume
   - ✓ Volver a practicar lo que es detectado por los controles
   - ✓ Volver a practicar las operaciones, los procedimientos de control, etc.
   - ✓ Volver a calcular de forma independiente
   - ✓ Comparar el valor esperado con el valor real
   - ✓ Comparar el comportamiento actual con el comportamiento esperado
   - ✓ Dar seguimiento de las transacciones a través de los procesos del sistema.

5. Verificar cálculos de forma automatizada, se refiere a:
   - ✓ Recoger muestras de datos
   - ✓ Analizar los datos usando técnicas de auditoría asistidas por computadora (CAATs).
   - ✓ Extraer excepciones o transacciones importantes

En General, los pasos de auditoría que permiten evaluar el ajuste del diseño de los controles son:

- ✓ Observar, inspeccionar y revisar el enfoque de control, y poner a prueba el diseño en temas de integridad, relevancia, oportunidad y capacidad de medición.
- ✓ Preguntar si se han asignado responsabilidades para prácticas de control y rendición de cuentas y a su vez, comprobar este punto. Probar si la rendición de cuentas y las responsabilidades asignadas han sido entendidas y aceptadas. Además, verificar que las habilidades sean las más adecuadas y que los recursos necesarios estén disponibles.
- ✓ Obtener información, a través de entrevistas con el personal clave de los procesos sobre si el mecanismo de control, propósito, rendición de cuentas y responsabilidades han sido bien entendidas y asimiladas.

En resumen, se debe determinar si:

- ✓ Están documentados los procesos de control
- ✓ Existe evidencia adecuada de los procesos de control.
- ✓ La responsabilidad y la rendición de cuentas son claras y efectivas.

Como resultado de esta actividad se obtiene un formulario donde se valida el cumplimiento de los objetivos de control y se asocia con la evidencia correspondiente.

2.1.3.4 Pruebas de la eficacia operativa del control

Para probar los resultados o la eficacia del control, el auditor debe efectuar pruebas directas e indirectas de los efectos del control en la calidad de las salidas del proceso, es decir, el logro real de los resultados.

El Auditor debe obtener evidencia directa o indirecta de los elementos seleccionados para asegurarse de que el control examinado está funcionando eficazmente, mediante la aplicación de una técnica adecuada de prueba tal como se menciona en la prueba del diseño de control, además, debe realizar una revisión general la efectividad de los entregables generados del proceso bajo revisión y determinar el nivel de pruebas sustantivas adicionales y necesarias a realizarse para asegurar que el proceso sea adecuado.

Como resultado de esta actividad se obtiene un formulario donde se verifican los procedimientos ligados a los subprocesos, a través, de una valoración de las muestras esperadas versus las reales, además, se obtiene la calificación al proceso evaluado basado en el nivel de control, daño y riesgo.

2.1.3.5 Elaboración de Informe y comunicación de resultados

Elaboración del Informe

Cuando se encuentran deficiencias del control, éstas deben ser debidamente documentadas, teniendo en cuenta su naturaleza a menudo sensible y confidencial, además, la gravedad de las deficiencias observadas y el impacto que puede afectar al negocio.

El objetivo de este paso es llevar a cabo las pruebas necesarias de seguridad respecto a realización de un proceso y sus objetivos de control relacionados.

Cuando el impacto es alto o medio se observa que:

- ✓ Las medidas de control no estén en su lugar.
- ✓ Los controles no están funcionando como se espera.

- ✓ Los controles no se aplican consistentemente.

El resultado de este análisis es un conocimiento profundo de las debilidades de control, amenazas, vulnerabilidades y la comprensión del impacto potencial de las deficiencias de control.

A continuación se mencionan los pasos que **pueden** ser ejecutados para documentar el impacto de no alcanzar el objetivo de control:

a. Relacionar el impacto de no alcanzar el objetivo del control con casos reales en el mismo sector y puntos de referencia del mercado.
b. Enlazar indicadores de desempeño con resultados reales, en caso de que no existan, vincular la causa a su efecto.
c. Ilustrar el escenario que afectaría el impacto a través de errores, ineficiencias y mal uso.
d. Determinar las vulnerabilidades y amenazas que están más relacionadas con la operación no efectiva de los controles.
e. Documentar el impacto de las debilidades reales de control en términos del impacto, la integridad de la información financiera, las horas perdidas en el tiempo del personal, la pérdida en ventas, la habilidad para manejar y reaccionar a las exigencias del mercado, requerimientos de clientes y accionistas, etc.
f. Señalar las consecuencias del incumplimiento de los requisitos reglamentarios y acuerdos contractuales.
g. Medir el impacto real de las interrupciones de los procesos de negocio y objetivos.
h. Documentar el costo de los errores generados por la no aplicación de controles eficaces.
i. Medir y documentar el costo de la reanudación de trabajo como una medida de eficiencia afectada por deficiencias en el control.
j. Medir los beneficios de negocio reales e ilustrar los ahorros de costes de los controles eficaces después de los hechos.

k. Utilizar gráficos extensivos para ilustrar los problemas.

Además, de la valoración de los controles descrita en los párrafos anteriores, se debe determinar si los riesgos claves del negocio han sido considerados y evaluar que tan efectivos son los controles y procedimientos que mitigan estos riesgos a niveles aceptables, es decir, opinar sobre el riesgo residual.

Comunicación de resultados, conclusiones y recomendaciones

Cualquier deficiencia del control identificada debe ser documentada, así como amenazas y vulnerabilidades resultantes, el impacto real y potencial sobre los objetivos del negocio y el nivel de madurez actual del proceso a ser evaluado, aspecto que servirá para el análisis GAP en la fase de Monitoreo.

Un aspecto importante, es proporcionar información comparativa para establecer un punto de referencia sobre el cual se evalúan los resultados.

El objetivo es identificar los elementos de importancia que requieren especial atención y expresarlo de forma clara y concreta a las partes interesadas, así como las recomendaciones para corregir las deficiencias encontradas y las razones para la adopción de medidas correctivas a corto o largo plazo dependiendo del impacto sobre los objetivos del negocio a fin de mitigar el impacto de las debilidades de control.

Finalmente, se debe desarrollar las conclusiones con respecto a las deficiencias identificadas.

Como resultado de esta fase se obtiene el informe final de auditoría, documento que debe ser presentado a las partes interesadas, a fin de discutir los hallazgos, efectos, y recomendaciones; y acordar el plan de acción a seguir, o a su vez descargar las observaciones que podrían ser solventadas durante la realización de la auditoría.

2.1.4 MONITOREO

A fin de efectivizar el modelo propuesto, es necesario contar una etapa que permita monitorear el avance de las recomendaciones efectuadas en auditorías anteriores, empezando con un análisis GAP entre el nivel de madurez obtenido y el deseado, aspecto que debe considerarse en un informe que tiene como objetivo principal comunicar a los interesados el nivel de madurez en el que se ubica actualmente el proceso evaluado y hacia donde se quiere llegar. La periodicidad de esta fase será determinada por la Alta Gerencia, tomando en cuenta las normativas establecidas por la Superintendencia de Bancos en relación al seguimiento de las observaciones levantadas en los exámenes de auditoría.

2.1.4.1 Análisis de madurez anterior vs. deseado (GAP)

El análisis GAP de la madurez obtenida versus la deseada (siguiente nivel), permitirá al auditor determinar si fueron solucionadas las falencias expuestas como observaciones de auditoría relacionas con fortalezas y debilidades observadas, hallazgos y análisis de riesgos y recomendaciones para lograr el nivel esperado, es decir, si las acciones tomadas sobre los objetivos de control no cumplidos, mejoraron la gestión y estas permitieron alcanzar el nivel de madurez superior deseado o se mantiene el nivel anterior, aspecto que impactaría significativamente al valor agregado que genera el trabajo de auditoría.

2.1.4.2 Elaboración del informe de monitoreo

Los resultados obtenidos deben ser documentados y presentados a la Alta Gerencia con el fin de comunicar el logro de los objetivos de control implementados y la nueva ubicación en otro nivel de madurez superior, de ser el caso, caso contrario se señalará que el estatus no ha variado con relación al análisis anterior y el impacto de los atributos no logrados.

A continuación se usa el modelo desarrollado en el presente capítulo, a fin de validar su aplicabilidad en un caso de estudio.

CAPÍTULO 3. VALIDACIÓN DE LA APLICABILIDAD DEL MODELO A TRAVÉS DE UN CASO DE ESTUDIO EN UNA ENTIDAD FINANCIERA

Una vez obtenido un conocimiento general sobre la Entidad financiera a aplicar el modelo, para el caso de estudio CoopABC Ltda., se procede a aplicar el modelo establecido en el capítulo II; es importante indicar que como caso de estudio se va a efectuar un examen de auditoría sobre un subproceso considerado de riesgo alto para la Institución.

Para la elaboración del plan de auditoría se utilizará una herramienta de propiedad de los autores elaborada en Excel la cual se basa en los criterios de riesgos que han sido establecidos por la Alta Gerencia y la metodología propia de la Entidad Financiera.

Para la desarrollo del examen de auditoría se utilizará una aplicación para efectuar auditorías basadas en riesgos llamada ERA (Enterprise Risk Assesor) cuyo fin es apoyar a este tipo de auditorías, además, esta herramienta permitirá la optimización de tiempos en la emisión del informe, gestión de papeles de trabajo, y mejoramiento del desempeño del equipo de auditoría.

Es importante indicar que el equipo de trabajo se apoya en formatos Excel que han permitido efectuar de forma adecuada el desarrollo de la presente propuesta.

A continuación se detalla la aplicación del modelo:

3.1 PLANIFICACION

3.1.1 ENTENDIMIENTO DE OBJETIVOS Y PROCESOS DEL NEGOCIO

3.1.1.1 CARACTERIZACIÓN DE LA EMPRESA

Historia

La CoopABC Ltda. tiene 42 años en el mercado financiero, se fundó con el único afán de contribuir al desarrollo económico del sector con soluciones financieras, tanto en créditos, por sus tasas bajas, como por sus inversiones de rentabilidad elevada, por lo cual hasta la fecha prestan servicios en la matriz, en varias sucursales y ventanillas de extensión ubicadas estratégicamente en varias ciudades del país.

La entidad financiera guía su desarrollo sobre la base de sus sueños expresos en una misión y visión que orientan el comportamiento de quienes la conforman: personal, directivos, proveedores, socios y clientes, cuyo fundamento de actuación se declara en los valores que se practican.

Misión

Servir a socios clientes, de manera competitiva y equitativa facilitando la entrega de productos y servicios financieros, retribuyendo valor a los aportes de los socios, que aseguren el mejoramiento de la calidad de vida, el progreso de la comunidad y del país, utilizando la tecnología disponible, respaldados en el compromiso de su talento humano que fortalecen la confianza, solidez y crecimiento de la Institución.

Visión

Ser líderes en la innovación en el sistema cooperativo, y ser competitivos en el sistema financiero nacional para satisfacer las necesidades de nuestros socios clientes contribuyendo a su bienestar y de la comunidad.

Objetivos Estratégicos

Los objetivos estratégicos están fundamentados en las metas y estrategias planteadas por la Organización a fin de alcanzar los resultados esperados en un tiempo determinado a través de acciones que permitan cumplir con la misión y apalancados en la visión.

Los objetivos estratégicos de la Entidad son:

- ✓ Alcanzar una estructura financiera que permita la sustentatibilidad del negocio en el largo plazo.
- ✓ Satisfacer las espectativas de los socios.
- ✓ Alcanzar niveles de excelencia comercial y operativa que garantice la entrega oportuna de productos y servicios.
- ✓ Fortalecer la cultura organizacional basada en el compromiso y la maximización del potencial del Talento Humano.
- ✓ Gestionar los riesgos institucionales.
- ✓ Fortalecer la responsabilidad social y el Cooperativismo.

Estructura Organizacional

La estructura organizacional de la Entidad Financiera está constituida de forma jerárquica a través de sus diversas líneas de negocios, distribuidas de forma estratégica, aspecto que ha permitido una gestión adecuada de sus operaciones financieras tanto a nivel del negocio, como a nivel administrado a través de sus áreas de apoyo. La siguiente figura, muestra la estructura orgánica de la Entidad.

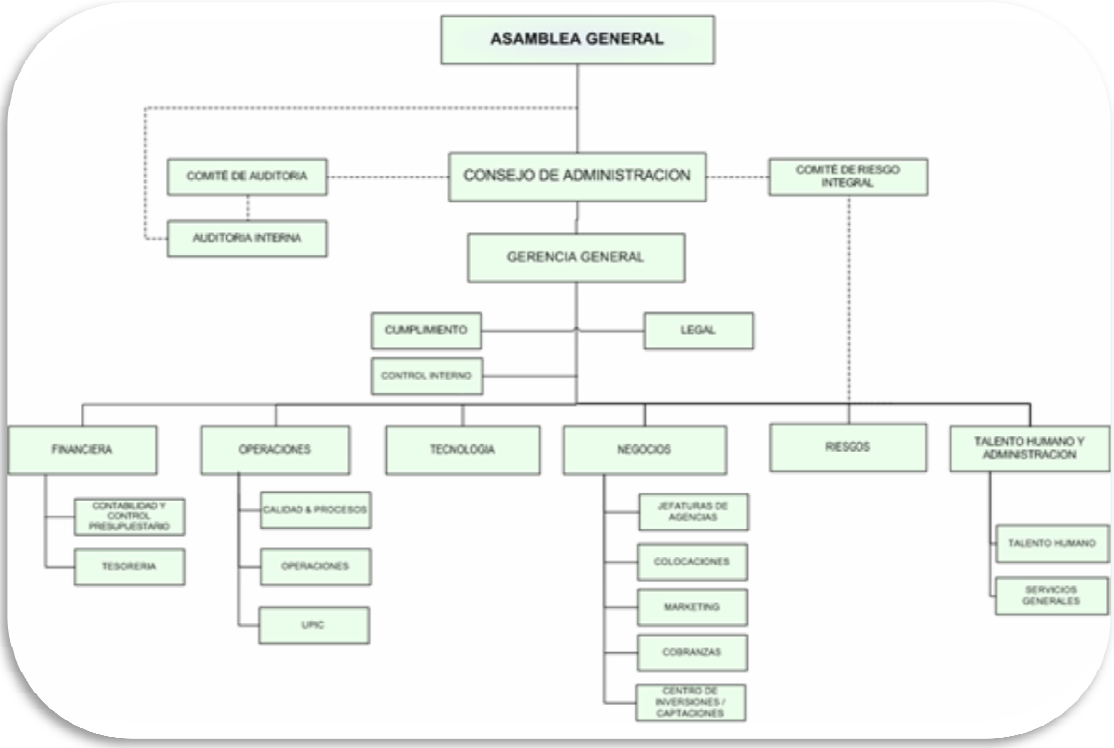


Figura 40 Organigrama Estructural CoopABC Ltda

Cultura Organizacional

La cultura organizacional de la Institución está regida por el plan estratégico, planes operativos, estatutos, reglamentos internos, instructivos, manuales, planos estructurales, de comunicaciones, eléctricos, resoluciones emitidas por la Superintendencia de Bancos y Seguros. Toda la documentación mencionada está formalmente aprobada por los entes reguladores o de control.

La siguiente tabla detalla lo indicado.

No.	DOCUMENTO	DESCRIPCION	RESPONSABLE	FECHA APROBACION
		PLANES		
1	Plan estratégico 2010	Contiene las estrategias para lograr los objetivos organizacionales	Gerente	Por aprobar
2	Plan Operativo x áreas	Contiene las actividades a realizarse para lograr las estrategias planteadas en el plan estratégico	Cada área	Por aprobar
		NORMAS, REGLAMENTOS		
3	Código de ética	Contiene	Talento Humano	Aprobado
4	Reglamento interno	Contiene todas las normas a cumplirse por parte del personal	Talento Humano	Aprobado
5	Estatutos de la Entidad Financiera	Contiene	Presidencia	
6	Reglamento de salud ocupacional		Talento Humano	Por aprobar
7	Decreto 194	Organización, funcionamiento y liquidación de las Entidad Financieras de Ahorro y Crédito		
8	Resolución 834	Riesgo Operativo	Riesgos	N/A
9	Resolución SBS-2005-0586	Transparencia	Cumplimiento	N/A
10	Resolución JB-2010-1683	Lavado de activos	Cumplimiento	N/A
11	Ley General de Instituciones del Sistema Financiero	Toda la Entidad Financiera	Toda la Entidad Financiera	N/A
12	Resolución JB-2004-834	Riesgo Operativo	Riesgos	N/A
13	Resolución JB-2002-429	Administración y Gestión del riesgo de mercado y liquidez	Riesgos	N/A
14	Resolución No JB-2010-1538	Administración y Gestión del Riesgo Integral	Riesgos	N/A
15	Instructivos dictados por la UIF.	Normas y regulaciones dictaminados por la Unidad de Inteligencia financiera	Control interno, Cumplimiento	N/A
16	Todas la normativa vigente para el sistema financiero			
		PLANOS		
17	Redes y Comunicaciones	Se detalla el esquema de enlaces, equipos y dispositivos	Tecnología	Mayo, 2010
18	Eléctricos	Se esquematiza los dispositivos eléctricos, su ubicación y enlace	Tecnología	Julio, 2009

Tabla 1 Cultura Organizacional

Mapa de Procesos

La Institución financiera, conforme lo establecido en la resolución JB-2005-834 [6], ha determinado en una primera instancia la necesidad de identificar los procesos existentes en cada una de las áreas de la entidad conforme se muestra en la siguiente figura:

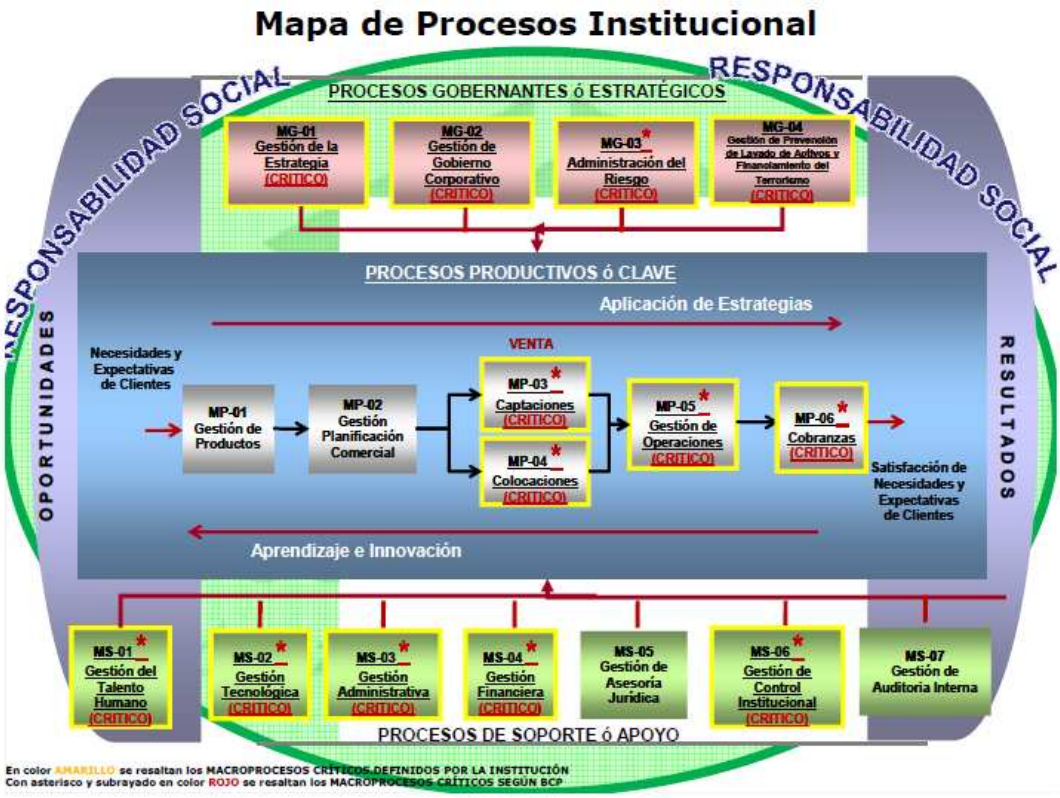


Figura 41 Mapa de Procesos Institucionales

3.1.1.2 CARACTERIZACIÓN DEL SISTEMA

La caracterización del sistema es el punto de partida y la base fundamental para obtener un conocimiento global de los subprocesos a ser evaluados, por lo tanto, el Auditor debe solicitar información general del gobierno de TI, tal como se muestra en los temas que se detallan a continuación:

Misión del área de TI

Dotar de servicios tecnológicos que garanticen el adecuado funcionamiento de las aplicaciones de infraestructura de TI a ser utilizada por la Entidad Financiera, ofreciendo la mejor calidad y productividad.

Visión del área de TI

Ser un área de servicios tecnológicos innovadores para la Entidad Financiera con un nivel de valor agregado, calidad y satisfacción a nuestros clientes internos y externos.

Valores estratégicos del área de TI

- ✓ Liderazgo
- ✓ Orientación al Cliente
- ✓ Orientación al Logro
- ✓ Flexibilidad
- ✓ Trabajo en Equipo
- ✓ Excelencia en la Gestión
- ✓ Disponibilidad

Estructura orgánica del área de TI

La estructura orgánica de TI refleja el nivel de jerarquía que existe dentro del área de Tecnología, es también uno de aspectos fundamentales que el Auditor debe conocer a fin de obtener un grado de conocimiento sobre las funciones,

responsabilidades, nivel jerárquico a quien reporta o sus pares y sobre todo validar si existe segregación de funciones, dependiendo del nivel de riesgo asociado a los procesos de los cuales son responsables. En la siguiente figura se muestra el organigrama del área de Tecnología y a continuación se detalla las funciones y responsabilidades de los cargos de los funcionarios del área.

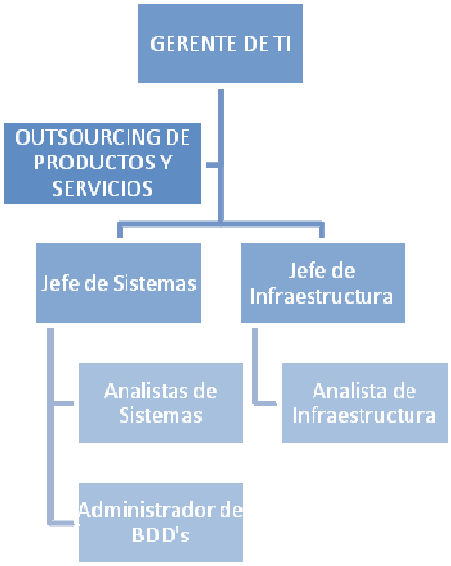


Figura 42 Orgánico Funcional TI

Gestión de Tecnología:

1. Analizar, determinar e implementar la arquitectura del Inventario tecnológico de la organización
2. Definir y ejecutar el presupuesto tecnológico en base a la detección de necesidades de las áreas
3. Definir la arquitectura de comunicación e interconexión de la Institución
4. Planificar y controlar el mantenimiento adecuado del inventario tecnológico de la organización.

5. Planificar e implementar política de seguridad y respaldo de datos administrados
6. Establecer prioridades y directrices respecto de herramientas, metodologías, hardware, software y comunicaciones que permitan la implantación del plan de soluciones informáticas
7. Garantizar que las inversiones tecnológicas de la Institución están bajo el marco de políticas y procedimientos y mejores prácticas de TI.
8. Dirigir, integrar y asegurar que los diseños técnicos de arquitecturas elaborados por las distintas unidades se encuentren dentro del marco de la arquitectura global definida en el plan de soluciones.
9. Elaborar y proponer los procedimientos y planes de contingencia y continuidad del área de Sistemas
10. Establecer y acordar políticas de administración de Bases de datos para elaborar propuesta al Consejo de Administración
11. Planificar, dirigir y controlar la elaboración y ejecución de los planes operativos acorde al plan estratégico.
12. Garantizar el óptimo desarrollo y coordinación del equipo a su cargo, y la implementación del modelo de gestión y de cambio organizativo y cultural de información.
13. Garantizar el correcto cumplimiento de los servicios y estándares de calidad de atención de los requerimientos de usuario y en su caso dirigir la solución de problemas.
14. Analizar, desarrollar y viabilizar la factibilidad de proyectos tecnológicos y aquellos designados por la Gerencia General
15. Dirigir y controlar la calidad del resultado de la laborar del personal de tecnología, a fin de garantizar la entrega de servicios e información oportuna y confiable que permita la toma de decisiones
16. Garantizar la custodia de la documentación técnica y funcional en las distintas unidades Tecnológica; y por la correcta definición y desarrollo de los procedimientos generales y planes de puesta en producción.

17. Implementar iniciativas que mejoren los resultados globales en su unidad, con el fin de permitir la creación y el desarrollo de nuevas oportunidades

Gestión de Infraestructura:

- ✓ Asegurar que los diseños técnicos de arquitecturas de las unidades a su cargo se encuentran dentro del marco de la arquitectura global, definida en el plan estratégico de TI, para soportar eficientemente la demanda generada por los sistema de la Entidad Financiera
- ✓ Garantiza la alta disponibilidad del sitio alterno y de la infraestructura de contingencias que permita la continuidad del negocios y el cumplimiento de los acuerdos de servicio pactados
- ✓ Garantiza la alta disponibilidad de los canales electrónicos de la Institución, con el fin de mantener la más elevada calidad en el servicio.
- ✓ Garantizar alta disponibilidad de la infraestructura de procesamiento de datos considerando el H, S y C, que soportan los servicios y productos que entrega la Institución a sus clientes.
- ✓ Controlar, dirigir y coordinar la elaboración de los planes operativos acorde al plan estratégico.
- ✓ Realizar investigación y desarrollo de nuevas tecnologías de HSC, que permitan generar una ventaja competitiva para Institución
- ✓ Garantizar la existencia y actualización de la documentación técnica y funcional del inventario tecnológico a su cargo con el fin de mantener actualizada la biblioteca de la infraestructura de H, S y C. de la Institución.
- ✓ Sugerir y diseñar la arquitectura de todos y cada uno de los componentes de H, S, T para la incorporación de las mejoras tecnologías dentro del ámbito de las mejores prácticas tecnológicas

- ✓ Garantizar el correcto cumplimiento de los servicios y estándares de calidad de atención de los requerimientos de usuario, administrar los recursos para la solución de problemas.
- ✓ Garantizar el óptimo desarrollo del equipo a su cargo, mediante la preparación y actualización a fin de garantizar los estándares de calidad
- ✓ Proponer e implementar iniciativas que mejoren los resultados globales en su unidad, con el fin de permitir la creación y el desarrollo de nuevas oportunidades
- ✓ Definir lineamientos, en coordinación con el área de talento humano, diseñar el plan de capacitación del personal a cargo con el fin de incorporarlo al plan de capacitación integral del área.

Gestión de aplicaciones:

- ✓ Controlar la correcta funcionalidad de la aplicación de puestos en producción por la Entidad Financiera.
- ✓ Dirigir y coordinar que los diseños técnicos de arquitecturas elaborados por las distintas unidades se encuentran dentro del marco de la arquitectura global definida en el plan de soluciones informáticas.
- ✓ Garantizar la óptima capacitación de la arquitectura de sistemas, plataformas de información y componentes de software necesarios para proyectar en un adecuado funcionamiento en el tiempo.
- ✓ Planificar y organizar la definición, diseño, selección e implementación de la arquitectura de sistemas, plataformas de información y componentes de software necesarios
- ✓ Planificar, definir y ejecutar los lineamientos y estándares de calidad para el adecuado procesamiento de la información y la óptima funcionalidad en los servicios centrales y distribuidos.

- ✓ Elaborar/actualizar la documentación de las medidas técnicas aplicadas durante la puesta en producción de los desarrollos
- ✓ Asegurar el soporte necesario a la unidad de soporte a usuarios, durante la implantación de la aplicación, realizando las adecuaciones necesarias a la aplicación cuando surjan problemas
- ✓ Analizar los reportes de errores detectados en el procesamiento de la información, identificando las causas del problema y coordinando las medidas necesarias para la corrección de las mismas.
- ✓ Elaborar los análisis requeridos para garantizar la correcta funcionalidad de los servidores centrales y distribuidos, el ámbito que le corresponda
- ✓ Identificar y solucionar los problemas reportados por el servicio a usuarios, que se presenten de forma repetitiva en la infraestructura de procesamiento
- ✓ Verificar la correcta disponibilidad de recursos para el procesamiento de la información en el ámbito que corresponda
- ✓ Solucionar los problemas técnicos que se presenten con los servidores y aplicaciones, según el ámbito que corresponda, identificando las causas del problema y las medidas a tomar para su solvencia.
- ✓ Informar sobre incidencias y aplicar las medidas correctivas a su alcance para solucionar problemas presentados en la infraestructura de procesamiento
- ✓ Realizar el seguimiento y monitoreo de los equipos de infraestructura de procesamiento cumpliendo la programación establecida
- ✓ Aplicar las definiciones y programaciones necesarias en lo referente a la administración de los servidores centrales y distribuidos que garanticen el cumplimiento
- ✓ Analizar los requerimientos de implementación de las actividades del área de sistemas, propuestas de mejora de usuarios , evaluando su factibilidad

- ✓ Apoyar en la definición de las necesidades de servicios de tecnología derivadas de las aplicaciones diseñadas garantizando su posterior implantación.
- ✓ Realizar los análisis técnicos necesarios para la instalación de infraestructura de sistemas, plataformas y software de los servidores centrales y distribuidos
- ✓ Realizar los análisis técnicos necesarios para la selección de los componentes de procesamiento central y distribuido idóneos a la arquitectura definida y diseñada
- ✓ Prestar apoyo en los análisis técnicos necesarios para la realización de la planificación de recursos de procesamiento de información, dentro del ámbito que maneja
- ✓ Desarrollar los trabajos necesarios para la ejecución de las actividades del área de sistemas que permiten asegurar la calidad, costo y plazo.
- ✓ Realizar los análisis técnicos necesarios para la realización de la planificación de la infraestructura de procesamiento tecnológico.
- ✓ Proveer de los análisis técnicos necesarios que permitan definir y diseñar la plataforma de seguridad, desde el punto de vista de tecnología de información
- ✓ Realizar los análisis necesarios que apoyan a la definición de las políticas y acciones del plan de contingencias y la plataforma de seguridad de sistemas.
- ✓ Aplicar las metodologías definidas para el desarrollo de proyectos dentro de su ámbito técnico
- ✓ Presta apoyo en los análisis técnicos necesarios para la elaboración de las partidas presupuestarias correspondientes

Administración de BDD:

- ✓ Realizar actualizaciones, creaciones de todo objeto a nivel de base de datos
- ✓ Monitorear y gestionar la creación de dispositivos de base de datos
- ✓ Optimizar los procesos de base de datos para obtener mejores rendimientos
- ✓ Otorgar y administrar las seguridades de la base de datos
- ✓ Realizar tareas de TUNING de base de datos
- ✓ Evaluar el rendimiento de los motores de base de datos

Posición en la toma de decisiones

El área de TI está representada por el Gerente de Tecnología, quien asiste a todas las reuniones del Consejo de Administración, para la toma de decisiones en consenso con todas las áreas que conforman el nivel directivo. La siguiente figura muestra la estructura para la toma de decisiones.

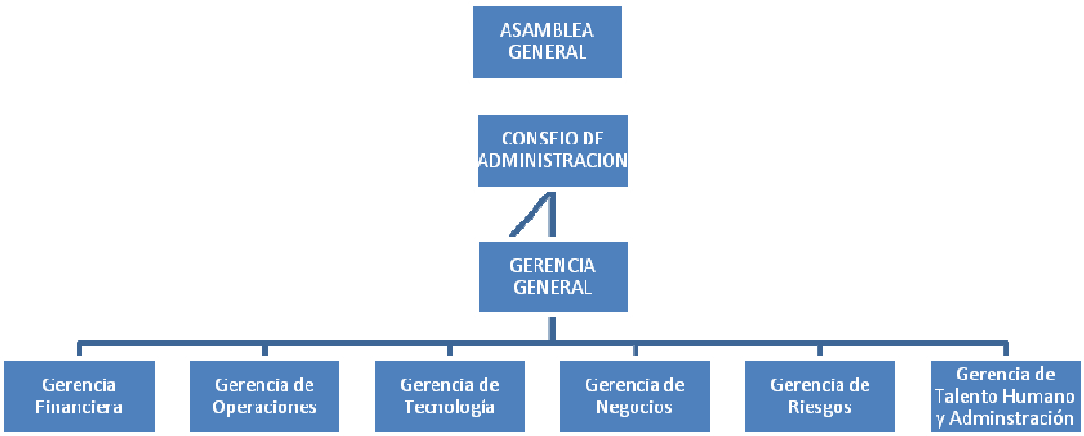


Figura 43 Posición Toma de decisiones

3.1.1.3 Caracterización de la Capacidad Instalada

La capacidad instalada en la entidad financiera, se consolida en el diagrama de red que representa la arquitectura actual sobre la cual se opera el proceso transaccional, la forma de interconexion entre las diferentes agencias, los principales caneles y equipos de comunicaciones a nivel interno y externo, los medios de protección, los distintos medios de almacenamiento como son los servidores principales, entre otros. La siguiente figura muestra el diagrama de red de nuestro caso de estudio.

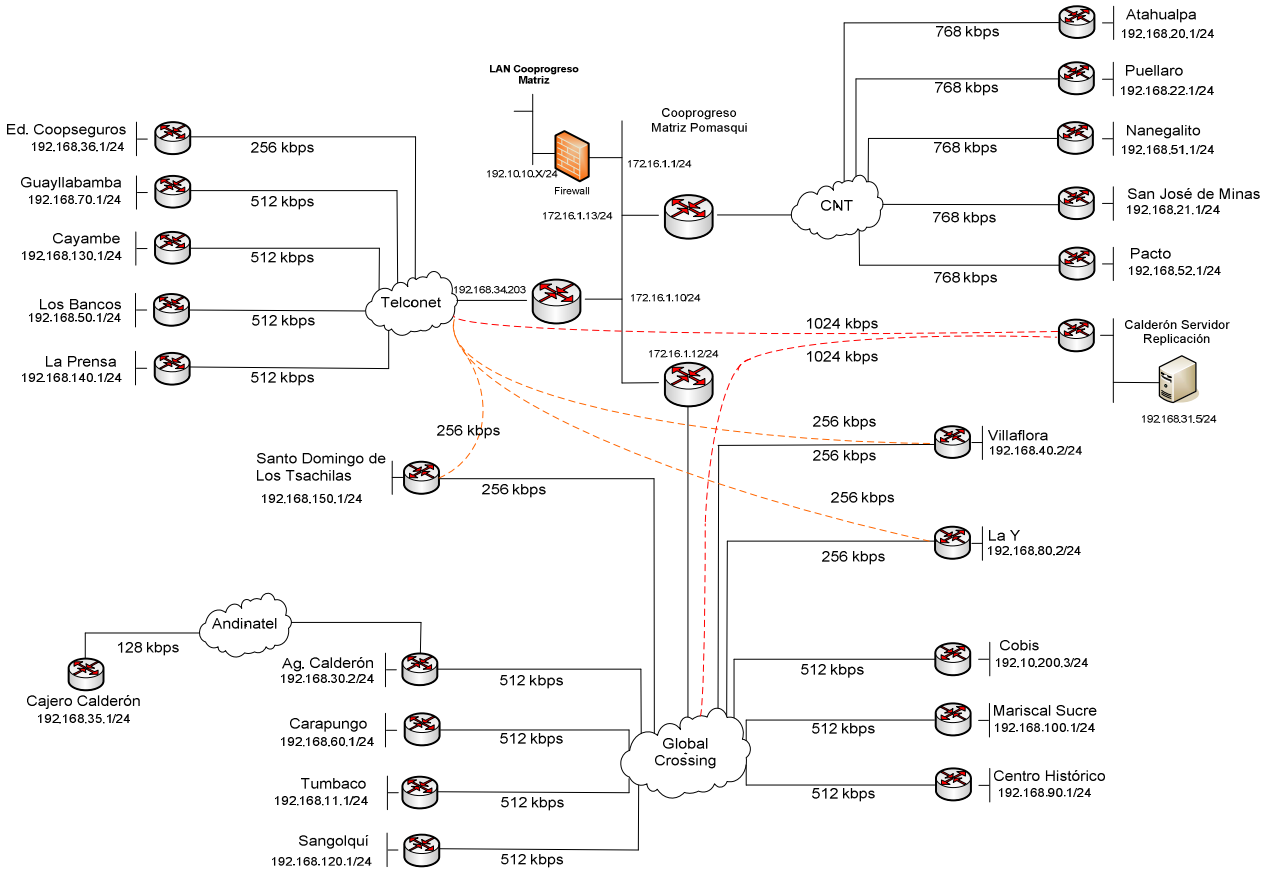


Figura 44 Arquitectura de Red

3.1.1.4 CARACTERIZACIÓN DE LA UNIDAD DE SEGURIDAD DE LA INFORMACIÓN

Otra de la áreas importantes dentro de la Organización es el área de Seguridad de la Información que debe ser independiente del área de Tecnología a fin de garantizar de forma efectiva la salvaguarda del activo más importante para cualquier Institución, como es la información, por lo tanto, es necesario que el Auditor adquiera nivel de conocimiento elevado del funcionamiento de esta área. A continuación se detalla la caracterización del área de Seguridad de la Información.

Misión del área de Seguridad de la Información

Implementar seguridad a procesos tecnológicos y operativos para asegurar la continuidad del negocio de una manera eficiente y efectiva, agregando competitividad a la institución.

Visión del área de Seguridad de la Información

Fortalecer las estrategias de seguridad de la información de acuerdo a las necesidades del negocio y su crecimiento.

Estructura Orgánica del área Seguridad de la Información

Para el caso de estudio la estructura orgánica del área de Seguridad de la Información es simple debido a que solo existen dos personas responsables del área, la siguiente figura muestra lo indicado, seguido de la descripción de las responsabilidades de sus integrantes.

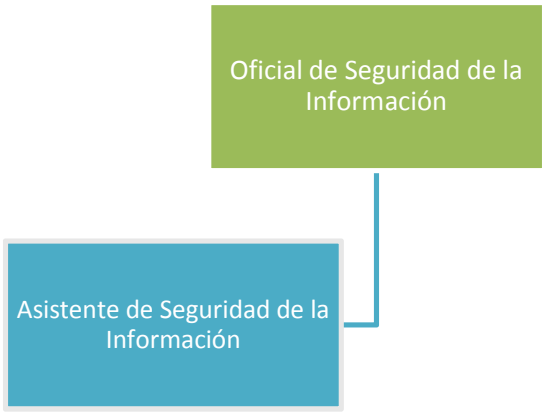


Figura 45 Estructura Orgánica S.I.

Gestión de seguridad de la información:

- ✓ Implantar en la Entidad la arquitectura de seguridad: políticas, estándares, procesos, procedimientos y modelo de seguridad establecido y aprobado por el Comité de Seguridad.
- ✓ Hacer que toda la estructura organizacional de seguridad funcione acorde a su rol y en caso de no ser así informar al Comité de Seguridad para que se tomen las medidas correctivas.
- ✓ Mantener informada a la Organización sobre estrategias y normatividad en seguridad de la información definidos a nivel institucional y de todo cambio en las políticas, estándares, proceso y procedimiento aprobados.
- ✓ Alertar al Comité de Seguridad, a la Alta Gerencia de todos los riesgos en temas de seguridad de la información y los planes de acción para ir cubriéndolos.
- ✓ Gestionar las estrategias de seguridad de la información relacionadas con la arquitectura de Seguridad institucional
- ✓ Asegurar que los propietarios de la información ejerzan su responsabilidad sobre los activos que manejan.

- ✓ Velar por la implantación de todos los procesos de seguridad en la Institución con medidas de gestión claras, y medibles.
- ✓ Gestionar un plan de seguridad de la información manteniendo informad al Comité de Seguridad de la Información sobre desviaciones y acciones correctivas a tomarse.
- ✓ Identificar procesos de riesgo en seguridad de la información

3.1.2 IDENTIFICACIÓN DE PROCESOS Y RIESGOS ASOCIADOS

Para esta actividad el departamento de Riesgos de la Entidad Financiera “ABC Coop” que es la encargada de gestionar los riesgos, basándose en la distribución de los procesos conforme la estructura recomendada en la resolución JB-2005-834 [6] emitida por las Superintendencia de Bancos. Los riesgos que a continuación se presenta fueron levantados por los dueños de los procesos en coordinación con la gerencia de Riesgos, expertos en la metodología de Gestión de Riesgos “AZ-NZS:4360” [9].

Para el efecto, la Entidad financiera, a través de la Unidad de Riesgos utiliza una herramienta que establece una matriz entre los procesos, los riesgos y controles asociados.

La siguiente tabla muestra los riesgos levantados para el área de Tecnología por cada subproceso:

DESCRIPCION PROCESO				
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	Incremento de la productividad del área por retrasos en las entregas de equipos y servidores que dilatan otras actividades del personal del IT. debido a actividades ya establecidas o calendarizadas al personal de IT que no cumplen con los tiempos establecidos
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	Incremento en los costos de operación por los equipos que deben ser retornados al área de IT para su revisión por preparación errónea o instalaciones no adecuadas que no dan el funcionamiento que el usuario requiere, además, se preparan equipos y servidores sin tomar en cuenta la función que va a desempeñar el mismo
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	Incremento en los costos de operación. Por Los equipos no funcionan adecuadamente. Por las fallas en el Sistema Operativo. los sistemas operativos se corrompen o han sido instalados o manipulados de forma errónea
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	Incremento de la productividad del área. Por se necesita la reinstalación de la aplicación. Instalación mal efectuada o no realizada. no funciona o no tiene el adobereader.
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	Incremento de la productividad del área. Por realiza revisiones en las impresoras ingresando al equipo del cliente para la revisión de la impresora el usuario no puede imprimir

DESCRIPCION PROCESO				
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	Incremento de la productividad del área. Por es necesario la revisión nuevamente del equipo o servidor. el mismo presenta fallas en las configuraciones por defecto. el usuario no puede realizar o usar adecuadamente las aplicaciones de la Cooperativa
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	Incremento en los costos de operación. Porque no funcionan las cámaras de vigilancia. Por fallas en los equipo o software. no presenta las imágenes a grabar
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	incremento de la productividad del área: Por al no permitir ingresar con un usuario súper administrador a dar soporte al ingresar a un equipo y servidor con este usuario: cuando se requiere soporte sobre el equipo o servidor
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Licenciamiento	Incremento de costos porque se dan adquisiciones de licencias no adecuadas como parte de un errado análisis del proceso de adquisición, cuando la institución o usuario solicitan un licenciamiento
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Licenciamiento	Incremento de la operatividad del área porque se deben reingresar y revisar todas las adquisiciones como parte del ingreso de licencias adquiridas cuando se adquieren nuevas licencias

DESCRIPCION PROCESO				
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Soporte a Usuarios	Incremento en la operatividad del área, porque hay incidentes no resueltos, como resultado de un SLA fuera del ámbito definido como consecuencia de obviar los puntos de escalamiento Cuando estos no son entregados acorde a la matriz y SLA previamente acordados en la institución
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Soporte a Usuarios	Pérdida de productividad del área, Porque son requerimiento ingresado sin su debido respaldo o con deficiencias en la descripción resultado de un desconocimiento del usuario Cuando este no describe claramente el problema a ser ingresado en el F11
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Bases de Datos	Incremento en costos de operación, Por se aplicaron procesos de dimensionamiento no adecuados. el tener datos no exactos de crecimiento de los últimos 3 años mas el incremento proyectado. se realizan las actividades de capacity planing del a Base de datos
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Bases de Datos	Incremento de la operatividad del área Por existen datos que causan lentitud en las operaciones. por la no aplicación correcta de las operaciones de depuración: Cuando no se lo realizan con la planificación existente mensual
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Bases de Datos	Incremento en costos de operación, Por no se llevan a cabo un continuo monitoreo de las bases de datos. al no ejecutar las respectivas rutinas de visualización del estado delas B.D Cuando, no se ejecutan las mismas de forma diaria

DESCRIPCION PROCESO				
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Bases de Datos	Perdida de oportunidad del área. Porque al no ejecutar las rutinas de depuración. por la no ejecución de las ruticas. con los procesos mensuales definidos
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Redes LAN y Cableado	Incremento en la operatividad del área. Por se realiza un inadecuado análisis de cableado y medio de conexión Como. Al no intervenir o contar con todos los datos para el mapa lógico Cuando se ejecutan nuevas instalaciones o readecuaciones
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Redes LAN y Cableado	Incremento de costos de operaciones Por fallan los equipos de interconexión lan y cableados utilizados: por fallas propias del equipo o equipos con fallas propias. sucediendo en cualquier momento
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Redes LAN y Cableado	Incremento de costos de operaciones. Porque fallan las contingencias eléctricas Como produciendo la indisponibilidad o quema de los equipos. Cuando existen cortes de fluido eléctrico y las plantas alternas o UPS no funcionan adecuadamente
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Enlaces y Redes WAN	Dejar de percibir ingresos. Por no se puede procesar en línea las transacciones Como consecuencia de fallas en los enlaces Cuando los equipos fallan, daños, u otros eventos que impiden la interconexión, existen daños en los equipos de interconexión o sus enlaces propios
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Enlaces y Redes WAN	Dejar de percibir ingresos. Porque los equipos pierden el fluido eléctrico Como consecuencia del corte o falta de elementos alternos Cuando el fluido eléctrico normal se pierde

DESCRIPCION PROCESO				
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Enlaces y Redes WAN	Incremento de la operatividad del área. Por no están actualizadas las rutas y mapa de red Como consecuencia de no contar con un esquema de actualización. Cuando no se ha solicitado las nuevas incorporaciones de red
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de costos de operaciones, reposición. Por daño de los equipos o elementos como cintas. Deterioro de los suministros, mala programación, hardware sin mantenimiento . Cuando; no existe un adecuado mantenimiento de los medios y hardware que intervienen en este proceso
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de costos de operaciones, reposición. Por el software falla. Consecuencia de una errada configuración. Cuando; esta ha sido manipulada o no monitoreada
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de la operatividad del área. Porque no se cuenta con los respaldos etiquetados y correctamente almacenados por un salto al procedimiento de almacenamiento y etiquetación. Cuando el analista no realiza el trabajo de forma adecuada
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de costos de operaciones, reposición. Por daño de los equipos o elementos como cintas. deterioro de los suministros, mala programación, hardware sin mantenimiento . Cuando; no existe un adecuado mantenimiento de los medios y hardware que intervienen en este proceso
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de costos de operaciones, reposición. Por el software falla. consecuencia de una errada configuración . Cuando; esta ha sido manipulada o no monitoreada

DESCRIPCION PROCESO				
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de costos de operaciones, reposición. Por el software falla. consecuencia de una errada configuración . Cuando; esta ha sido manipulada o no monitoreada
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de costos de operaciones, reposición. Por daño de los equipos o elementos como cintas. Deterioro de los suministros, mala programación, hardware sin mantenimiento. Cuando; no existe un adecuado mantenimiento de los medios y hardware que intervienen en este proceso
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de costos de operaciones, reposición. Por daño de los equipos o elementos como cintas. Deterioro de los suministros, mala programación, hardware sin mantenimiento. Cuando; no existe un adecuado mantenimiento de los medios y hardware que intervienen en este proceso
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de la operatividad del área. Porque las imágenes no son grabadas o respaldadas acorde al proceso existente debido a que los jefes de agencias obvian proc3esos. el equipo falla o se comete omisiones
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de costos de operaciones, reposición. Por el software falla. consecuencia de una errada configuración . Cuando; esta ha sido manipulada o no monitoreada

DESCRIPCION PROCESO				
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de costos de operaciones, reposición. Por daño de los equipos o elementos como cintas. Deterioro de los suministros, mala programación, hardware sin mantenimiento. Cuando; no existe un adecuado mantenimiento de los medios y hardware que intervienen en este proceso
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Seguridades físicas y lógicas de aplicaciones	Incremento de costos de operaciones por reposición o indemnizaciones Por saltar procesos establecido Como la falta de seguimiento a los mismos. Cuando ingresan personal no autorizado al área de IT.
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Seguridades físicas y lógicas de aplicaciones	Incremento de la operatividad del área Por los procesos propios de ingreso no son cumplidos Como porque los usuarios no cumplen. internamente no se controla el ingreso
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Seguridades físicas y lógicas de aplicaciones	Incremento de operatividad del área. Por falta de registro reingreso posterior de los registros sin firmas de responsabilidad, se saltan los procesos de ingreso y notación en las bitácoras respectivas
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Organización de TI	Definición de plan estratégico-operativo de TI	Pérdida de productividad del área de TI Porque no contar con un área que controles los proyectos entre las áreas funcionales y tecnología, por la no priorización de proyectos institucionales
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Organización de TI	Definición de plan estratégico-operativo de TI	Que Pérdida de identificación de soluciones para la institución Porque no contar con un portafolio de aplicaciones y sistemas, no contar con una metodología en base a las mejores prácticas.

DESCRIPCION PROCESO				
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Organización de TI	Definición de plan estratégico-operativo de TI	Que perdida de identificación de proyectos y su plan de implementación Porque no existe un marco de trabajo para la gestión de proyectos, al realizar los proyectos estos no culminen en la línea base y fracasen
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Organización de TI	Definición de plan estratégico-operativo de TI	Que no se difundan las políticas, procedimientos y estándares de servicio Por que no se cuenta con un Área que realice la Gestión de Niveles de Servicio, una aplicación falle y no se del seguimiento por que no está definido el SLA
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Organización de TI	Definición de plan estratégico-operativo de TI	Que las aplicaciones tengan defectos por no realizar la evaluación respectiva Porque no existe software para realizar el capacity management, cuando una aplicación degrade su performance
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Organización de TI	Definición de estructura y responsabilidades de TI	Que el proceso de reclutamiento de personal de TI no cumpla las políticas y procedimientos de la institución Por que no se realice la evaluación técnica y competencias que requiere el cargo especializado, por no cumplir con la evaluación requerida
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Organización de TI	Definición de estructura y responsabilidades de TI	Que el proceso de capacitación e inducción no se realice apenas el recurso ingrese a la institución Por que no se cuente con una planificación de capacitación e inducción en el Área, ingrese y no conozca los procedimientos a realizar

DESCRIPCION PROCESO				
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Organización de TI	Definición de estructura y responsabilidades de TI	Que no se realicen las evaluaciones periódicamente contra las metas e indicadores del Área Por que no se cuenta con una medición del desempeño y evaluación de indicadores, no se mide las métricas de desempeño
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Organización de TI	Definición de estructura y responsabilidades de TI	Que no se tomen las medidas expeditas respecto a los cambios de puestos, desvinculación o renuncia del recurso Por que no exista un sistema de entrega/recepción del puesto, se cumpla el que y no realiza el acta de entrega de puesto.
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Monitoreo y Evaluación de TI	Monitoreo y control interno de TI	Incremento en la operatividad del área debido a la ejecución errónea de los procesos de cierre por personal nuevo.
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Monitoreo y Evaluación de TI	Monitoreo y control interno de TI	Perdida de la imagen del área debido a la ejecución errónea de los procesos de cierre por personal nuevo.
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Monitoreo y Evaluación de TI	Monitoreo y control interno de TI	Pérdida de imagen del área debido a la falta de planificación en el tiempo adicional del sistema requerido por otras áreas debido a solicitudes tardías de habilitación.
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Monitoreo y Evaluación de TI	Monitoreo y control interno de TI	Incremento en la productividad por falta del monitoreo de aplicaciones del analista de turno por la falta de concientización.
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Monitoreo y Evaluación de TI	Monitoreo y control interno de TI	Pérdida de imagen del área por falta del monitoreo de aplicaciones del analista de turno por la falta de concientización.

DESCRIPCION PROCESO				
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Aplicaciones de operaciones	Pérdida de productividad del área por la no participación en la revisión del software antes de la adquisición lo que provoca que al momento de la instalación se no se analicen los sistemas que pueden verse afectados en su conjunto
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Aplicaciones de operaciones	Pérdida de productividad del área, por el desconocimiento de las especificaciones y la certificación del software y hardware de las aplicaciones lo que puede ocasionar el no funcionamiento o mal funcionamiento de las aplicaciones y equipos
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Aplicaciones de operaciones	Pérdida de productividad del área por las llamadas de soporte en los aplicativos o software instalados y solicitados por otras áreas; debido a la falta de conocimiento del aplicativo y de un doliente que conozca el aplicativo al 100%
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Aplicaciones de operaciones	Pérdida de productividad del área por la no participación en la revisión del software antes de la adquisición lo que provoca que al momento de la instalación no se conozca la arquitectura de la aplicación y la integración con nuestros sistemas
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Cambios	Pérdida de productividad del área debido a requerimientos no acordes a lo que necesita el usuario por la falta de información detallada en el documento RFC que se recibe (inexactitud del proceso requerido).

DESCRIPCION PROCESO				
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Cambios	Pérdida de imagen del área debido a requerimientos no acordes a lo que necesita el usuario por la falta de información detallada en el documento RFC que se recibe (inexactitud del proceso requerido).
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Cambios	Incremento en la productividad del área debido al desconocimiento de los usuarios del proceso global que se requiere automatizar lo que puede ocasionar que el cambio no se efectué dentro de los sistemas, no se aplique de forma correcta y no cumpla con lo requerido por el usuario.
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Cambios	Pérdida de imagen del área debido al desconocimiento de los usuarios del proceso global que se requiere automatizar lo que puede ocasionar que el cambio no se efectué dentro de los sistemas, no se aplique de forma correcta y no cumpla con lo requerido por el usuario.
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Cambios	Pérdida de productividad del área por la falta un guion detallado de pruebas que registre excepciones y particularidades puede ocasionar que el producto desarrollado no sea de buena calidad
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Cambios	Pérdida de imagen del área por la falta un guion detallado de pruebas que registre excepciones y particularidades puede ocasionar que el producto desarrollado no sea de buena calidad
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Cambios	Incremento de la operatividad por documentación o programas recibidos incompletos por parte del proveedor lo que ocasiona puestas en producción tardías

DESCRIPCION PROCESO				
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Cambios	Perdida de reputación por documentación o programas recibidos incompletos por parte del proveedor lo que ocasiona puestas en producción tardías
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión del Gobierno de IT	Los componentes de COBIT 4.1 no sean mejorados desde las necesidades iniciales hasta la implantación de la solución Porque no se utilice la hoja de ruta de proyectos para el Gobierno de TI, en todo el ciclo de estructura del Gobierno de TI
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión del Gobierno de IT	Que no exista una alineación estratégica priorizando la implementación de nuevas Tecnologías de información Porque no se identifiquen las necesidades y alcances respectivos, cuando se realice la fase inicial del proyecto.
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión del Gobierno de IT	Que no exista un monitoreo con forme los proyectos avancen, que afecte la toma de decisiones Porque no exista medidas de control, cuando el proyecto este ejecutándose.
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión del Gobierno de IT	Que no esté identificado el plan de implementación Por que no se identifique necesidades, visión solución, plan de solución y implementación de solución, cuando el proyecto no cumpla los hitos.
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Proyectos	Que los requerimientos funcionales no tengan una justificación o incidencia económica Porque no existe un marco de trabajo definido en la institución, al iniciar un proyecto sin el respectivo factor costo - beneficio.

DESCRIPCION PROCESO				
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Proyectos	Que la implementacion y estabilización en producción no cumpla los tiempos establecidos Porque debido a que no existe un area de Change managament y release managament, al iniciar la solicitud y al culminar el hito de pruebas.
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Proyectos	Que la aplicación de problemas al usuario final provocando inestabilidad Porque no se elabore un plan del rollback en el proyecto, pasa a producción la aplicación sufra problemas y no exista el plan
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Proyectos	Que no se realicen las propuestas conforme al RFP realizado Porque debido a que los proveedores terceros no contemplen todos las especificaciones, al realizar el envío de convocatoria a proveedores.

Tabla 2 Riesgos por Proceso de TI

3.1.3 EVALUACIÓN DE RIESGOS

Una vez levantados los riesgos por procesos en la matriz preliminar, se procede a evaluar los riesgos en la misma matriz, la cual constituye una herramienta flexible que documenta los procesos y evalúa de manera integral el riesgo de la Institución, la cual permite realizar un diagnóstico objetivo de la situación global de riesgo de la Entidad. La formulación de la matriz exige la participación activa de las unidades de negocios, operativas y funcionales en la definición de la estrategia institucional.

La Entidad define a la Matriz de Riesgos como la combinación de medición y priorización de riesgos que consiste en la medición del impacto y la frecuencia esperada de los eventos a partir de estos resultados se define una escala de calificación definidos en grupos tales como: Extremo, Alto, Medio y Bajo.

Posteriormente, se procede a establecer los controles que permitan mitigar el riesgo a través de un plan de acción.

La siguiente tabla muestra la evaluación de riesgos y los controles, después de la aplicación de la metodología adoptada por la Entidad financiera, la AZ-NZS:4360 [9].

DESCRIPCION PROCESO					IMPACTO	PROBABILIDAD	RIESGO	No. de Controles	CONTROL
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo					
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	Incremento de la productividad del área por retrasos en las entregas de equipos y servidores que dilatan otras actividades del personal del IT. debido a actividades ya establecidas o calendarizadas al personal de IT que no cumplen con los tiempos establecidos	2	2	4	1	Solicitud de preparación de equipos y servidores en el F11
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	Incremento en los costos de operación por los equipos que deben ser retornados al área de IT para su revisión por preparación errónea o instalaciones no adecuadas que no dan el funcionamiento que el usuario requiere, además, se preparan equipos y servidores sin tomar en cuenta la función que va a desempeñar el mismo	2	2	4	1	Acta de entrega recepción de equipos con el destinatario y función a cumplir
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	Incremento en los costos de operación. Por Los equipos no funcionan adecuadamente . por las fallas en el Sistema Operativo. los sistemas operativos se corrompen o han sido instalados o manipulados de forma errónea	2	2	4	1	Equipo maestro en funcionamiento clonado para la preparación
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	incremento de la productividad del área. Por se necesita la reinstalación de la aplicación. instalación mal efectuada o no realizada. no funciona o no tiene el adobereader	1	1	1	1	Equipo maestro en funcionamiento clonado para la preparación

DESCRIPCION PROCESO					IMPACTO	PROBABILIDAD	RIESGO	No. de Controles	CONTROL
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo					
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	incremento de la productividad del área. Por realiza revisiones en las impresoras ingresando al equipo del cliente para la revisión de la impresora el usuario no puede imprimir	1	2	2	1	impresión de la hoja de prueba
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	incremento de la productividad del área. Por es necesario la revisión nuevamente del equipo o servidor. el mismo presenta fallas en las configuraciones por defecto. el usuario no puede realizar o usar adecuadamente las aplicaciones de la Cooperativa	1	1	1	1	Equipo maestro en funcionamiento clonado para la preparación
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	incremento en los costos de operación. Porque no funcionan las cámaras de vigilancia. por fallas en los equipo o software. no presenta las imágenes a grabar	1	1	1	1	Acta de entrega recepción de equipos con el funcionamiento correcto
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Equipos y Servidores	incremento de la productividad del área: Por al no permitir ingresar con un usuario super administrador a dar soporte al ingresar a un equipo y servidor con este usuario: cuando se requiere soporte sobre el equipo o servidor	1	1	1	1	Equipo maestro en funcionamiento clonado para la preparación
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Licenciamiento	Incremento de costos porque se dan adquisiciones de licencias no adecuadas como parte de un errado análisis del proceso de adquisición, cuando la institución o usuario solicitan un licenciamiento	2	2	4	1	Solicitud de adquisición de licencias y tipo

DESCRIPCION PROCESO					IMPACTO	PROBABILIDAD	RIESGO	No. de Controles	CONTROL
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo					
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Licenciamiento	Incremento de la operatividad del área porque se deben reingresar y revisar todas las adquisiciones como parte del ingreso de licencias adquiridas cuando se adquieren nuevas licencias	1	2	2	1	Hoja de registro de licencias
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Soporte a Usuarios	Incremento en la operatividad del área, porque hay incidentes no resueltos, como resultado de un SLA fuera del ámbito definido como consecuencia de obviar los puntos de escalamiento Cuando estos no son entregados acorde a la matriz y SLA previamente acordados en la institución	2	2	4	1	monitoreo de los SLA's ingresados y cumplidos
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Soporte a Usuarios	Perdida de productividad del área, Porque son requerimiento ingresado sin su debido respaldo o con deficiencias en la descripción resultado de un desconocimiento del usuario Cuando este no describe claramente el problema a ser ingresado en el F11	1	2	2	1	capacitaciones y noticias para un correcto ingreso de requerimientos
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Bases de Datos	Incremento en costos de operación, Por se aplicaron procesos de dimensionamiento no adecuados. el tener datos no exactos de crecimiento de los últimos 3 años mas el incremento proyectado. se realizan las actividades de capacity planing del a Base de datos	3	1	3	1	Capacity Planning inicio de año Plan operativo

DESCRIPCION PROCESO					IMPACTO	PROBABILIDAD	RIESGO	No. de Controles	CONTROL
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo					
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Bases de Datos	Incremento de la operatividad del área Por existen datos que causan lentitud en las operaciones. por la no aplicación correcta de las operaciones de depuración: Cuando no se lo realizan con la planificación existente mensual	4	2	8	1	Site Alterno
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Bases de Datos	Incremento en costos de operación, Por no se llevan a cabo un continuo monitoreo de las bases de datos. al no ejecutar las respectivas rutinas de visualización del estado delas B.D Cuando, no se ejecutan las mismas de forma diaria	3	2	6	1	Bitácoras de Monitoreo y respaldos de información
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Bases de Datos	Perdida de oportunidad del área. Porque al no ejecutar las rutinas de depuración. por la no ejecución de las ruticas. con los procesos mensuales definidos	3	2	6	1	Bitácoras de ejecución
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Redes LAN y Cableado	Incremento en la operatividad del área. Por se realiza un inadecuado análisis de cableado y medio de conexión Como. Al no intervenir o contar con todos los datos para el mapa lógico Cuando se ejecutan nuevas instalaciones o readecuaciones	2	2	4	1	Documento de aceptación de diseño y cableado
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Redes LAN y Cableado	Incremento de costos de operaciones Por fallan los equipos de interconexión lan y cableados utilizados: por fallas propias del equipo o equipos con fallas propias. sucediendo en cualquier momento	2	2	4	1	Equipos de contingencia

DESCRIPCION PROCESO					IMPACTO	PROBABILIDAD	RIESGO	No. de Controles	CONTROL
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo					
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Redes LAN y Cableado	Incremento de costos de operaciones. Porque fallan las contingencias eléctricas Como produciendo la indisponibilidad o quema de los equipos. Cuando existen cortes de fluido eléctrico y las plantas alternas o UPS no funcionan adecuadamente	2	2	4	1	Contrato de mantenimiento de UPS y pruebas de generadores
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Enlaces y Redes WAN	Dejar de percibir ingresos. Por no se puede procesar en línea las transacciones Como consecuencia de fallas en los enlaces Cuando los equipos fallan, daños, u otros eventos que impiden la interconexión, existen daños en los equipos de interconexión o sus enlaces propios	3	2	6	1	Enlaces de contingencia
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Enlaces y Redes WAN	Dejar de percibir ingresos. Porque los equipos pierden el fluido eléctrico Como consecuencia del corte o falta de elementos alternos Cuando el fluido eléctrico normal se pierde	3	2	6	1	Equipos eléctricos redundantes
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Enlaces y Redes WAN	Incremento de la operatividad del área. Por no están actualizadas las rutas y mapa de red Como consecuencia de no contar con un esquema de actualización. Cuando no se ha solicitado las nuevas incorporaciones de red	1	2	2	1	SLA's

DESCRIPCION PROCESO					IMPACTO	PROBABILIDAD	RIESGO	No. de Controles	CONTROL
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo					
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de costos de operaciones, reposición. Por daño de los equipos o elementos como cintas. deterioro de los suministros, mala programación, hardware sin mantenimiento . Cuando; no existe un adecuado mantenimiento de los medios y hardware que intervienen en este proceso	3	2	6	1	Contratos de mantenimiento
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de costos de operaciones, reposición. Por el software falla. consecuencia de una errada configuración . Cuando; esta ha sido manipulada o no monitoreada	3	2	6	1	Monitoreo de eventos del sistema
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de la operatividad del área. Porque no se cuenta con los respaldos etiquetados y correctamente almacenados por un salto al procedimiento de almacenamiento y etiquetación. Cuando el analista no realiza el trabajo de forma adecuada	2	2	4	1	Bitácora de respaldos
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de costos de operaciones, reposición. Por daño de los equipos o elementos como cintas. deterioro de los suministros, mala programación, hardware sin mantenimiento . Cuando; no existe un adecuado mantenimiento de los medios y hardware que intervienen en este proceso	3	2	6	1	Contratos de mantenimiento

DESCRIPCION PROCESO					IMPACTO	PROBABILIDAD	RIESGO	No. de Controles	CONTROL
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo					
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de costos de operaciones, reposición. Por el software falla. consecuencia de una errada configuración . Cuando; esta ha sido manipulada o no monitoreada	3	2	6	1	Monitoreo de eventos del sistema
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de costos de operaciones, reposición. Por el software falla. consecuencia de una errada configuración . Cuando; esta ha sido manipulada o no monitoreada	2	2	4	1	Bitácoras de pruebas
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de costos de operaciones, reposición. Por daño de los equipos o elementos como cintas. deterioro de los suministros, mala programación, hardware sin mantenimiento . Cuando; no existe un adecuado mantenimiento de los medios y hardware que intervienen en este proceso	2	2	4	1	Bitácoras de pruebas
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de costos de operaciones, reposición. Por daño de los equipos o elementos como cintas. deterioro de los suministros, mala programación, hardware sin mantenimiento . Cuando; no existe un adecuado mantenimiento de los medios y hardware que intervienen en este proceso	3	2	6	1	Bitácoras de respaldos de imágenes y etiquetado de DVD

DESCRIPCION PROCESO					IMPACTO	PROBABILIDAD	RIESGO	No. de Controles	CONTROL
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo					
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de la operatividad del área. Porque las imágenes no son grabadas o respaldadas acorde al proceso existente debido a que los jefes de agencias obvian proc3esos. el equipo falla o se comete omisiones	3	2	6	1	Bitácoras de respaldos de imágenes y etiquetado de DVD
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de costos de operaciones, reposición. Por el software falla. consecuencia de una errada configuración . Cuando; esta ha sido manipulada o no monitoreada	3	2	6	1	Monitoreo de eventos del sistema
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Respaldos	Incremento de costos de operaciones, reposición. Por daño de los equipos o elementos como cintas. deterioro de los suministros, mala programación, hardware sin mantenimiento . Cuando; no existe un adecuado mantenimiento de los medios y hardware que intervienen en este proceso	3	2	6	1	Contratos de mantenimiento
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Seguridades físicas y lógicas de aplicaciones	Incremento de costos de operaciones por reposición o indemnizaciones Por saltar procesos establecido Como la falta de seguimiento a los mismos. Cuando ingresan personal no autorizado al área de IT.	2	2	4	1	Acceso limitado al área con registro y aprobaciones
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Seguridades físicas y lógicas de aplicaciones	Incremento de la operatividad del área Por los procesos propios de ingreso no son cumplidos Como porque los usuarios no cumplen. internamente no se controla el ingreso	2	2	4	1	Control de bitácoras

DESCRIPCION PROCESO					IMPACTO	PROBABILIDAD	RIESGO	No. de Controles	CONTROL
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo					
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Seguridades físicas y lógicas de aplicaciones	Incremento de operatividad del área. Por falta de registro reingreso posterior de los registros sin firmas de responsabilidad, se saltan los procesos de ingreso y notación en las bitácoras respectivas	2	2	4	1	Control de bitácoras
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Organización de TI	Definición de plan estratégico-operativo de TI	Pérdida de productividad del área de TI Porque no contar con un área que controles los proyectos entre las áreas funcionales y tecnología, por la no priorización de proyectos institucionales	3	4	12	0	
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Organización de TI	Definición de plan estratégico-operativo de TI	Que Pérdida de identificación de soluciones para la institución Porque no contar con un portafolio de aplicaciones y sistemas, no contar con una metodología en base a las mejores prácticas.	3	4	12	0	
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Organización de TI	Definición de plan estratégico-operativo de TI	Que perdida de identificación de proyectos y su plan de implementación Porque no existe un marco de trabajo para la gestión de proyectos, al realizar los proyectos estos no culminen en la línea base y fracasen	3	4	12	0	
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Organización de TI	Definición de plan estratégico-operativo de TI	Que no se difundan las políticas, procedimientos y estándares de servicio Por que no se cuenta con un Área que realice la Gestión de Niveles de Servicio, una aplicación falle y no se de el seguimiento por que no esta definido el SLA	3	4	12	0	

DESCRIPCION PROCESO					IMPACTO	PROBABILIDAD	RIESGO	No. de Controles	CONTROL
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo					
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Organización de TI	Definición de plan estratégico-operativo de TI	Que las aplicaciones tengan defectos por no realizar la evaluación respectiva Por que no existe software para realizar el capacity management, cuando una aplicación degrade su performance	3	4	12	0	
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Organización de TI	Definición de estructura y responsabilidades de TI	Que el proceso de reclutamiento de personal de TI no cumpla las políticas y procedimientos de la institución Por que no se realice la evaluación técnica y competencias que requiere el cargo especializado, por no cumplir con la evaluación requerida	2	1	2	0	
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Organización de TI	Definición de estructura y responsabilidades de TI	Que el proceso de capacitación e inducción no se realice apenas el recurso ingrese a la institución Por que no se cuente con una planificación de capacitación e inducción en el Área, ingrese y no conozca los procedimientos a realizar	2	1	2	0	
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Organización de TI	Definición de estructura y responsabilidades de TI	Que no se realicen las evaluaciones periódicamente contra las metas e indicadores del Área Por que no se cuenta con una medición del desempeño y evaluación de indicadores, no se mide las métricas de desempeño	2	1	2	0	

DESCRIPCION PROCESO					IMPACTO	PROBABILIDAD	RIESGO	No. de Controles	CONTROL
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo					
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Organización de TI	Definición de estructura y responsabilidades de TI	Que no se tomen las medidas expeditas respecto a los cambios de puestos, desvinculación o renuncia del recurso Por que no exista un sistema de entrega/recepción del puesto, se cumpla el que y no realiza el acta de entrega de puesto.	2	1	2	0	
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Monitoreo y Evaluación de TI	Monitoreo y control interno de TI	Incremento en la operatividad del área debido a la ejecución errónea de los procesos de cierre por personal nuevo.	2	2	4	1	Bitácora de Cierre Diario
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Monitoreo y Evaluación de TI	Monitoreo y control interno de TI	Perdida de la imagen del área debido a la ejecución errónea de los procesos de cierre por personal nuevo.	2	2	4	1	Bitácora de Cierre Diario
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Monitoreo y Evaluación de TI	Monitoreo y control interno de TI	Perdida de imagen del área debido a la falta de planificación en el tiempo adicional del sistema requerido por otras áreas debido a solicitudes tardías de habilitación.	2	2	4	1	Registro en Service Desk / mails
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Monitoreo y Evaluación de TI	Monitoreo y control interno de TI	Incremento en la productividad por falta del monitoreo de aplicaciones del analista de turno por la falta de concientización.	2	1	2	1	Bitácora de Inicio y Fin de Día
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Monitoreo y Evaluación de TI	Monitoreo y control interno de TI	Perdida de imagen del área por falta del monitoreo de aplicaciones del analista de turno por la falta de concientización.	2	1	2	1	Bitácora de Inicio y Fin de Día
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Aplicaciones de operaciones	Perdida de productividad del área por la no participación en la revisión del software antes de la adquisición lo que provoca que al momento de la instalación se no se analicen los sistemas	2	4	8	0	

DESCRIPCION PROCESO					IMPACTO	PROBABILIDAD	RIESGO	No. de Controles	CONTROL
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo					
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Aplicaciones de operaciones	Pérdida de productividad del área, por el desconocimiento de las especificaciones y la certificación del software y hardware de las aplicaciones lo que puede ocasionar el no funcionamiento o mal funcionamiento de las aplicaciones y equipos	2	4	8	0	
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Aplicaciones de operaciones	Pérdida de productividad del área por las llamadas de soporte en los aplicativos o software instalados y solicitados por otras áreas; debido a la falta de conocimiento del aplicativo y de un doliente que conozca el aplicativo al 100%	2	3	6	1	F11
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Entrega y Soporte de TI	Aplicaciones de operaciones	Perdida de productividad del área por la no participación en la revisión del software antes de la adquisición lo que provoca que al momento de la instalación no se conozca la arquitectura de la aplicación y la integración con nuestros sistemas	3	4	12	0	
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Cambios	Perdida de productividad del área debido a requerimientos no acordes a lo que necesita el usuario por la falta de información detallada en el documento RFC que se recibe (inexactitud del proceso requerido).	2	3	6	1	Registro en Service Desk
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Cambios	Perdida de imagen del área debido a requerimientos no acordes a lo que necesita el usuario por la falta de información detallada en el documento RFC que se recibe .	2	3	6	1	Registro en Service Desk

DESCRIPCION PROCESO					IMPACTO	PROBABILIDAD	RIESGO	No. de Controles	CONTROL
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo					
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Cambios	Incremento en la productividad del área debido al desconocimiento de los usuarios del proceso global que se requiere automatizar lo que puede ocasionar que el cambio no se efectué dentro de los sistemas, no se aplique de forma correcta y no cumpla con lo requerido por el usuario.	2	3	6	1	Registro en Service Desk
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Cambios	Perdida de imagen del área debido al desconocimiento de los usuarios del proceso global que se requiere automatizar lo que puede ocasionar que el cambio no se efectué dentro de los sistemas, no se aplique de forma correcta y no cumpla con lo requerido por el usuario.	2	3	6	1	Registro en Service Desk
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Cambios	Perdida de productividad del área por la falta un guion detallado de pruebas que registre excepciones y particularidades puede ocasionar que el producto desarrollado no sea de buena calidad	2	3	6	1	Registro en Service Desk
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Cambios	Perdida de imagen del área por la falta un guion detallado de pruebas que registre excepciones y particularidades puede ocasionar que el producto desarrollado no sea de buena calidad	2	3	6	1	Registro en Service Desk

DESCRIPCION PROCESO					IMPACTO	PROBABILIDAD	RIESGO	No. de Controles	CONTROL
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo					
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Cambios	Incremento de la operatividad por documentación o programas recibidos incompletos por parte del proveedor lo que ocasiona puestas en producción tardías	2	3	6	1	Registro en Service Desk
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Cambios	Perdida de reputación por documentación o programas recibidos incompletos por parte del proveedor lo que ocasiona puestas en producción tardías	2	3	6	1	Registro en Service Desk
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión del Gobierno de IT	Los componentes de COBIT 4.1 no sean mejorados desde las necesidades iniciales hasta la implantación de la solución Porque no se utilice la hoja de ruta de proyectos para el Gobierno de TI, en todo el ciclo de estructura del Gobierno de TI	3	4	12	0	
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión del Gobierno de IT	Que no exista una alineación estratégica priorizando la implementación de nuevas Tecnologías de información Porque no se identifiquen las necesidades	3	4	12	0	
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión del Gobierno de IT	Que no exista un monitoreo con forme los proyectos avancen, que afecte la toma de decisiones Porque no exista medidas de control.	3	4	12	0	
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión del Gobierno de IT	Que no este identificado el plan de implementacion Por que no se identifique necesidades, visión solución, plan de solución y implementación de solución,	3	4	12	0	

DESCRIPCION PROCESO					IMPACTO	PROBABILIDAD	RIESGO	No. de Controles	CONTROL
TIPO DE PROCESO	MACROPROCESO	PROCESO	SUBPROCESO	Descripción del Riesgo					
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Proyectos	Que los requerimientos funcionales no tengan una justificación o incidencia ecónomica Porque no existe un marco de trabajo definido en la institución, al iniciar un proyecto sin el respectivo factor costo - beneficio.	3	4	12	0	
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Proyectos	Que la implementacion y estabilización en producción no cumpla los tiempos establecidos Porque debido a que no existe un area de Change managament y release managament, al iniciar la solicitud y al culminar el hito de pruebas.	3	4	12	0	
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Proyectos	Que la aplicación de problemas al usuario final provocando inestabilidad Porque no se elabore un plan del rollback en el proyecto, pasa a producción la aplicación sufra problemas y no exista el plan	3	4	12	0	
PROCESO DE SOPORTE	Gestión de Tecnología y de Telecomunicaciones	Adquisición e Implementación de TI	Gestión de Proyectos	Que no se realicen las propuestas conforme al RFP realizado Porque debido a que los proveedores terceros no contemplen todos las especificaciones, al realizar el envío de convocatoria a proveedores.	3	4	12	0	

Tabla 3 Evaluación de riesgos

3.1.4 VALORACIÓN DE ALTO NIVEL

Para la valoración de alto nivel, se desarrolló una herramienta en una hoja de cálculo, la cual permite asociar los subprocesos con los criterios de riesgo establecidos por la alta gerencia y ponderación respectiva de acuerdo al criterio del auditor, lo que generara el score que permitirá tener la valoración de alto nivel para su priorización, este procedimiento se efectuara por cada subproceso para posteriormente generar un reporte ordenado de acuerdo al score obtenido por criterio de riesgo y ponderación, el cual servirá para la elaboración de la planificación anual de auditoría. La valoración de alto nivel se muestra en la siguiente figura:

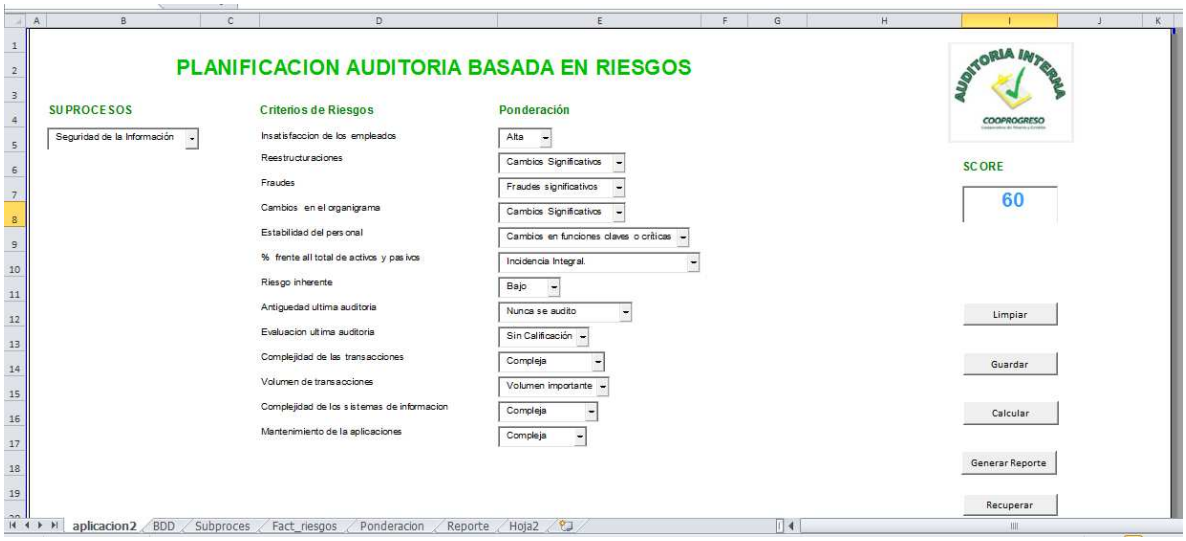


Figura 46 Herramienta Planificación Auditoría

La ponderación de los criterios de riesgos está definida por el nivel de incidencia del subproceso.

A continuación se presenta la ponderación planteada en el caso de estudio de acuerdo a sus respectivos criterios de riesgos [17].

El criterio 1, Insatisfacción de los empleados, se refiere a la insatisfacción de los empleados en cuanto a la capacidad y desempeño de los servicios ofrecidos, las aplicaciones, infraestructura, comunicaciones, entre otros.

CRITERIO 1	1
Insatisfacción de los empleados	
Baja	1
Media	2
Alta	3

Tabla 4 Criterio 1

El criterio 2, Reestructuraciones trata sobre los cambios que pudieron modificar ciertos procesos.

CRITERIO 2	1
Reestructuraciones	
No hubo cambios	1
Cambios moderados	2
Cambios significativos	3

Tabla 5 Criterio 2

El criterio 3, Fraudes, se refiere a si en el año se produjo algún tipo de fraude que ocasionó pérdidas financieras a la Entidad.

CRITERIO 3	1
Fraudes	
No hubo fraudes	1
Fraudes pequeños	2
Fraudes moderados	3
Fraudes significativos	4

Tabla 6 Criterio 3

El criterio 4, Cambios en el organigrama, se refiere a si existió una modificación en la estructura organizacional del área de TI.

CRITERIO 4	1
Cambios en el Organigrama	
No hubo cambios	1
Cambios moderados	5
Cambios significativos	9

Tabla 7 Criterio 4

El criterio 5, Estabilidad del personal, se refiere a la rotación que puede afectar el logro de los objetivos.

CRITERIO 5	1
Estabilidad del personal	
No se conocen cambios	1
Cambios que podrían afectar	5
Cambios en funciones claves o críticas	9

Tabla 8 Criterio 5

El criterio 6, % frente al total de activos y pasivos quiere decir la afectación que puede tener la ejecución de un determinado proceso.

CRITERIO 6	1
% frente al total de Activos y Pasivos	
Sin incidencia	1
Hasta el 5% del Total Act, Pasivos o Gtos	3
Entre el 5% y el 15% de Act. Pasivos o Gtos	5
Del 15% y más de Act, Pasivos o Gtos	7
Incidencia Integral.	9

Tabla 9 Criterio 6

El criterio 7 se refiera al riesgo que está presente en una actividad sin tener en cuenta el efecto de los controles.

CRITERIO 7	1
Riesgo Inherente	
Bajo	1
Medio Bajo	3
Medio	5
Medio Alto	7
Alto	9

Tabla 10 Criterio 7

El criterio 8, Antigüedad de la última Auditoría, se refiere a si ha efectuado o no un examen a uno de los subprocesos.

CRITERIO 8	1
Antigüedad Ultima Auditoría	
En los últimos 12 meses	1
En los últimos 24 meses	3
En los últimos 36 meses	5
Nunca se auditó	9

Tabla 11 Criterio 8

El criterio 9, Evaluación de la última auditoría se refiere al puntaje obtenido en el examen de auditoría efectuado a un proceso determinado.

CRITERIO 9	1
Evaluación última auditoría	
Adecuado	1
Aceptable	3
Regular	5
Deficiente	7
Sin Calificación	9

Tabla 12 Criterio 9

El criterio 10, Complejidad de las transacciones, se refiere al grado de dificultad en el procesamiento de las transacciones de las aplicaciones de software presentes en la Entidad y que representa una incidencia alta para la Entidad.

CRITERIO 10	1
Complejidad de las transacciones	
Bastante Simple	1
Simple	3
Moderada	5
Compleja	7

Tabla 13 Criterio 10

El criterio 11 Volumen de las transacciones, se refiere a la cantidad de transacciones obtenidas del proceso bajo revisión.

CRITERIO 11	1
Volumen de Transacciones	
Volumen mínimo	1
Volumen moderado	5
Volumen importante	9

Tabla 14 Criterio 11

El criterio 12, complejidad de los sistemas de información se refiere al grado de dificultad de los sistemas de información de la Entidad.

CRITERIO 12	1
Complejidad de los sistemas de información	
Bastante Simple	1
Simple	2
Moderada	3
Compleja	4

Tabla 15 Criterio 12

El criterio 13, Mantenimiento de las aplicaciones se refiere a la incidencia que puede tener el mantenimiento.

CRITERIO 13	1
Mantenimiento de la aplicaciones	
Bastante Simple	1
Simple	2
Moderada	3
Compleja	4

Tabla 16 Criterio 13

Después de ingresar los parámetros correspondientes se evalúa el score total a través de la herramienta, del cual se obtiene el reporte generado para el área de TI se podría mostrar como en la siguiente tabla.

SUBPROCESOS	SCORE
Gestión de Proyectos	53.7
Gestión Gobierno Corporativo	49.9
Gestión de Cambios	49.4
Monitoreo y Evaluación de TI	46.5
Base de Datos	40.3
Seguridades Físicas y Lógicas	39.9
Seguridad de la Información	36.4
Respaldos	31.9
Enlaces y comunicaciones	31
Aplicaciones de Operaciones	29.1
Definición Plan Estratégico y Operativo	29
Help Desk	23.1
Estructura y Responsabilidades TI	18.7
Inventario de Hardware y Software	18.2

Tabla 17 Score de los procesos de TI

3.1.5 DEFINICIÓN DEL PLAN

Una vez efectuada la valoración de alto nivel, el Auditor debe establecer el plan anual de auditoría asignando recursos y tiempos requeridos para efectuar cada una de las revisiones de los procesos de acuerdo al score obtenido. Por lo general, se asignan de 4 a 6 semanas para cada una de las revisiones, esto depende del grado de complejidad y el tamaño de las mismas. La siguiente figura es un ejemplo de un plan de auditoría anual.

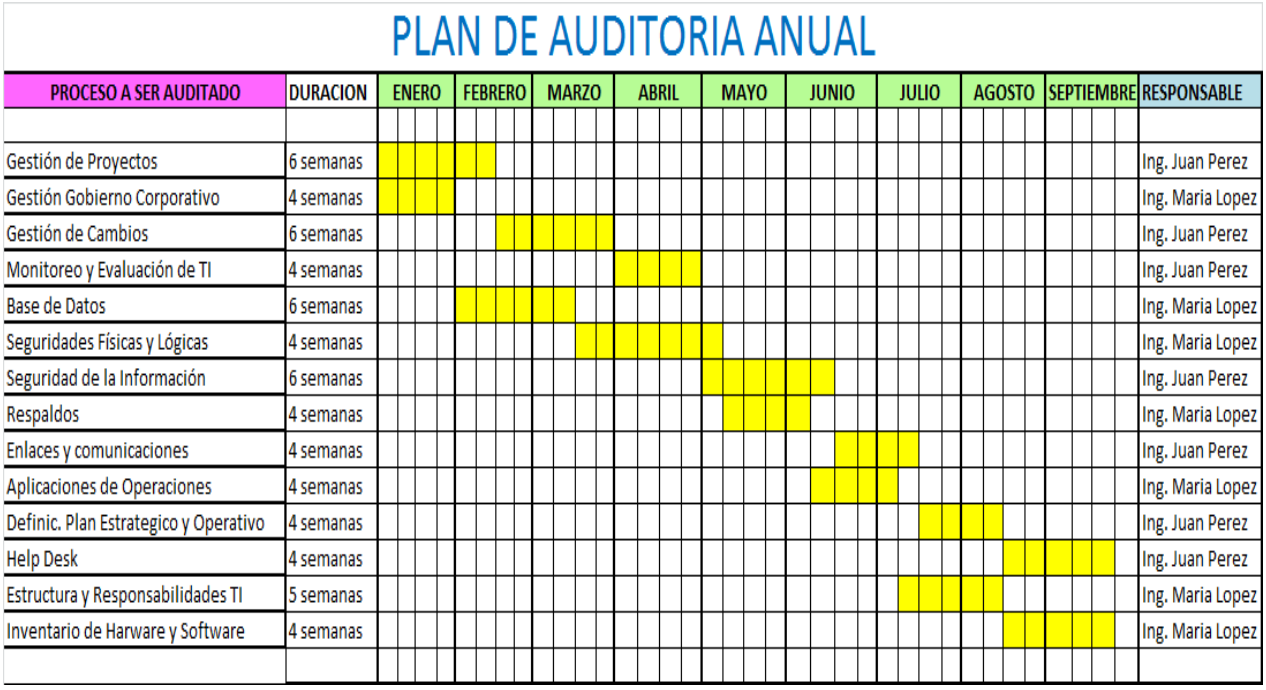


Figura 47 Plan Anual de Auditoría

3.2 DEFINICIÓN DEL ALCANCE

Para este caso de estudio se ha tomado el proceso Gestión de Proyectos que tiene el más alto score.

3.2.1 DEFINICIÓN DE LOS OBJETIVOS DE LA AUDITORÍA

La definición de los objetivos y el alcance de auditoría deben ser establecidos por el auditor responsable del proceso a ser evaluado, basado en la información obtenida de la valoración de alto nivel, que efectuó el Auditor General y para el cual fue asignado.

En la siguiente tabla se muestra el formato para la definición de los objetivos y el alcance del examen de auditoría.

PROCESO A SER AUDITADO:	GESTIÓN DE PROYECTOS
Responsable:	Ing. Juan Pérez
Objetivos:	• Revisar el procedimiento para la implementación proyectos informáticos • Evaluar la metodología adoptada por la Cooperativa para gestión de proyectos • Evaluar los templates establecidos para cada una de las fases de la gestión de proyectos • Revisión a los contratos establecidos para proyectos informáticos
Alcance:	Conforme al plan anual de Auditoría Interna, se desarrollará la revisión Gestión de Proyectos, que contempla la revisión del procedimiento para la implementación de proyectos informáticos, la metodología utilizada y los contratos de proyectos de TI.

Tabla 18 Definición de los objetivos de Auditoría

3.2.2 RELEVAMIENTO DEL PROCESO

El Auditor asignado efectuará un primer acercamiento con el dueño del proceso, con el fin de obtener un conocimiento claro del proceso que está auditando, el mismo que será documentado de forma general, obteniendo así el relevamiento del proceso.

En la siguiente tabla se muestra el formato para el relevamiento del proceso.

PROCESO A SER AUDITADO:	GESTIÓN DE PROYECTOS
Dueño del proceso:	Ing. Pablo Arias
Fecha de Acercamiento Inicial:	5 de Enero del 2012
Subprocesos:	• Implementación de proyectos informáticos • Ejecución de metodología para gestión de proyectos • Elaboración de Templates conforme a la metodología • Gestión de contratos de proyectos de TI
Relevamiento del proceso:	El área de Calidad y Procesos es la Unidad responsable de gestionar los proyectos institucionales, por lo que el subproceso gestión de proyectos de TI está inmerso en este proceso a nivel institucional, por lo que la implementación de proyectos informáticos debe estar alineada con la metodología adoptada por la Cooperativa enmarcada dentro del estándar PMBOK 4.0. En la metodología se consideran 5 fases: inicio, planificación, ejecución, cierre y monitoreo, como resultado de estas, se obtienen entregables formalizados. La formalidad con el proveedor de productos o servicios de TI se refleja en los contratos que deben existir físicamente, contener las cláusulas legales, mismas que evitarán conflictos con las partes, así como la vigencia de estos.

Tabla 19 Relevamiento del proceso a ser auditado

Obtención del Nivel de Madurez

El Auditor debe valorar el nivel de madurez del proceso apoyado en el modelo PAM [4], iniciando con la valoración del desempeño que aplica para todos los niveles del 1 al 5, tomando en cuenta que el cumplimiento de los objetivos de control debe basarse en evidencia tal como se indica en la siguiente figura:

ID	PO10		
Nombre del Proceso	Administración de Proyectos		
Propósito	Cumplir con los requisitos de negocio para asegurar la entrega de los resultados del proyecto dentro plazos acordados, presupuesto y calidad.		
Resultados (Os)	**Número**	**Descripción**	
	PO10-O1a	Esta definido un marco de gestión del programa?	SI
	PO10-O1b	Se sigue un marco de gestión del programa?	SI
	PO10-O1c	Se logró los resultados esperados con las contribuciones de los proyectos dentro del programa?	SI
	PO10-O1d	Se gestionan actividades, interdependencias, necesidades de recursos y conflictos de varios proyectos?	SI
	PO10-O2a	Se ha definido un marco de gestión de proyectos?	SI
	PO10-O2b	Los proyectos siguen un proceso de gestión de proyectos que requieren aprobaciones adecuadas, gestión, gestión de calidad y la supervisión?	SI
	PO10-O3	La planificación del proyecto se realiza para cada proyecto y se detalla en la cartera de proyecto?	SI
	PO10-O4	Existe compromiso y participación del negocio y usuarios finales en los proyectos?	SI

Prácticas Base (BPs)	Número	Descripción	Soporte
	PO10-BP1	Definir un marco de gestión de programa / cartera de inversiones en TI.	PO10-O1
	PO10-BP2	Establecer y mantener un marco de proyecto de gestión de TI.	PO10-O2
	PO10-BP3	Establecer y mantener un proyecto de TI, seguimiento, medición y gestión.	PO10-O2
	PO10-BP4	Construir Project Charter, programas, planes, presupuestos, comunicación y planes de gestión del riesgo.	PO10-O2
	PO10-BP5	Asegurar la participación y el compromiso de los interesados en el proyecto	PO10-O1c, O4
	PO10-BP6	Asegurar el control eficaz de los proyectos y los cambios del proyecto	PO10-O1b, O1c, O3
	PO10-BP7	Definir e implementar el aseguramiento de los proyectos y métodos de revisión.	PO10-O2

Entradas		
Número	**Descripción**	**Soporte**
PO1-WP3	Portafolio de proyectos de TI	PO10-O1, O2
PO5-WP4	Portafolio de proyectos de TI actualizado	PO10-O3
PO7-WP2	Matriz de habilidades de TI	PO10-O1a, O1b, O2a
PO8-WP2	Estandares de desarrollo	PO10-01, 02
AI7-WP5	Revisión post-implementación	PO10-O3, O4

Salidas			
Número	**Descripción**	**Entrada al**	**Soporte**
PO10-WP1	Reportes de desempeño del proyecto	ME1	PO10-O1b, O1d, O4
PO10-WP2	Plan de gestión de riesgos de proyectos	PO9, AI3	PO10-O1c, O1d, O3
PO10-WP3	Guias de gestion de proyectos	AI1 al AI7	PO10-02, 03
PO10-WP4	Planes de proyectos detallados	PO8, AI1 al AI7, DS6	PO10-O1c, O3
PO10-WP5	Portafolio de proyectos de TI actualizados	PO1, PO5	PO10-01, O3

Figura 48 Valoración de desempeño del proceso

Seguidamente, se procede con la obtención de la madurez del proceso, evaluando los atributos correspondientes y asignando un puntaje de logro alcanzado en el nivel del de madurez 1 como se indica en la siguiente figura:

PA 1.1 Rendimiento del proceso, una medida del grado en que se logra el propósito del proceso. El pleno desarrollo de los resultados de este atributo está en resultados definidos.			
Resultado de la plena realización de los atributos	**Prácticas Genéricas (GPs)**	**Productos de Trabajo genéricos (GWPs)**	
El proceso alcanza sus resultados definidos.	GP 1.1.1 Lograr los resultados del proceso. Hay evidencia de que la intención de la práctica de base está siendo realizado	Se producen productos de trabajo , que proporcionan evidencia de los resultados del proceso.	SI

Figura 49 Nivel de Madurez 1

Si cumple con establecido por este atributo tomando en cuenta las prácticas genéricas y los productos de trabajo como evidencia, se procede a evaluar el siguiente nivel como se indica en las siguientes figuras:

PA 2.1 Gestión del Rendimiento, una medida del grado en que se gestiona el rendimiento del proceso. Como resultado del logro pleno de este atributo: una. Se identifican los siguientes objetivos para el rendimiento del proceso: a. Fueron identificados objetivos para el desempeño del proceso? b. Se Organizó y se controló el rendimiento del proceso. c. Se ajusta el rendimiento del proceso para cumplir los planes. d. Se definen, asignan y comunican las responsabilidades y autoridades para la realización del proceso. e. Se identifica, pone a disposición, distribución y uso de recursos e información necesaria para realizar el proceso. f. Se gestionan las interfaces entre las partes involucradas se gestionan para garantizar una comunicación eficaz y una clara asignación de responsabilidades.			
Resultado de la plena realización de los atributos	**Prácticas Genéricas (GPs)**	**Productos de Trabajo genéricos (GWPs)**	
a. El proceso alcanza sus resultados definidos.	GP 2.1.1 Identificar los objetivos del rendimiento del proceso. Los objetivos del desempeño, el ámbito junto con las hipótesis y limitaciones, están definidas y son comunicadas.	GWP 1.0 La documentación de procesos debe describir el alcance del proceso. GWP 2.0 El plan de trabajo debería proporcionar los detalles de los objetivos de rendimiento del proceso	SI
b. Se Organizó y se controló el rendimiento del proceso.	GP 2.1.2 Planificar y controlar el rendimiento del proceso para cumplir con los objetivos identificados. Las medidas básicas de rendimiento de los procesos vinculados a objetivos empresariales se han establecido y monitoreado. Se incluyen los principales hitos, actividades requeridas, estimaciones y horarios.	GWP 2.0 El plan de trabajo debería proporcionar los detalles de los objetivos de rendimiento del proceso GWP 9.0 Los registros del rendimiento de proceso deben proporcionar detalles de los resultados. Nota: En este nivel, el registro de proceso el rendimiento puede ser: informes,resgistro de resultados o cualquier registro informal.	SI
c. Se ajusta el rendimiento del proceso se ajusta para cumplir los planes.	GP 2.1.3 Ajuste el rendimiento del proceso. Se toman medidas cuando el desempeño previsto no se alcanzado. Las acciones incluyen la identificación de problemas de rendimiento del proceso y el ajuste de los planes y horarios, según corresponda	GWP 4.0 Registro Calidad debería informar de la acción tomada cuando el rendimiento no se consigue.	SI
d. Se definen, asignan y comunican las responsabilidades y autoridades para la realización del proceso.	GP 2.1.4 Definir las responsabilidades y autorizaciones para realizar el proceso. Las principales responsabilidades y autorizaciones de ejecución de las actividades clave delproceso se definen, se asignan y se comunican. La necesidad de la experiencia del rendimiento del proceso, conocimientos y habilidades están definidas.	GWP 1.0 La documentación del proceso debe proporcionar la identificación del propietario del proceso y quién es el responsable, rendición de cuentas, consulta y / o informado (RACI). GWP 2.0 El plan de trabajo debe incluir detalles del plan de comunicación del proceso, así como la experiencia del rendimiento del proceso y las habilidades requeridas.	SI
e. Se identifica, pone a disposición, distribución y uso de recursos e información necesaria para realizar el proceso.	GP 2.1.5 Identificar y poner los recursos a disposición de realizar el proceso de acuerdo con el plan. Los recursos y la información necesaria para realizar las actividades clave del proceso se identifican, asignan y utilizan	GWP 2.0 El Plan de trabajo deberían proporcionar los detalles del plan de capacitación del proceso y plan del recursos del proceso.	SI
f. Se gestionan las interfaces entre las partes involucradas se gestionan para garantizar una comunicación eficaz y una clara asignación de responsabilidades.	GP 2.1.6 Gestionar las interfaces entre las partes involucradas. Los individuos y grupos involucrados con el proceso se identifican, las responsabilidades se definen y mecanismos eficaces de comunicación están bien ubicados.	GWP 1.0 La documentación del proceso debe proporcionar los detalles de las personas y grupos involucrados (proveedores, clientes y RACI). GWP 2.0 El plan de trabajo 2.0 deberían proporcionar los detalles del plan de comunicación del proceso.	SI

Figura 50 Nivel de Madurez II – Atributo 1

PA 2.2 Gestión de Producto de Trabajo: una medida del alcance para que los productos de trabajo producidos por el proceso son apropiadamente gestionados. Los productos de trabajo a que se refiere la presente cláusula son aquellos que se derivan de la consecución de los resultados del proceso. Como resultado de plena realización de este atributo: a. Se han definido los productos de trabajo del proceso b. Se han definido los requisitos para la documentación y el control de los productos de trabajo c. Los productos de trabajo estén debidamente identificados, documentados y controlados. d. Los productos de trabajo se revisan de acuerdo con los planes previstos, y los ajustes necesarios para cumplir con los requisitos. Nota: Los requisitos para la documentación y el control de los productos de trabajo pueden incluir requisitos para la identificación de los cambios y estado de revisión, aprobación y re-aprobación de los productos del trabajo, y la creación de versiones pertinentes de los productos de trabajo aplicables disponibles en los puntos de uso.			
Resultado de la plena realización de los atributos	**Prácticas Genéricas (GPs)**	**Productos de Trabajo genéricos (GWPs)**	
a. Se han definido los productos de trabajo del proceso	GP 2.2.1 Definir los requisitos para los productos de trabajo incluyendo la estructura y contenido de calidad de los criterios.	GWP3.0 El plan de calidad debe proporcionar los detalles de criterios de calidad y contenido y estructura de los del productos de trabajo.	SI
b. Se han definido los requisitos para la documentación y el control de los productos de trabajo	GP 2.2.2 Definir los requisitos para la documentación y el control de los productos de trabajo. Esto debería incluir la identificación de las dependencias, aprobaciones y la trazabilidad de los requisitos.	GWP 1.0 La documentación de procesos debe proporcionar los detalles de los controles (control de la matriz). GWP 3.0 El Plan de calidad debería proporcionar los detalles del producto de trabajo, criterios de calidad, requerimientos de documentación y control de cambios.	SI
c. Los productos de trabajo estén debidamente identificados, documentados y controlados.	GP 2.2.3 Identificar, documentar y controlar los productos de trabajo. Los productos de trabajo están sujetas a cambios, control de versiones y gestión de la configuración según sea apropiado.	GWP 3.0 El Plan de calidad debería proporcionar los detalles del producto de trabajo, criterios de calidad, requerimientos de documentación y control de cambios.	SI
d. Los productos de trabajo se revisan de acuerdo con los planes previstos, y los ajustes necesarios para cumplir con los requisitos.	GP 2.2.4 Revisar y ajustar los productos de trabajo para cumplir con los requisitos definidos. Los productos de trabajo son objeto de revisión versus los requerimientos en acuerdo con lo planificado y cualquier tema que surge es resulto.	GWP4.0 Los registros de calidad deben proporcionar pistas de auditoría de los exámenes realizados.	NO

Figura 51 Nivel de Madurez II – Atributo 2

Como para el caso de estudio si cumple con los atributos para el Nivel de Madurez II, se evaluará el siguiente nivel, ver siguiente figura:

PA 3.1 Definición del proceso: una medida del alcance que mantiene un proceso estándar para apoyar el despliegue del proceso definido. Como resultado de la realización completa de este atributo: a. Un proceso estándar, incluyendo las directrices apropiadas, se define, describe los elementos fundamentales que deben ser incorporados en un proceso definido. b. Esta determinada la secuencia y la interacción del proceso estándar con otros procesos. c. Se identifican competencias y roles requeridos para llevar a cabo un proceso como parte del proceso estándar. d. Se identifican Infraestructura requerida y ambiente de trabajo para realizar un proceso como parte del proceso estándar. e. Se determinan los métodos adecuados para el seguimiento de la eficacia e indoneidad del proceso. Nota: Un proceso estándar puede ser utilizado como cuando se despliega un proceso definido, en el que las guias deberian ser necesarias.			
Resultado de la plena realización de los atributos	**Prácticas Genéricas (GPs)**	**Productos de Trabajo genéricos (GWPs)**	
a. Un proceso estándar, incluyendo las directrices apropiadas, se define, describe los elementos fundamentales que deben ser incorporados en un proceso definido.	GP 3.1.1 Definir el proceso estándar que apoyara la implementación del proceso definido. Un proceso estándar es definido cuando identifica los elementos fundamentales de este y proporciona la guia y procedimientos para apoyar la aplicación y orientación sobre la forma en que se puede adaptar cuando sea necesario.	GWP 5.0 Políticas y estandares deben proporcionar detalles de los objetivos de la organización para el proceso, los estándares mínimos de desempeño, estandares de procedimientos y requerimientos de informes y seguimiento. El requisito probatorio en este nivel no es sólo que las políticas y las normas existan, sino que se apliquen en toda la organización.	SI
b. Esta determinada la secuencia y la interacción del proceso estándar con otros procesos.	GP 3.1.2 Determinar la secuencia e interacción entre los procesos para que funcionen como un sistema integrado. El estandar de la secuencia y la interacción con otros procesos se determinan y se mantiene cuando un proceso se implementa en diferentes partes de la organización.	GWP 5.0 Políticas y estandares deben proporcionar un mapeo con los detalles de los procesos estándar y las secuencias e interacción esperadas. El requisito probatorio a este nivel no es sólo que existan las políticas y estandares, sino que se aplique a través de la organización.	NO
c. Se identifican competencias y roles requeridos para llevar a cabo un proceso como parte del proceso estándar.	GP 3.1.3 Identificar los roles y Competencias para realizar el Proceso Estándar.	GWP 5.0 Políticas y estandares deben proporcionar detalles de las funciones y competencias para llevar a cabo. El requisito probatorio en este nivel no es sólo que las políticas y estandares, sino que se aplique a través de la organización.	SI
d. Se identifican Infraestructura requerida y ambiente de trabajo para realizar un proceso como parte del proceso estándar.	GP 3.1.4 Identificar la infraestructura necesaria y el ambiente de trabajo para la realización del proceso estandar. La infraestructura (instalaciones, herramientas,métodos, etc) y el ambiente de trabajo para ejecutar el proceso estándar se identifican.	GWP 5.0 Políticas y estandares deben identificar infraestructura mínima requerida y el ambiente de trabajo para realizar el proceso. El requisito probatorio en este nivel no es sólo que las políticas y estandares, sino que se aplique a través de la organización.	NO
e. Se determinan los métodos adecuados para el seguimiento de la eficacia e indoneidad del proceso.	GP 3.1.5 Determinar los métodos adecuados para el seguimiento la eficacia y la idoneidad del proceso estandar, incluida la garantía de que los criterios apropiados y los datos necesarios para el seguimiento de la eficacia y la factibilidad del proceso esten definidos, y se establece la necesidad de llevar a cabo la auditoría interna y revisión por la dirección.	GWP 5.0 Políticas y estandares deben proporcionar detalles de los objetivos de la organización para el proceso, estándares mínimos de desempeño, estandares de procedimientos y requerimientos de informes y seguimiento. El requisito probatorio en este nivel no es sólo que las políticas y las normas existan, sino que se apliquen en toda la organización. GWP 4.0 Registros de calidad y GWP 9.0 registros de desempeño del procesos proporcionan la evidencia de exámenes realizados.	NO

Figura 52 Nivel de Madurez III – Atributo 1

Para el nivel 3 ya no se cumple con los parámetros del atributo 1, por lo que no es necesario continuar con la evaluación del siguiente atributo, seguidamente se procede a cuantificar el cumplimiento como se describe en las siguientes figuras:

PA 1.1 Rendimiento del proceso, una medida del grado en que se logra el propósito del proceso. El pleno desarrollo de los resultados de este atributo está en resultados definidos.

Cumple	100.0%
No cumple	0.0%

PUNTAJE:	**F**

Figura 53 Evaluación Nivel de Madurez I

PA 2.1 Gestión del Rendimiento, una medida del grado en que se gestiona el rendimiento del proceso. Como resultado del logro pleno de este atributo: una. Se identifican los siguientes objetivos para el rendimiento del proceso:
a. Fueron identificados objetivos para el desempeño del proceso?
b. Se Organizó y se controló el rendimiento del proceso.
c. Se ajusta el rendimiento del proceso para cumplir los planes.
d. Se definen, asignan y comunican las responsabilidades y autoridades para la realización del proceso.
e. Se identifica, pone a disposición, distribución y uso de recursos e información necesaria para realizar el proceso.
f. Se gestionan las interfaces entre las partes involucradas se gestionan para garantizar una comunicación eficaz y una clara asignación de responsabilidades.

Objetivos	Cumple	No cumple	Peso
a	x		16.7%
b	x		16.7%
c	x		16.7%
d	x		16.7%
e	x		16.7%
f	x		16.7%
			100.0%

Cumple	100.0%
No cumple	0.0%

PUNTAJE:	**F**

Figura 54 Evaluación Nivel de Madurez – Atributo 1

PA 2.2 Gestión de Producto de Trabajo: una medida del alcance para que los productos de trabajo producidos por el proceso son apropiadamente gestionados. Los productos de trabajo a que se refiere la presente cláusula son aquellos que se derivan de la consecución de los resultados del proceso. Como resultado de plena realización de este atributo:
a. Se han definido los productos de trabajo del proceso
b. Se han definido los requisitos para la documentación y el control de los productos de trabajo
c. Los productos de trabajo estén debidamente identificados, documentados y controlados.
d. Los productos de trabajo se revisan de acuerdo con los planes previstos, y los ajustes necesarios para cumplir con los requisitos.
Nota: Los requisitos para la documentación y el control de los productos de trabajo pueden incluir requisitos para la identificación de los cambios y estado de revisión, aprobación y re-aprobación de los productos del trabajo, y la creación de versiones pertinentes de los productos de trabajo aplicables disponibles en los puntos de uso.

Objetivos	Cumple	No cumple	Peso
a	x		25.0%
b	x		25.0%
c	x		25.0%
d		x	25.0%
			100.0%

Cumple	75.0%
No cumple	25.0%

PUNTAJE:	**L**

Figura 55 Evaluación Nivel de Madurez II – Atributo 2

PA 3.1 Definición del proceso: una medida del alcance que mantiene un proceso estándar para apoyar el despliegue del proceso definido. Como resultado de la realización completa de este atributo:
a. Un proceso estándar, incluyendo las directrices apropiadas, se define, describe los elementos fundamentales que deben ser incorporados en un proceso definido.
b. Esta determinada la secuencia y la interacción del proceso estándar con otros procesos.
c. Se identifican competencias y roles requeridos para llevar a cabo un proceso como parte del proceso estándar.
d. Se identifican Infraestructura requerida y ambiente de trabajo para realizar un proceso como parte del proceso estándar.
e. Se determinan los métodos adecuados para el seguimiento de la eficacia e indoneidad del proceso.
Nota: Un proceso estándar puede ser utilizado como cuando se despliega un proceso definido, en el que las guias deberian ser necesarias.

Objetivos	Cumple	No cumple	Peso
a	x		20.0%
b		x	20.0%
c	x		20.0%
d		x	20.0%
e		x	20.0%
			100.0%

Cumple	40.0%
No cumple	60.0%

PUNTAJE:	**P**

Figura 56 Evaluación Nivel de Madurez III – Atributo I

A fin de obtener un mejor conocimiento sobre la evaluación del nivel de madurez del proceso sobre el cumplimiento de sus atributos es adecuado efectuar un cuadro resumen como se indica a continuación:

NOMBRE EL PROCESO EVALUADO	Nivel 1	Nivel 2		Nivel 3	
	PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2
Proceso Gestión de Cambios	F	F	L	P	N

NIVEL DE CAPACIDAD:	*Gestionado*

3.2.3 SELECCIÓN DEL MARCO DE REFERENCIA

Una vez efectuado el Relevamiento del Proceso Gestión de Proyectos, el Auditor procede a seleccionar el Marco de Referencia, el cual permitirá la seguridad de que ningún proceso relacionado se quede por fuera sin ser evaluado. Para el caso de estudio Gestión de Proyectos de TI se escogerán los marcos de referencia relacionados tal como se muestra en la siguiente tabla.

PROCESO A SER AUDITADO:	**GESTIÓN DE PROYECTOS**	
Marco de Referencia:	COBIT 4.1	Dominio: Planificación y Organización, Proceso: PO10 Administrar Proyectos

Tabla 20 Marco de Referencia seleccionado

3.2.4 IDENTIFICACIÓN DE LOS SUBPROCESOS DE TI A SER EVALUADOS

Para este caso de estudio se va a evaluar todos los subprocesos del proceso Gestión de Proyectos de TI, en vista de que nunca se ha efectuado una auditoría de éste, la tabla 21 muestra los subprocesos seleccionados para el examen.

MARCO DE REFERENCIA:	**COBIT 4.1**
Subprocesos de TI a ser evaluados:	• Implementación de proyectos informáticos • Ejecución de metodología para gestión de proyectos • Elaboración de Templates conforme a la metodología • Gestión de contratos de proyectos de TI

Tabla 21 Identificación de subprocesos a ser evaluados

3.2.5 SELECCIÓN DE LOS OBJETIVOS DE CONTROL A SER USADOS PARA LA AUDITORÍA

Una vez seleccionados los subprocesos a ser evaluados se escogen los objetivos de control a ser usados como referencia de control para la auditoría tal como muestra la tabla 22.

OBJETIVOS DE CONTROL SELECCIONADOS:	• **PO10.1** Marco de Trabajo para la Administración de Programas • **PO10.2** Marco de Trabajo para la Administración de Proyectos • **PO10.3** Enfoque de Administración de Proyectos • **PO10.4** Compromiso de los interesados • **PO10.5** Declaración de Alcance del Proyecto • **PO10.6** Inicio de las Fases del Proyecto • **PO10.8** Recursos del Proyecto • **PO10.13** Medición del Desempeño, Reporte y Monitoreo del proyecto • **PO10.14** Cierre del Proyecto

Tabla 22 Selección de objetivos de control

Como resultado de la aplicación de todos los pasos anteriores el Auditor obtendrá un documento como el que se muestra en la siguiente figura:

DEFINICION DE ALCANCE Y OBJETIVOS

Revisión:	Gestión de Proyectos de TI
Responsable:	Ing. Juan Perez

Objetivos:

1. Revisar el procedimiento para la implementacion de proyectos informaticos.
2. Evaluar la metodologia adoptada por la cooperativa para gestión de proyectos
3. Evaluar los templates establecidos para cada una de las fases de gestion de proyectos
4. Revisión a los contratos establecidos para proyecctos informaticos.

Alcance: Conforme al plan anual de Auditoría Interna, se desarrollará la revisión Gestión de Proyectos, que contempla la revisión del procedimiento para la implementación de proyectos informáticos, la metodología utilizada y los contratos de proyectos de TI.

RELEVAMIENTO DEL PROCESO

MARCO GENERAL:	**SUBPROCESOS:**
El área de Calidad y Procesos es la Unidad responsable de gestionar los proyectos institucionales, por lo que el subproceso gestión de proyectos de TI está inmerso en este proceso a nivel institucional, por lo que la implementación de proyectos informáticos debe estar alineada con la metodología adoptada por la Cooperativa enmarcada dentro del estándar PMBOK 4.0. En la metodología se consideran 5 fases Inicio, planificación, ejecución, cierre y monitoreo, como resultado de estas, se obtienen entregables formalizados. La formalidad con el proveedor de productos o servicios de TI se refleja en los contratos qlue deben existir físicamente, contener las cláusulas legales, mismas que evitarán conflictos con las partes, así como la vigencia de estos.	Implementación de proyectos informáticos Ejecución de metodología para gestión de proyectos Elaboración de Templates conformae a la metodología Gestión de contratos de proyectos de TI

Marco de Referencia de Control

COBIT 4.1	Dominio:	Planificación y Organización
	Proceso:	PO10 Administrar Proyectos

Nivel de Madurez

Nivel de Madurez:	Gestionado (2)

Marco de Referencia de Control

Implementación de proyectos informáticos
Ejecución de metodología para gestión de proyectos
Elaboración de Templates conformae a la metodología
Gestión de contratos de proyectos de TI

Objetivos de Control a ser usados

PO10.1	Marco de Trabajo para la Administración de programas
PO10.2	Marco de Trabajo para la Administración de Proyectos
PO10.3	Enfoque de Administración de Proyectos
PO10.4	Compromiso de los Interesados
PO10.5	Declaración de Alcance del Proyecto
PO10.6	Inicio de las Fases del Proyecto
PO10.8	Recursos del Proyecto
PO10.13	Medición del Desempeño, Reporte y Monitoreo del proyecto
PO10.14	Cierre del Proyecto

Figura 57 Definición de alcance y objetivos

3.3 EJECUCIÓN

3.3.1 ENTENDIMIENTO DEL OBJETO DE LA REVISIÓN

A fin de entender más claramente el entorno para efectuar la auditoría el Auditor debe apoyarse en una plantilla que le permitirá establecer de forma detallada, el responsable, la fecha de inicio y fin de la revisión, el área a ser auditada, los objetivos de la revisión, el contenido de la auditoría, las entradas, salidas y el procedimiento utilizado para el desarrollo de la misma. La siguiente figura muestra la plantilla a utilizarse para el caso de estudio:

PLAN DETALLADO DE PROCESO AUDITADO No. 1 -2012

Revisión:	Gestion de Proyectos TI		
Responsable:	Ing. Juan Perez		
Fecha de Incio:	2 de Enero 2012	**Fecha Fin:**	10 de Febrero del 2012
Area Auditada:	Tecnologia		

Objetivos:

1 Revisar el procedimiento para la implementación proyectos informáticos
2 Evaluar la metodología adoptada por la Cooperativa para gestión de proyectos
3 Evaluar los templates establecidos para cada una de las fases de la gestión de proyectos
4 Revisión a los contratos establecidos para proyectos informáticos

CONTENIDO DE LA AUDITORIA	ENTRADAS	SI	NO	SALIDAS	SI	NO	PROCEDIMIENTO
Implementación de proyectos informáticos	Portafolio de proyectos de TI actualizado Matriz de Responsabilidades	√		Plan de Implementacion de Proyectos (plan Operativo)	√		Validar si la implementación de proyectos informáticos está alineada con la metodología de gestión de proyectos adoptada por la Cooperativa Validar si Tecnología cumple con los estándares establecidos para la elaboración de entregables
Metodología para Gestión de proyectos	Manual de Gestion de Proyectos Manual de Funciones del Oficial de Proyecctos y del Comite de Proyectos	√		Actas del Comite de Proyectos	√		Solicitar metodología de proyectos Validar si se da cumplimiento a la metodología adoptada por la Cooperativa Verificar si existe un responsable para la Gestión de Proyectos Validar si se ha establecido el perfil para el Oficial de Proyectos Verificar si la metodología ha sido difundida a los funcionarios de la Cooperativa Verificar si se han establecido las funciones y responsabilidades para el Comité de Proyectos Verificar si se ha definido periodicidad para reuniones del Comité de Proyectos Solicitar las actas del Comité de Proyectos Validar si el Manual de Proyectos ha sido aprobado por el Comité de Proyectos y el CDA. Validar si se cuenta con una herramienta automatizada para Gestión de Proyectos
Templates de metodologia	Manual de Gestion de Proyectos Plantillas	√		Entregables de cada fase del ciclo de vida del proyecto	√		Validar si los templates para los entregables de cada una de las fases de Gestión de Proyectos solventan las necesidades de la Cooperativa y están en base a la metodología
Contratos de proyectos de TI	Contratos	√		Contratos	√		Revisar la existencia física de los contratos vigentes de TI Revisar términos contractuales establecidos entre los proveedores y la Cooperativa y validar con lo establecido en el Manual de Adquisiciones

Figura 58 Plan detallado del proceso a ser auditado

3.3.2 REFINAMIENTO DEL ALCANCE

El refinamiento del alcance consiste, para el caso de estudio, en asociar los riesgos, objetivos de control asociados a los subprocesos a ser auditados además de la ampliación del alcance bajo este criterio. Como resultado de este paso se obtiene el documento que se muestra en la siguiente figura:

REFINAMIENTO DEL ALCANCE No.1-2012

Revisión:	Gestion de Proyectos TI		
Responsable:	Ing. Juan Perez		
Fecha de Incio:	2 de Enero 2012	**Fecha de Fin:**	10 de Febrero del 2012
Area Auditada:	Tecnologia		

Objetivos:	
	1 Revisar el procedimiento para la implementación proyectos informáticos
	2 Evaluar la metodología adoptada por la Cooperativa para gestión de proyectos
	3 Evaluar los templates establecidos para cada una de las fases de la gestión de proyectos
	4 Revisión a los contratos establecidos para proyectos informáticos

Alcance Refinado:	Conforme al plan anual de Auditoría Interna, se desarrollará la revisión Gestión de Proyectos, que contempla la revisión del procedimiento para la implementación de proyectos informáticos, la metodología utilizada y los contratos de proyectos de TI, los riesgos asociados a cada uno de los subprocesos y los objetivos de control utilizados para evaluar el proceso auditado como se detalla a continuacion.

Marco de Referencia de Control	
• COBIT 4.1	Dominio: Planificación y Organización, Proceso: PO10 Administrar Proyectos

SUBPROCESOS	RIESGOS EXISTENTES	OBJETIVOS DE CONTROL	PROCEDIMIENTO	Nivel de Riesgo		
				Alto	Medio	Bajo
Implementación de proyectos informáticos	Incumplimiento de requerimientos solicitados por el usuario Consumo inefectivo de recursos Pérdidas financieras elevadas	PO10.1 Marco de Trabajo para la Administracion de Programas PO10.2 Marco de Trabajo para la Administracion de Proyectos. PO10.5 Declaración de Alcance del Proyecto PO10.6 Inicio de las Fases del Proyecto PO10.13 Medición del Desempeño, Reporte y Monitoreo del proyecto	Validar si la implementación de proyectos informáticos está alineada con la metodología de gestión de proyectos adoptada por la Cooperativa Validar si Tecnología cumple con los estándares establecidos para la elaboración de entregables		X	
Ejecución de metodología para gestión de proyectos	Incumplimiento de lo establecido por la Coooperativa Falta de formalidad en cada fase de la gestión de proyectos	PO10.1 Marco de Trabajo para la Administracion de Programas PO10.2 Marco de Trabajo para la Administracion de Proyectos. PO10.5 Declaración de Alcance del Proyecto PO10.6 Inicio de las Fases del Proyecto PO10.8 Recursos del Proyecto PO10.13 Medición del Desempeño, Reporte y Monitoreo del proyecto PO10.14 Cierre del Proyecto	Solicitar metodología de proyectos Validar si se da cumplimiento a la metodología adoptada por la Cooperativa Verificar si existe un responsable para la Gestión de Proyectos Validar si se ha establecido el perfil para el Oficial de Proyectos Verificar si la metodología ha sido difundida a los funcionarios de la Cooperativa Verificar si se han establecido las funciones y responsabilidades para el Comité de Proyectos Verificar si se ha definido periodicidad para reuniones del Comité de Proyectos Solicitar las actas del Comité de Proyectos Validar si el Manual de Proyectos ha sido aprobado por el Comité de Proyectos y el CDA. Validar si se cuenta con una herramienta automatizada para Gestión de Proyectos	X		
Elaboración de Templates conforme a la metodología	Documentos inconsistentes con la metodología adoptada por la Cooperativa	PO10.2 Marco de Trabajo para la Administración de Proyectos	Validar si los templates para los entregables de cada una de las fases de Gestión de Proyectos solventan las necesidades de la Cooperativa y están en base a la metodología		X	
Gestión de contratos de proyectos de TI	Contratos caducados Incumplimiento de la prestación de servicios Problemas de tipo legal por incumplimiento de las partes	PO10.4 Compromiso de los interesados	Revisar la existencia física de los contratos vigentes de TI Revisar términos contractuales establecidos entre los proveedores y la Cooperativa y validar con lo establecido en el Manual de Adquisiciones	X		

Figura 59 Refinamiento del alcance

3.3.3 PRUEBAS DEL DISEÑO DEL CONTROL

Las pruebas del diseño del control se efectúan a fin de determinar si el control existe y quien es el responsable, para lo cual el Auditor puede apoyarse en listas de chequeo o cuestionarios, para esto se deben registrar los subprocesos pertenecientes al proceso que está siendo auditado, así como los objetivos de control relacionados, su cumplimiento y la evidencia que respalda este cumplimiento.

Para lo expuesto en el párrafo anterior se hace uso de una plantilla a fin de determinar el cumplimiento o no de los objetivos de control atados a los subprocesos del proceso bajo revisión, esto le permitirá al Auditor obtener una idea clara sobre si los objetivos de control existen y son efectivos sustentándose en la evidencia que permita tener la certeza de su existencia, la misma que será entregada de forma física o magnética por parte del dueño del proceso.

La siguiente figura muestra la lista de chequeo utilizada para probar el diseño del control.

PRUEBA DE DISEÑO DE CONTROL

Revisión:	Gestion de Proyectos TI		
Responsable:	Ing. Juan Perez		
Fecha de Incio:	2 de Enero 2012	**Fecha Fin:**	10 de Febrero del 2012
Area Auditada:	Tecnologia		

Marco de Referencia de Control

- **COBIT 4.1** Dominio: Planificación y Organización, Proceso: PO10 Administrar Proyectos

SUBPROCESOS	OBJETIVOS DE CONTROL	CUMPLIMIENTO		EVIDENCIA
		SI	NO	
Implementación de proyectos informáticos	PO10.1 Marco de Trabajo para la Administracion de Programas	x		Metodologia Pmbok 4.0
	PO10.2 Marco de Trabajo para la Administracion de Proyectos.	x		Metodologia Pmbok 4.0
	PO10.5 Declaración de Alcance del Proyecto	x		Project Charter
	PO10.6 Inicio de las Fases del Proyecto	x		Acta de Inicio
	PO10.13 Medición del Desempeño, Reporte y Monitoreo del proyecto	x		Actas de Avance de Proyecto
	PO10.14 Cierre del Proyecto	x		Acta de Cierre
Ejecución de metodología para gestión de proyectos	PO10.1 Marco de Trabajo para la Administracion de Programas	x		Manual de Gestion de Proyectos Institucionales
	PO10.2 Marco de Trabajo para la Administracion de Proyectos.	x		Manual de Gestion de Proyectos Institucionales
	PO10.5 Declaración de Alcance del Proyecto	x		Project Charter
	PO10.6 Inicio de las Fases del Proyecto	x		Acta de Inicio
	PO10.8 Recursos del Proyecto		x	
	PO10.13 Medición del Desempeño, Reporte y Monitoreo del proyecto	x		Actas de Avance de Proyecto
	PO10.14 Cierre del Proyecto	x		Acta de Cierre
Elaboración de Templates conforme a la metodología	PO10.2 Marco de Trabajo para la Administración de Proyectos	x		Plantillas de Todas las Fases del Proyecto
Gestión de contratos de proyectos de TI	PO10.4 Compromiso de los interesados	X		Contratos

Figura 60 Prueba de diseño de control

3.3.4 PRUEBAS DE LA EFICACIA OPERATIVA DEL CONTROL

Las pruebas de eficacia operativa están destinas a la verificación del funcionamiento del control, por lo que el Auditor deberá apoyarse en varias técnicas manuales y asistidas por computador a fin de validar si el control está operativo o no.

Para el objetivo expuesto se hace uso de una plantilla de evaluación de la eficacia operativa, la cual es el reflejo de la situación actual del proceso, producto o revisión efectuada y es la base para la redacción del informe y reportes; además, es el sustento para otorgar una calificación al proceso basados en el nivel de control, daño y riesgo, generando una TABLA DE EVALUACION. Esta debe contener las actividades o controles que se van a evaluar y que forman parte del proceso que se está revisando, deben incluirse los aspectos a revisar en todas las áreas que intervienen en el proceso; la cantidad o número de aspectos a revisar, evaluar, comprobar dependerá del proceso.

La matriz es de vital importancia ya que en esta se detallan todos los aspectos revisados; identificando el número de aciertos y errores encontrados por actividad y área interviniente en el proceso. Además se establece de manera general una calificación para los controles existentes y se obtiene a través de una tabla el nivel de riesgo existente.

Esta plantilla debe dividirse por subprocesos revisados; de tal manera que se pueda evaluar de manera independiente a cada uno y posteriormente unificar todos para obtener una evaluación global; lo mencionado permite evidenciar cual es el aspecto que mantiene más observaciones y que debe ser corregido. El obtener un promedio de todos los subprocesos evidenciará como se encuentra el cumplimiento y los riesgos de todo el proceso considerado en su conjunto. Todo lo expuesto se detalla en la siguiente figura:

PRUEBA DE EFICACIA OPERATIVA

Revisión:	Gestion de Proyectos TI		
Responsable:	Ing. Juan Perez		
Fecha de Incio:	2 de Enero 2012	**Fecha Fin:**	10 de Febrero del 2012
Area Auditada:	Tecnologia		

SUBPROCESOS	VERIFICACION DE APLICACIÓN DE PROCEDIMIENTOS	VALORACION	MUESTRAS ESPERADAS	MUESTRAS REALES		N/A	CUM.	
				SI	NO			
Implementación de proyectos informáticos	El subproceso Gestión de Proyectos está ubicado estratégicamente	5	1	1	0		5,00	
	La implementación de proyectos informáticos está alineada con la metodología adoptada por la Cooperativa?	5	1	1	0		5,00	
	Tecnología cumple con los estándares establecidos por la Cooperativa en cuanto a entregables?	5	1	0,8	0,2		4,00	
	TOTAL	**15**	**3**	**2,8**	**0,2**		**14**	
	Porcentaje de cumplimiento						**93,33**	**ACEPTABLE**
Ejecución de metodología para gestión de proyectos	Existe una metodología para Gestión de Proyectos?	5	1	1	0		5,00	
	Se cumple la metodología de Gestión de Proyectos?	5	1	0,2	0,8		1,00	
	Ha sido difundida la metodología de Gestion de Proyectos?	5	1	0,5	0,5		2,50	
	Existe un responsable de la Gestión de Proyectos?	5	1	1	0		5,00	
	Se ha establecido un perfil para el Oficial de Proyectos?	5	1	1	0		5,00	
	Existe un Comité de Proyectos?	5	1	1	0		5,00	
	Se han establecido funciones para el Comité de Proyectos?	5	1	1	0		5,00	
	Se ha establecido periodicidad de reuniones para el Comité de Proyectos y esta se cumple?	5	1	0,5	0,5		2,50	
	Existen actas de las reuniones del Comité de Proyectos?	5	2	2	0		5,00	
	El Manual de Proyectos ha sido aprobado por el Comité de Proyectos?	5	1	1	0		5,00	
	El Manual de proyectos cuenta con los parámetros que se ajustan a las necesidades de la Institución, es decir, es aplicable a todos los proyectos de la Institución, valor del proyecto, areas funcionales, tiempo, proceso, estructura organizativa, descripcion entregables, glosario de términos?	5	7	4	3		2,86	
	El Manual de Gestión de Proyectos ha sido aprobado por el Consejo de Administración?	5	1	0	1		0,00	
	La Cooperativa cuenta con una herramienta para gestión de proyectos formalizada?	5	1	0,5	0,5		2,50	
	TOTAL	**65**	**20**	**13,7**	**6,3**		**46,36**	
	Porcentaje de cumplimiento						**71,32**	**DEFICIENTE**
Elaboración de Templates conforme a la metodología	Los templates se han elaborado en base a la metodología adoptada por la Cooperativa, PMBOK?	5	5	5	0		5,00	
	Los templates elaborados para el ciclo de vida de los proyectos solventan las necesidades de la Cooperativa	5	5	3,5	1,5		3,50	
	Se han definido plantillas para proyectos que no son considerado institucionales	5	1	0	1		0,00	
	TOTAL	**15**	**11**	**8,5**	**2,5**		**8,5**	
	Porcentaje de cumplimiento						**56,67**	**DEFICIENTE**
Gestión de contratos de proyectos de TI	Para los proyectos de TI, se cuenta con los documentos	5	3	2,5	0,5		4,17	
	Los contratos contienen los términos contractuales	5	15	14	1		4,67	
	TOTAL	**10**	**18**	**16,5**	**1,5**		**8,83**	
	Porcentaje de cumplimiento						**88,33**	**ACEPTABLE**

TABLA DE EVALUACION PROMEDIO

AREA	CALIFICACION	EVALUACION	CONTROL	ONDERACIO	DAÑO	RIESGO
Implementación de proyectos informáticos	93,33	ACEPTABLE	2,00	10,00	1,00	2,00
Ejecución de metodología para gestión de proyectos	71,32	DEFICIENTE	3,00	15,00	1,50	4,50
Elaboración de Templates conforme a la metodología	56,67	DEFICIENTE	3,00	10,00	1,00	3,00
Gestión de contratos de proyectos de TI	88,33	ACEPTABLE	2,00	15,00	1,50	3,00
Total por Áreas	**309,65**		**10**	**50**	**5**	**13**
Resultado Promedio	**77,41**	**REGULAR**	**2,50**	**12,50**	**1,25**	**3,13**

TABLA DE EVALUACIÓN		
PONDERACION	Correspondencia	
0 - 75	Deficiente	
76 - 85	Regular	3
86 - 95	Aceptable	2
96 -100	Adecuado	1

			DAÑO		
			Alto	Medio	Bajo
CONTROL		CONTROL	3	2	1
	Requiere mejoras URGENTES	3	9	6	3
	Requiere mejoras	2	6	4	2
	Satisfactorio	1	3	2	1

RIESGO	Alto	5	9
	Medio	2,5	4,9
	Bajo	1	2,4

Figura 61 Plantilla prueba eficacia operativa

3.3.5 ELABORACIÓN DEL INFORME Y COMUNICACIÓN DE LOS RESULTADOS.

3.3.5.1 Elaboración del Informe

El informe es un documento en el que deben constar las observaciones encontradas, las recomendaciones planteadas para solucionar los hallazgos detectados, así como las respuestas dadas por los dueños de los procesos quienes se comprometen a realizar acciones para mejorar los hallazgos; siendo necesario que se establezcan fechas de cumplimiento, por todo lo mencionado es importante establecer un esquema para la elaboración de los informes de auditoría. Para el caso de estudio se propone la siguiente estructura:

a. Objetivos y Alcance
b. Antecedentes
c. Hallazgos encontrados en la revisión
d. Impacto
e. Recomendaciones
f. Respuesta de los dueños de los procesos auditados que incluye fecha de implementación de las recomendaciones y entregables
g. Conclusiones

Al informe, se debe anexar un **Resumen Ejecutivo** el cual es documento que contiene un extracto de la auditoría a fin de tener una idea general del estado del proceso, sus observaciones y recomendaciones, mismo que será la hoja de presentación principal para la comunicación de resultados.

Además, el área de Auditoría se apoya en la herramienta ERA (Enterprise Risk Assessor), la cual le permitirá al Auditor evaluar los subprocesos de forma integral, sobre un enfoque de riesgos. Esta herramienta está basada en

la norma ISO 31000 [18] y básicamente en la AZ-NZS:4360 [9]. Un ejemplo del uso de la herramienta se lo puede apreciar en el Anexo No. 5.

Es importante indicar que cuando el Auditor observa hallazgos de alto riesgo debe comunicar de manera inmediata a la Gerencia responsable, es decir, que no se debe esperar la culminación de la revisión y la presentación del informe.

Es de vital importancia que la persona que redacta el informe lo haga de manera clara y precisa de tal manera que la o personas que lean el informe comprendan lo que se está comunicando.

El informe de auditoría contendrá recomendaciones tendientes a mejorar el sistema administrativo y financiero, el control interno, convertir las debilidades en fortalezas, aprovechar las oportunidades, evitar las amenazas y disminuir los riesgos. Las recomendaciones deben ser factibles de ejecutarse y deben contar con la aceptación de dueño del proceso, quien es la persona encargada de verificar el cumplimiento del compromiso asumido.

Objetivos y Alcance: Se registra los objetivos establecidos para la revisión del caso de estudio, además, el alcance que la auditoría.

Antecedentes: Es el detalle de lo que llevó al desarrollo de la actual auditoría.

Descripción del Hallazgo: Se describe el incumplimiento, contravención, falta de documentación, conocimiento, etc. de los controles, constituye el motivo de la observación; además, se indica que ocasiona el problema, es decir, la causa de la observación (desconocimiento, errores de supervisión, inadecuada segregación de funciones, falta de capacitación, entrenamiento, manuales, instructivos, información, etc.).

Impacto: Consiste en detallar a que conlleva el problema, cuáles son las connotaciones más importantes, los efectos del error u omisión: información inconsistente, pérdida potencial, mal servicio, etc.

Recomendación o sugerencia de solución y sus alternativas: Una solución correcta se debe a un problema bien identificado y sustentado. En algunos casos la solución es implícita (que se retomen procedimientos, re instruir al personal, regularizar, etc.). En otros casos es necesario recomendar algo nuevo, idear controles, formularios, cambios a procedimientos, constituye el apoyo o aporte a la Administración.

Respuestas de involucrados, compromiso y fecha de regularización: Estas deben ser claras y referentes al punto reportado y a las recomendaciones planteadas, las fechas deben ser objetivas y con plazos acordes a la complejidad de la observación.

Se debe tener en cuenta que todas las observaciones son identificadas determinando la importancia de las mismas así: Alto, moderado y bajo.

Conclusiones: El informe debe contener una conclusión objetiva que indique de manera concreta los problemas encontrados, de no existir novedades se debe mencionar lo indicado. Deberá, además, incluirse la calificación en función del nivel de riesgo de los aspectos evaluados en la plantilla de controles. Si intervienen más de un área en el proceso revisado, esta calificación deberá ser determinada para cada área en función del grado de responsabilidad sobre el aspecto evaluado.

3.3.5.2 Comunicación de Resultados

Una vez elaborado el informe este debe ser entregado a la Gerencia Responsable, a su vez estos documentos serán puestos en conocimiento de la Alta Gerencia con el fin de que se conozca si existen debilidades o falencias en el subproceso o subproceso evaluados y cuáles van a ser la medidas correctivas que la Gerencia responsable se ha comprometido a mitigar, así como el plazo para logra el compromiso.

A continuación se muestra el resumen ejecutivo para el caso de estudio, un ejemplo de resumen completo se puede revisar en el Anexo No. 6.

RESUMEN EJECUTIVO

TABLA DE CONTENIDO

1. OBJETIVOS Y ALCANCE

OBJETIVOS:

• Revisar el procedimiento para la implementación de proyectos informáticos

• Evaluar la metodología adoptada por la Cooperativa para gestión de proyectos

• Evaluar los templates establecidos para cada una de las fases de proyectos

• Revisión de contratos establecidos para proyectos informáticos

ALCANCE:

Conforme al plan anual de Auditoría Interna, se desarrolló la revisión Gestión de Proyectos, que contempla la revisión del procedimiento para la implementación de proyectos informáticos, la metodología utilizada y los contratos de proyectos de TI.

2. ANTECEDENTES

La gestión de proyectos institucionales no estaba normada, por lo que la Cooperativa adoptó la metodología PMBOK, para gestión de proyectos en Junio de 2011; al ser un tema de alta importancia para la Institución, se incluyó en la planificación de auditoría para el año 2012 a fin de analizar la madurez alcanzada una vez implementada la metodología.

3. CONCLUSIONES

• El nivel de Madurez logrado por el proceso de Gestión de Proyectos es nivel 2: Gestionado, por lo tanto la Cooperativa debe tomar acciones a fin de subir un escalón más en su madurez y mejorar la gestión de todos los subprocesos relacionados.

• La Cooperativa ha adoptado una metodología para gestión de los proyectos institucionales, la cual está en fase inicial de difusión a las diferentes áreas.

• La metodología PMBOK adoptada por la Cooperativa en Junio de 2011 está siendo aplicada en forma esporádica para los proyectos institucionales y de Tecnología, debido a que esta no ha sido sociabilizada adecuadamente, es decir, el uso de los templates establecidos para cada una de las fases del ciclo de vida del proyecto no se usan en su totalidad.

• En la Cooperativa se instituyó un Comité de Proyectos en Mayo de 2011, el cual se ha reunido una única vez en el año 2011 y en Abril de 2012, durante el transcurso de la presente revisión, sin dar cumplimiento, con lo establecido en el Manual de Comités en cuanto a la frecuencia de reunión.

• En la Intranet está publicado el Instructivo Administración de Proyectos CoopABC, sin embargo, se ha elaborado el Manual Administración de Proyectos el cual aún no ha sido aprobado por el Consejo de Administración, aspecto que es importante regularizar a fin de contar con un documento completo y formalizado.

• En el Manual de Administración de proyectos no se especifica como regular proyectos importantes que por su trascendencia deben ser considerados como proyectos institucionales. Además, no se incluye la estructura jerárquica y su línea de reporte, no se incluye la estructura del proceso (alcance, flujograma, descripción del proceso) que es el estándar de todos los manuales de la Cooperativa, y el glosario de términos es demasiado extenso y se incluyen términos que no tienen relación en ninguna parte del manual.

• El Analista de Proyectos actualmente cumple funciones solo de coordinación, por lo que es importante revisar las funciones y establecer un rol de gestión de proyectos.

• Actualmente, la Cooperativa no cuenta con una herramienta de gestión de proyectos formalizada, la cual permita gestionar de manera adecuada y organizada actividades, recursos tiempos y costos.

• Los riesgos establecidos para el subproceso Gestión de Proyectos de TI fueron levantados por el área de Tecnología, al existir un área para gestión de proyectos, estos deben ser validados por el área actualmente responsable, así como también incluir riesgos que a criterio de Auditoría deben ser incluidos en la matriz de riesgos.

• En resumen la evaluación integral al proceso de Estructura y Responsabilidades de Tecnología, registra una calificación de 77,41 con un sistema de control interno REGULAR, generando un riesgo MODERADO.

4. RESULTADOS

Se efectuó la valoración del Nivel de Madurez para el proceso Gestión de Proyectos, donde se observa que alcanza el nivel 2: Gestionado, toda vez que se ha procedido a evaluar los atributos correspondientes de cada nivel, a continuación se presenta el cuadro resumen:

NOMBRE EL PROCESO EVALUADO	**Nivel 1**	**Nivel 2**		**Nivel 3**	
	PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2
Proceso Gestión de Cambios	F	F	L	P	N

NIVEL DE CAPACIDAD:	*Gestionado*

Una vez medido el nivel de madurez del proceso, a continuación se detallan los hallazgos encontrados al efectuar la evaluación del proceso sobre amenazas y vulnerabilidades que causa un impacto considerable para la Institución

4.1. Metodología para Gestión de Proyectos

4.1.1. Metodología no aplicada

Referencia	Categorización Hallazgos	Importancia
GEPR-002	Riesgo operativo	Alto

Descripción

La metodología adoptada por la Cooperativa es PMBOK, a partir de ésta se elaboró el instructivo ADMINISTRACIÓN DE PROYECTOS EN COOPABC, el cual está publicado en la Intranet institucional y que fue difundido con fecha 02 de Junio de 2011 a todos las Gerencias y Jefaturas para su aplicación.

En la conversación mantenida con el Analista de Proyectos, se verificó que hasta la fecha no se está utilizando la metodología para ningún proyecto.

El Analista de Proyectos indicó que a partir de su incorporación a la Cooperativa con fecha 19 de Diciembre de 2011, se retomó el tema y que actualmente se está dando seguimiento, a través del control de cronogramas de control, a los siguientes proyectos institucionales que están en curso:

1. Workflow

2. Tarjeta de Crédito

3. Creer

Para los 2 primeros proyectos no existen los templates establecidos en el Instructivo que fue publicado en la Intranet el 02 Junio de 2011, a pesar de que Workflow y Tarjeta de Crédito fueron retomados de anteriores períodos de ejecución. Para el proyecto Creer se cuenta únicamente con plantillas de seguimiento y control.

Adicionalmente, el Analista de Proyectos nos proporcionó 4 informes de seguimientos a los proyectos mencionados, en donde se observa que no se especifica a quien va dirigido el informe, el asunto del informe, la fecha de emisión y la firma de responsabilidad. Además, se debería anexar el cronograma a fin de evidenciar el avance o retraso de los proyectos.

Es importante mencionar que en el transcurso de la revisión se efectuó una primera presentación de la metodología de Gestión de Proyectos a las diferente áreas de la Cooperativa (aspectos básicos tales como: políticas, estructura de la oficina de proyectos, roles y responsabilidades, fases del proyecto, entre

otros), sin embargo, esta charla no se incluyó una presentación sobre las plantillas de los entregables aplicables a cada una de las fases del ciclo de vida del proyecto.

4.1.2. Incumplimiento del Comité de Proyectos

Referencia	Categorización Hallazgos	Importancia
GEPR-003	Riesgo operativo	Moderado

Descripción

Se ha incumplido lo establecido en el documento Estructura y Operatividad Comité de Proyectos donde se menciona:

"El Comité se reunirá por lo menos una vez cada 3 meses en reunión ordinaria presidida por la Gerencia General. ..."

Sin embargo, en el año 2011 se ha efectuado únicamente una reunión del Comité con fecha 31 de Mayo, en la cual se trataron los siguientes temas:

• Estructura y Operatividad del Comité de Proyectos

• Lineamientos Generales para Manejo de Proyectos

• Definición de Proyectos

• Priorización de Proyectos

• Metodología para Administración de Proyectos

En el transcurso de la revisión se efectuó el Comité con fecha 30 de Abril de 2012.

Revisando el acta respectiva, entre los temas tratados en el Comité están:

1. Sanciones por incumplimientos

2. Ajuste de responsabilidades del Líder del Proyecto y del Analista de Proyectos

3. Se acepta la metodología de Administración de proyectos con los cambios planteados

4. Se autoriza la capacitación de la metodología y aprueba el material correspondiente orientado a las Gerencias y Jefaturas.

En esta acta no se registran fecha de cumplimiento para los temas que se establecen como pendientes (5 temas).

4.1.3. Manual no aprobado por CDA

Referencia	Categorización Hallazgos	Importancia
GEPR-004	Riesgo operativo	Moderado

Descripción

La capacitación recibida en el mes de Mayo de 2012, se basó en el Manual que ha sido elaborado por el Analista de Proyectos, el mismo que aún no ha sido aprobado por el Consejo de Administración. En la Intranet se observa el instructivo mismo que no estaría vigente, por cuanto lo que actualmente regiría es lo establecido en el Manual.

4.1.4. Manual de proyectos inconsistente

Referencia	Categorización Hallazgos	Importancia
GEPR-005	Riesgo operativo	Moderado

Descripción

En el Manual de proyectos se han establecido 5 dimensiones para que un proyecto sea considerado como institucional, sin embargo, pueden existir proyectos importantes que por su trascendencia deban ser considerados como tales.

Así mismo se debe incluirse los siguientes puntos:

• Descripción clara de los entregables por cada fase del proyecto.

• Estructura jerárquica y su línea de reporte de los participantes de los proyectos

• Estructura del proceso (alcance, flujograma, descripción del proceso) que debe estar conforme al estándar para la elaboración de los manuales de la Institución.

• El glosario de términos debe contener solo términos usados en el Manual, en el documento aparecen 8 hojas con conceptos que no tienen relaciona con el Manual.

4.1.5. Funciones y responsabilidades del Analista de Proyectos incompletas

Referencia	Categorización Hallazgos	Importancia
GEPR-006	Estructura Organizacional	Moderado

Descripción

Se revisó las funciones y responsabilidades del Analista de Proyectos, observándose que entre sus funciones principales están socializar la metodología de gestión de proyectos y validar que se cumpla

con la misma, dar seguimiento a los avances de los proyectos bajo su coordinación; sin embargo, en el Manual de administración de proyectos, el Analista asume la función de Gerente de Proyectos, el cual debería empoderarse más de la gestión de cada uno de los proyectos, es decir, asumir el rol de planificador, administrador y mentor, aspectos que en el Manual aún no aprobado constan como responsabilidades del Líder de Proyecto.

4.2. Validación de Templates

4.2.1. Templates no utilizados

Referencia	Categorización Hallazgos	Importancia
GEPR-008	Riesgo operativo	Alto

Descripción

En la Intranet se han publicado los templates aplicables a todas las fases de la gestión de proyectos basada en la metodología PMBOK: inicio, planificación, ejecución, monitoreo y cierre.

Revisados la documentación de los proyectos Creer y Gestión de Cambios y Configuración, se observa que el uso de las plantillas es esporádico, esto debido a que aún no se ha formalizado la obligación de utilizar estos formatos para todos los proyectos sean o no institucionales.

En el proyecto Creer lo único que mantiene son las plantillas de seguimiento y control.

Para el Proyecto Gestión de Cambios y Configuración, se ha utilizado la plantilla Project Charter, Acta KickOff, Check list de presentación de reunión kickoff, aun faltando documentación establecida como obligatoria.

4.3. Contratos de TI

4.3.1. Incumplimiento de cláusulas que deben incluirse en contratos

Referencia	Categorización Hallazgos	Importancia
GEPR-009	Riesgo operativo	Moderado

Descripción

Para objeto de la presente auditoría se revisaron los contratos de los proyectos de TI en los que el Gerente de Tecnología está como Líder del Proyecto:

1. Cámara de Compensación Digital

2. Gestión de Cambios y Configuración

3. Comunicaciones Unificadas

Donde se observa:

• El Proyecto Cámara de Compensación Digital aún no se inicia, la fecha de inicio planteada era 15 de abril del 2012; hasta la presente no se ha dado comienzo al proyecto, conforme lo indicado por el Gerente de Tecnología la nueva fecha de inicio se coordinará con el Proveedor, debido problemas internos.

Se solicitó a Control Interno información a fin de evidenciar si se han efectuado cambios en las fechas inicialmente programadas en el plan estratégico para este proyecto, indicándonos que no ha sido formalizado el cambio de fechas para este proyecto.

Revisado el contrato, la fecha de la firma del contrato fue el 13 de Abril de 2012, además en este documento no se incluye una cláusula para la entrega de documentación técnica y de usuario.

• Para el proyecto Gestión de Cambios y Configuración se ha finalizado la consultoría evidenciando que se ha cumplido los plazos establecidos y los entregables definidos por ambas partes así: Acta de inicio, Informe del levantamiento del proceso, manual de proceso y plantillas, informe de resultados de implementación, acta de cierre del proyecto, cronograma de actividades, project charter.

Revisado el contrato se validó que contenga las cláusulas establecidas en el Manual de Adquisiciones tales como: Niveles de servicio, penalizaciones por incumplimiento, cláusula de confidencialidad, plazo precio y formas de pago, plazo de entrega, cronograma de implementación, causales de terminación de contrato, propiedad intelectual, transferencia del conocimiento, entrega de documentación, cronograma de implementación, entre otros, si observar novedades relevantes.

• Para el proyecto Comunicaciones Unificadas, no se nos proporcionó el contrato Conforme consta en el mail enviado por el Gerente de TI al Jefe de Infraestructura le requiere la inclusión en el contrato de los niveles de servicio que tampoco se nos proporcionó.

Los entregables entregados fueron: cronograma de implementación y project charter .

4.4. Riesgos y Hallazgos Positivos

4.4.1. Riesgos importantes no considerados

Referencia	Categorización Hallazgos	Importancia
GEPR-010	Riesgo operativo	Moderado

Descripción

• En la matriz de riesgos relacionado con el subproceso de Gestión de Proyectos, a criterio de Auditoría Interna no se han considerado riesgos importantes en temas tales como:

- Desviaciones de recursos y tiempos programados

- Pérdida de personal clave que participa en los proyectos

- Lentitud en la toma de decisiones

- Cambios en el proyecto

• En cuanto a los controles establecidos para el subproceso de Gestión de Proyectos de TI, se observa que 2 riesgos registran riesgo residual EXTREMO y 2 como ALTO y a pesar de existir controles con riesgo residual se mantiene ALTO.

Atentamente,

AUDITORA INFORMATICA

3.4 MONITOREO

Para el presente caso de estudio por ser la primera vez que se efectúa una auditoría basada en riesgos, la fase de monitoreo no es aplicable como lo expone el modelo propuesto.

Se requiere cierto periodo de tiempo, que puede ser establecido por la Alta Gerencia o por las regulaciones emitidas por la Superintendencia de Bancos, para realizar un seguimiento adecuado a las medidas correctivas que se apliquen a los procesos auditados a fin de solucionar las falencias y debilidades encontradas que repercuten en el nivel de madurez obtenido al efectuar el examen de auditoría, sin embargo, se espera que esta fase definida en el modelo se la aplique en lo posterior a fin de validar su aplicación.

CAPÍTULO 4. CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- ✓ El resultado de la fase de planificación es el plan anual de auditoría, el cual garantiza que las Auditorías contempladas se desarrollen efectivamente, al momento de elaborar los objetivos y alcance de las mismas, propiciando el éxito de la fase de ejecución.

- ✓ En la fase de planificación, la herramienta diseñada para la elaboración del plan anual de auditoría, arrojó resultados positivos, su aplicación permitió efectuar la planificación basada en riesgos para el año 2013, misma que fue presentada a la Alta Gerencia para su aprobación y posteriormente presentada a la Superintendencia de Bancos adjuntando, la debida explicación del procedimiento seguido para la obtención de este entregable.

- ✓ La participación de la Alta Gerencia, en el establecimiento de los criterios de riesgos, permitió que la fase de planificación tenga un enfoque formal debido a que se consideraron aspectos tales como: que sean acordes con la naturaleza de la organización, que estén asociados con la estrategia y metas de la Institución, que se combinen factores predictivos o históricos, que reflejen las expectativas de la Alta Gerencia entre otros.

- ✓ El cálculo de la madurez del proceso evaluado permitió tener un conocimiento claro de cómo actualmente se desarrollan las actividades asociadas y si las entradas y salidas eran adecuadas; esta línea base permitió determinar el alcance y los objetivos del examen de auditoría del caso de estudio, garantizando que todos los aspectos importantes sean considerados y no se queden por fuera a fin de emitir recomendaciones que permitan a corto o largo plazo mejorar el nivel del madurez.

- ✓ El propósito fundamental de la etapa de ejecución es recopilar la evidencia que sustente los resultados de la valoración de los procesos; de esta fase depende las recomendaciones emitidas en el informe a fin de apoyar en la mitigación del riesgo que se obtuvo en la valoración de alto nivel de los procesos.

- ✓ El uso de prácticas profesionales para el aseguramiento, modelo de evaluación del proceso, prácticas de control, y otros documentos como herramientas de apoyo, permitió que el desarrollo y aplicación del modelo se lleve a cabo de forma objetiva y ordenada, bajo un enfoque basado en riesgos, objetivo principal del presente trabajo.

4.2 RECOMENDACIONES

- ✓ La Superintendencia de Bancos y Seguros emitió la resolución JB-2010-1549 [1], misma que debe ser cumplida por todas las instituciones financieras controladas por este organismo; la normativa indica que se deberá efectuar las auditorías basadas en riesgos al igual que los programas anuales, por tal razón se recomienda el uso del modelo propuesto que se adapta a las exigencias de la resolución.

- ✓ Se recomienda el uso de la herramienta para la valoración del alto nivel que para el caso de estudio permitió obtener el plan anual de auditoría, considerando de vital importancia la participación de la Alta Gerencia en la definición de los criterios de riesgos.

- ✓ Se recomienda que el Auditor Informático obtenga un conocimiento claro del marco de referencia COBIT 4.1 [2], de las prácticas profesionales para el aseguramiento ITAF™ [3], del modelo de evaluación del proceso PAM [4], de las prácticas de control y de las guías de auditoría de ISACA [5], a fin de que la aplicación del modelo propuesto no se convierta en algo difícil de usar.

BIBLIOGRAFÍA

[1] JUNTA BANCARIA DEL ECUADOR, «Resolución No. JB-2010-1549,» 2010.

[2] I. G. INSTITUTE, COBIT 4.1, EE.UU, 2007.

[3] ISACA, «ITAF , A professional Practices Framework for IT Assurance,» 2008.

[4] ISACA, «PAM Process Assessment Model, Using COBIT 4.1,» 2011.

[5] ISACA, «IT Audit and Assurance Standards and Guidelines,» 2008.

[6] JUNTA BANCARIA DEL ECUADOR, «Resolución JB-2005-834 Gestión de Riesgo Operativo,» 2005.

[7] MINISTERIO DE HACIENDA DEL REINO UNIDO, «ITIL 3.0,» 2011.

[8] ISO/IEC, «Information technology - Security techniques - Information security management systems - Requirements,» 2007.

[9] INCOTEC, NTC5254 Gestión del Riego, Bogotá, 2006.

[10] ISO, «Risk Management 31000:2009,» 2009.

[11] COSO, «COSO ERM II Enterprise Risk Management,» 2004.

[12] COMITE BASILEA, «Basilea II,» 2005.

[13] IT GOVERNANCE INSTITUTE, «IT Assurance Guide: Using COBIT,» 2007.

[14] I. G. INSTITUTE, Assurance Guide: Using COBIT, EE.UU, 2007.

[15] ISO-IEC, « Software Process Improvement Capability,» 1998.

[16] T. Z. GABRIEL, «Implementacion de un Sistema de Gestión de Riesgos con la Auditoría Integrada,» de *Gestión de Riesgos*, 2010.

[17] COOP ABC, «Factores de Riesgos,» 2012.

[18] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, «ISO 31000 Gestión de Riesgos,» 2009.

[19] I. -. IEC, ISO/IEC 27002:2005 Gestion de la Seguridad de la Informacion, 2007.

GLOSARIO DE TERMINOS

Auditor: Persona que efectúa una auditoría.

Auditoría: Examen de las operaciones de una empresa efectuado por especialistas ajenos a ella y con objetivos de evaluar la situación de la misma.

Auditoría basada en riesgos: Es el examen de las operaciones de una empresa que le permite al auditor obtener una seguridad razonable de que en los estados financieros no existan declaraciones erróneas causadas por fraude o error.

COBIT: Objetivos de control de información y tecnologías relacionadas, es un conjunto de buenas prácticas para el manejo de información

Control: Las políticas, procedimientos, practicas y estructuras organizacionales diseñadas para proporcionar una garantía razonable de que los objetivos del negocio se alcanzarán y los eventos no deseados serán prevenidos o detectados

Control aplicativo: Es un conjunto de controles integrados dentro de las soluciones automatizadas (aplicaciones).

Control de detección: Un control que se usa para identificar eventos (indeseables o deseados), errores u otras ocurrencias con efecto material sobre un proceso o producto final, de acuerdo a lo definido por la empresa.

Control general: También control general de TI. Un control que se aplica al funcionamiento general de los sistemas de TI de la organización y a un conjunto amplio de soluciones automatizadas (aplicaciones).

Control Interno: Las políticas, procedimientos, practicas y estructuras organizacionales diseñadas para brindar una garantía razonable de que los

objetivos del negocio se alcanzarán y de que los eventos indeseables serán prevenidos o detectados y corregidos

Control preventivo: Un control interno que se usa para prevenir eventos indeseables, errores u otras ocurrencias que pudieran tener un efecto material negativo sobre un proceso o producto final, de acuerdo a la organización.

Declaración de auditoría: Documento que define el propósito, la autoridad y la responsabilidad de la actividad de auditoría interna, aprobado por el consejo

Directriz: La descripción de un modo particular de lograr algo, la cual es menos prescriptiva que un procedimiento.

Estándar: Una práctica de negocio o producto tecnológico que es una práctica aceptada, avalada por la empresa o por el equipo gerencial de TI. Los estándares se pueden Implementar para dar soporte a una política o a un proceso, o como respuesta a una necesidad operativa. Así como las políticas, los estándares deben incluir una descripción de la forma en que se detectará el incumplimiento.

ISO/IEC 27002:2005: Es código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 01 de julio de 2007.

ISO 31000: Norma para la gestión de riesgos.

Modelo: Una herramienta para los dueños de los procesos de negocio que facilita la descarga de sus responsabilidades a través de la procuración de un modelo de control de soporte.

Objetivo de control: Una declaración del resultado o propósito que se desea alcanzar.

Papeles de trabajo: Registra el planeamiento, naturaleza, oportunidad y alcance de los procedimientos de auditoría aplicados por el auditor y los resultados y conclusiones extraídas a la evidencia obtenida. Se utilizan para controlar el progreso del trabajo realizado para respaldar la opinión del auditor. Los papeles de trabajo pueden estar constituidos por datos conservados en papel, película, medios electrónicos u otros medios.

Proceso de negocio: Ver Proceso.

Proceso: Por lo general, un conjunto de procedimientos influenciados por las políticas y estándares de la organización, que toma las entradas provenientes de un número de fuentes, incluyendo otros procesos, manipula las entradas, y genera salidas, incluyendo a otros procesos, para los clientes de los procesos. Los procesos tienen razones claras de negocio para existir, dueños responsables, roles claros y responsabilidades alrededor de la ejecución del proceso, así como los medios para medir el desempeño.

Riesgo: El potencial de que una amenaza específica explote las debilidades de un activo o grupo de activos para ocasionar pérdida y/o daño a los activos. Por lo general se mide por medio de una combinación del impacto y la probabilidad de ocurrencia.

ANEXOS DIGITALES

Anexo No. 1 Inventario Consolidad HW

Anexo No. 2 Inventario Consolidad SW

Anexo No. 3 Inventario Consolidado Información

Anexo No.4 Inventario Consolidado Gente

Anexo No. 5 HERRAMIENTA ERA

Anexo No. 6 INFORME COMPLETO AUDITORÍA

Anexo No. 7 Resolución No. JB-2010-1549

Anexo No. 8 COBIT 4.1

Anexo No. 9 ITAF , A professional Practices Framework for IT Assurance

Anexo No. 10 PAM Process Assessment Model, Using COBIT 4.1

Anexo No. 11 IT Audit and Assurance Standards and Guidelines

Anexo No. 12 Resolución JB-2005-834 Gestión de Riesgo Operativo

Anexo No. 13 NTC5254 Gestión del Riego

Anexo No. 14 IT Assurance Guide: Using COBIT

Anexo No. 15 Certificación de Entidad Financiera sobre aplicabilidad del modelo