UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

CARRERA DE CONTADURÍA PÚBLICA E INGENIERÍA EN CONTABILIDAD Y AUDITORÍA

TÍTULO:

AUDITORÍA INFORMÁTICA SOPORTADA POR COBIT E ISO 27001 EN LAS INSTITUCIONES FINANCIERAS PÚBLICAS DE LA CIUDAD DE GUAYAQUIL

AUTORES:

MERO PAREDES, GEOCONDA DESIRE

ZAMBRANO GONZALEZ, STEPHANIE KATHERINE

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA.

TUTOR:

CPA. Delgado Loor, Fabián Andrés, MBA.

Guayaquil, Ecuador

5 de marzo del 2018

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

CARRERA DE CONTADURÍA PÚBLICA E INGENIERÍA EN CONTABILIDAD Y AUDITORÍA CPA

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por**: Mero Paredes, Geoconda Desire y Zambrano González, Stephanie Katherine**, como requerimiento parcial para la obtención del Título de: **Ingenieras en Contabilidad y Auditoría CPA.**

TUTOR

f. _____

CPA. Delgado Loor, Fabián Andrés, MBA.

DIRECTOR DE LA CARRERA

f. _____

CPA. Vera Salas, Laura Guadalupe, Msc.

Guayaquil, a los 5 días del mes de marzo del año 2018

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

CARRERA DE CONTADURÍA PÚBLICA E INGENIERÍA EN CONTABILIDAD Y AUDITORÍA CPA**.**

DECLARACIÓN DE RESPONSABILIDAD

Nosotras, Mero Paredes Geoconda Desire y Zambrano González Stephanie Katherine

DECLARAMOS QUE:

El Trabajo de Titulación **"Auditoria Informática soportada por COBIT e ISO 27001 en las Instituciones Financieras públicas de la ciudad de Guayaquil"** previa a la obtención del Título de: **Ingenieras en Contabilidad y Auditoría CPA**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de nuestra total autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad alcance científico del Trabajo de Titulación referido.

Guayaquil, a los 5 días del mes de marzo del año 2018

LAS AUTORAS

f. _____ f. _____

Mero Paredes, Geoconda Desire Zambrano González, Stephanie Katherine

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

CARRERA DE CONTADURÍA PÚBLICA E INGENIERÍA EN CONTABILIDAD Y AUDITORÍA CPA

AUTORIZACIÓN

Nosotros, Mero Paredes, Geoconda Desire y Zambrano González, Stephanie Katherine

Autorizamos a la Universidad Católica de Santiago de Guayaquil, la publicación en la biblioteca de la institución del Trabajo de Titulación “Auditoria Informática soportada por COBIT e ISO 27001 en las instituciones financieras públicas de la ciudad de Guayaquil”, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y total autoría.

Guayaquil, a los 5 días del mes de marzo del año 2018

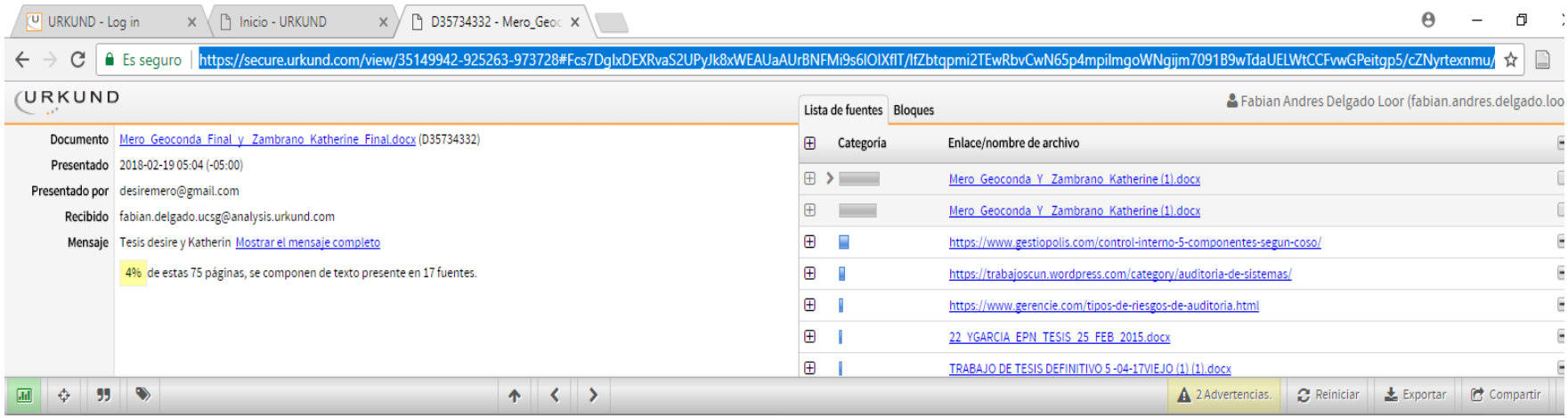
LAS AUTORAS

f. _____ f. _____

Mero Paredes, Geoconda Desire Zambrano González, Stephanie Katherine

REPORTE URKUND

https://secure.urkund.com/view/35149942-925263-973728#Fcs7DgIxDEXRvaS2UPyJk8xWEAUaAUrBNFMi9s6lOIXflT/lfZbtqpmi2TEwRbvCwN65p4mpiImgoWNgijm7091B9wTdaUELWtCCFvwGPeitgp5/cZNyrtexnmu/H/ujbPVSfbp6ho6cLVPb9wc=



TUTOR

f. _____

Ing. Delgado Loor , Fabian Andrés , MSc

AGRADECIMIENTO

Agradezco a Dios por darme una vida bendecida llena de oportunidades, y es el que me deja llegar a esta meta que me trace.

A mis padres queridos quienes han creído en mi en todo momento y son parte de este logro por sus ánimos y esfuerzos.

A mis hermanos que no me dejaron decaer en el camino y que motivaron a continuar, a mi cuñado por enseñarme que no existe pequeños esfuerzos cada paso es un gran reto.

A mi esposo quien es parte fundamental de este logro quien sacrifico momentos para ayudarme, motivarme y ser mejor cada día que me dio el abrazo en el momento indicado para luchar por mi sueño.

A mis sobrinos a quienes amo como hijos quienes han sido el motor para alcanzar el objetivo porque quiero ser un buen ejemplo para ellos, a mi angelito quien cuida de la tía en el cielo

El tiempo de Dios es perfecto y si sonrío es porque tengo una bella familia quienes están conmigo en cada paso de mi vida.

Geoconda Desire Mero Paredes

AGRADECIMIENTO

En primer lugar agradezco a Dios por ser mi pilar fundamental y haberme guiado por un buen camino, a mi madre que dejó unas bases bien puestas en mi gracias a ella soy lo que soy, a la persona que me crio como a una hija, por haberme dado ese apoyo y haber creído siempre en mí, a mi padre por siempre dar el apoyo moral de seguir con mi propósito, a mi esposo por darme ese apoyo incondicional día a día, a mis hijos que son mi motor para seguir luchando y cumplir cada una de mis meta trazada. A todos los que me ayudaron con un granito de arena a cumplir con esto.

Stephanie Katherine Zambrano González

DEDICATORIA

A mis padres Geoconda y Nicolás por el amor, constancia y esfuerzo que me inculcaron para ser una mujer con valores y una profesional.
A Alfredo, mi esposo que es mi refugio amor y futuro.
A mi ángel Jeremías quien me enseñó a ser más agradecida con Dios.

Geoconda Desire Mero Paredes

DEDICATORIA

Dedico esta tesis en memoria de mi madre, un ejemplo a seguir, una mujer luchadora, que jamás se rindió y siempre ayudo a toda su familia, a mis hijos por los cuales quiero ser cada día mejor.

Stephanie Katherine Zambrano González

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

CARRERA DE CONTADURÍA PÚBLICA E INGENERÍA EN CONTABILIDAD Y AUDITORÍA CPA.

TRIBUNAL DE SUSTENTACIÓN

f. _____

CPA. Vera Salas, Laura Guadalupe MSC.

DIRECTORA DE LA CARRERA

f. _____

EC. Baño Hifóng, María Mercedes .MSC

COORDINADOR DE ÁREA

f. _____

CPA. Samaniego Pincay , Pedro José , MSC.

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

CARRERA DE CONTADURÍA PÚBLICA E INGENERÍA EN CONTABILIDAD Y AUDITORÍA CPA.

CALIFICACIÒN

f. _____

Ing. Delgado Loor , Fabian Andrés , MSc

TUTOR

INDICE

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

RESUMEN

El siguiente trabajo de titulación describe la Auditoría Informática que se le realizará al Sistema Core Bancario Cobis en BanEcuador B.P, a su Gerencia Financiera, utilizando los estándares internacionales, ISO 27001 el cual sirve para especificar los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) basado en el ciclo de mejora continua en conjunto con COBIT que es una herramienta desarrollada para auditar la gestión y control de los sistemas de información.

Primero se definirán los principales conceptos de la auditoria informática, ISO 27001, COBIT y del área financiera, posterior y en conjunto con la identificación de la metodología a plantear y pasos a seguir, mediante el análisis de la información y ejecución de las técnicas de investigación se desprenderán los resultados de cuáles son los principales procesos críticos y la conexión de estos con el área de TI, evaluando su nivel de madurez, logrando identificar las debilidades que se corren en la organización por no tener mejores controles que permitan minimizar los riesgos.

Finalmente se emitirán conclusiones y recomendaciones para ser tomadas en consideración por BanEcuador B.P.

Palabras Claves: Auditoria de Sistemas, Integración, Riesgos, Vulnerabilidades, Procesos.

ABSTRACT

The following titration work describes the Computer Audit that will be done to the Banking Core Cobis System in BanEcuador BP, to its Financial Management, using international standards, ISO 27001, which serves to specify the requirements necessary to establish, implement, maintain and improve an information security management system (ISMS) based on the continuous improvement cycle in conjunction with COBIT, which is a tool developed to audit the management and control of information systems.

First, the main concepts of computer audit, ISO 27001, COBIT and the financial area will be defined, later and in conjunction with the identification of the methodology to be proposed and steps to follow, through the analysis of information and the execution of research techniques the results of what are the main critical processes and the connection of these with the IT area will be revealed, evaluating their level of maturity, managing to identify the weaknesses that are run in the organization because they do not have better controls to minimize the risks.

Finally, conclusions and recommendations will be issued to be taken into consideration by BanEcuador B.P.

Key words: Systems Audit, Integration, Risks, Vulnerabilities, Processes

INTRODUCCIÓN

El presente trabajo de titulación describe la Auditoría Informática realizada a BanEcuador B.P, en conjunto a los estándares de las normas internacionales COBIT e ISO 27001 a sus Sistemas de Tecnología e Información en el programa interno llamado Sistema Core Bancario Cobis.

La Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, manteniendo seguros los datos para poder alcanzar con eficacia los fines de la organización y tener la certeza para poder maximizar los recursos. (Romero S. C., Auditoria Informática)

Los sistemas informáticos se han convertido en piezas fundamentales en el desarrollo del día a día en todo tipo de organización y de cualquier tamaño. Conocer los riesgos que se enfrentan las instituciones por medios de sus sistemas informáticos son beneficios que se tiene para dar controles adecuados y necesarios en el manejo de la empresa.

La naturaleza propia de la auditoria de los sistemas informáticos y sus habilidades necesarias para llevar a cabo las mismas requieren el soporte de Normas Generales para la auditoría de los Sistemas de Información.Dos normas internacionales reconocidas para la evaluación de los sistemas de información que se pueden utilizar para todo tipo de empresa y con las cuales vamos a desarrollar esta tesis son:

- Objetivos de Control para Información y Tecnologías Relacionadas (COBIT, en inglés: Control Objectives for Information and related Technology).
- ISO 27001 Sistemas de gestión de la seguridad de la información (SGSI)

La implementación COBIT permite que las tecnologías de la información se gobiernen y administren de una manera holística a nivel organizacional manteniendo el alcance completo de las áreas de

responsabilidad funcional y negocios de las empresas considerando los intereses relacionados con la TI de las partes interesadas internas y externas.

La información y los procesos que la utilizan hacen parte de los activos más importantes de una organización. Definir, lograr, mantener y mejorar la seguridad de la información es esencial para mantener una ventaja competitiva que permita alcanzar el éxito y lograr continuidad en un mercado globalizado.

Para una organización competitiva es necesario implantar un sistema para la gestión de la seguridad de la información, que permita tener unos objetivos claros de seguridad y una evaluación de los riesgos posibles a los que esté expuesta su información, asegurando así la continuidad del negocio, minimizando el riesgo comercial y maximizando el retorno de las inversiones y las oportunidades comerciales.

La International Organization for Standardization e International Electrotechnical Commission ISO/IEC son los encargados de los estándares que proporcionan un marco de la gestión de la seguridad de la información utilizable para cualquier tipo de organización, privada o pública, pequeña o grande.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como "Ciclo de Deming": PDCA - acrónimo de **P**lan, **D**o, **C**heck, **A**ct (Planificar, Hacer, Verificar, Actuar). (27001, s.f.)

Al reconocer que la tecnología crece a pasos agigantados, los sistemas informáticos se les debería realizar una evaluación técnica basada con las mejores normas internacionales para lograr identificar posibles debilidades y emitir recomendaciones para minimizar los riesgos.

Formulación del problema

En la actualidad los sistemas informáticos, se han convertido en parte importante de la gestión empresarial en la toma de decisiones ; por ello, se deberían ajustar a las normas y estándares internaciones debidamente calificados, para estas evaluaciones tomando en cuenta que previo debe existir un análisis y aprobación del departamento de sistemas de la organización, el mismo que se encargara de la implementación de controles de accesos a la información, que se maneja en cada uno de los procesos de la empresa.

La comunidad científica ha investigado e implementado mecanismos que permitan disminuir y mitigar estos ataques de seguridad, empleando tecnologías de virtualización, cuya aplicación permite disminuir el riesgo a equipos y redes en producción, precautelando la información y servicios de las organizaciones. (Walter, 2011, pág. 39)

El término seguridad informática ha sido objeto de estudio por algunos autores, lo que permite tener una definición más exacta; por lo tanto, es un conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, la confidencialidad y disponibilidad de la información (Escrivá et al., 2013). Por otra parte, consiste en asegurar que los recursos del sistema de información de una organización sean utilizados de la manera que se decidió y que el acceso a la información, su respectiva modificación, sólo sea posible a las personas que se encuentren autorizadas y dentro de los límites de su autorización (Costas, 2014)

Estas definiciones complementan el concepto de seguridad informática como una serie de medias y procedimientos con el único fin de que los datos siempre estén disponibles y asegurar la información, por lo tanto, los procesos deben cumplir con los estándares de seguridad de la información.

Debido a los cambios que ha sufrido en los últimos años el sector bancario con la incorporación de tecnologías informáticas que faciliten el manejo de los datos y a su vez la seguridad informática, ofrecer mejoras en la toma de decisiones, cabe destacar, que los sistemas de información ofrecen una importante y notable satisfacción en los usuarios que lo operan, debido al fácil uso y acceso.

Por ello, las empresas están implementando normativas para asegurar que la información de la institución sea uso exclusivo del personal autorizado, existe la norma ISO 27001 que es de certificación a los sistemas de información junto con el COBIT, la aplicación de ambos permitirá reforzar las partes del sistema que tengan debilidades.

COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público. (ISACA, 2012)

El estudio de esta temática intentará aportar argumentos tanto conceptuales como prácticos, con la intención de aportar información sobre los estándares referidos a la seguridad de la información ya que como sabemos toda la información es un activo invaluable, por lo tanto al evaluar los procesos más críticos de una área específica podemos tomar como referencia como está estructurado el sistema que se está utilizando y revelar las debilidades y así poder mitigar los riesgos para mejorar la calidad de la información y por ende mejorar la toma de decisiones dentro de la organización.

Las interrogantes que serán resueltas son:

¿Qué procesos críticos dependen de TI?

¿Cuál es el beneficio de Implementar COBIT como marco de trabajo de gobierno de TI?

¿Son suficientes los recursos y la infraestructura de TI disponibles para conseguir los objetivos estratégicos de empresa requeridos?

¿Se maneja adecuadamente la confidencialidad, integridad y disponibilidad de los sistemas TI?

Objetivos de la investigación.

Objetivo General

Realizar una auditoría informática al Sistema Core Bancario Cobis de BanEcuador B.P en la Gerencia Financiera a los principales procesos, utilizando los estándares internacionales como el COBIT E ISO 27001 a fin de identificar las debilidades, desvíos a la norma y emitir recomendaciones que permitan minimizar los riesgos.

Objetivos Específicos

- Planificar una auditoria informática al sistema de BanEcuador B.P
- Aplicar el estándar COBIT 5 e ISO 270001 en la evaluación de riesgos hasta determinar el nivel de madurez de los procesos seleccionados.
- Identificar posibles debilidades, que se posean realizando un análisis de riesgos.
- Emitir recomendaciones para minimizar los riesgos y obtener mayor confidencialidad e integridad de la información.

Justificación

La información de una institución financiera es una de las partes más vulnerables, que conlleva a tener varias debilidades. La institución necesita estándares internacionales de calidad, para que no existan alteraciones en los estados financieros y que siempre estén disponibles.

Para el desarrollo de lo anterior mencionado existen normas que nos proporcionan estándares de calidad en cuanto a seguridad de la información se trata, este proyecto tendrá como guía a las norma integradora COBIT 5 compuesta a la ISO 27001 como marco referencial internacional , las que ayuda a comprender el tratamiento que se debe desarrollar con la unificación de las metas corporativas relacional a las TI para lograr minimizar los riesgos que pudieren tener dentro del sistema Core Bancario Cobis.

Considerando los estándares que tomaremos como base y el área en la que se desarrollará esta investigación que es la gerencia financiera, se

planifica las etapas respectivamente, empezando con el levantamiento de información sobre BanEcuador B.P, posteriormente entrevistas y encuestas respectivas para luego aplicar las matrices de desarrollo y así reconocer el nivel de riesgo que posee los sistemas de TI relacionados con el área en estudio.

Para BanEcuador B.P reconocer los riesgos que presenta una de las áreas más relevantes de su organización como es la Gerencia Financiera la misma que esta integrad por tres subgerencias Tesorería, Contabilidad y Control Financiero y Presupuesto, relacionado con controles que se pueden minimizar con procesos estandarizados, regulatorios y simples se convertirá en un gran aporte para mejorar sustancialmente logrando maximizar su rendimiento en busca de alcanzar su misión y visión.

BanEcuador B.P pudiera tener más controles dentro del Sistema Core Bancario Cobis, con esto puede asegurar de que solo el personal con los roles respectivos y autorizados puedan tener acceso al sistema.

Hipótesis

Una Institución pública debería cumplir con el estándar internacional COBIT 5 e ISO27001 para asegurar la optimización de los niveles de riesgos y mantener un equilibrio, beneficios, riesgo y recurso.

CAPÍTULO 1

MARCO TEÓRICO

Generalidades de Auditoria e Auditoria Informática

Auditoria

Auditoría, en su sentido más general, se puede entender como la investigación, consulta, revisión, verificación, comprobación y obtención de evidencia, desde una posición de independencia, sobre la documentación e información de una organización, realizadas por un profesional, el auditor, designado para desempeñar tales funciones. (Melo, 2014)

Auditoria Informática

Según Piattini, et al, (2008) dice que la auditoría en informática se desarrolla en función de normas, procedimientos y técnicas definidas por institutos establecidos a nivel nacional e internacional; por lo tanto, nada más se señalarán algunos aspectos básicos para su entendimiento. (BRAVO, 2015)

Es el conjunto de técnicas, actividades y procedimientos destinados a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control, eficacia, seguridad y adecuación del servicio informático de la empresa, ... con vistas a mejorar en rentabilidad, seguridad y eficacia.” (RIVAS, 1989)

Conjunto de Procedimientos y Técnicas para evaluar y controlar total o parcialmente un Sistema Informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existente en cada empresa, y para conseguir la eficacia exigida en el marco de la organización correspondiente.” (ACHA ITURMENDI J. J., 1996)

La importancia de este tipo de auditoría radica en que permite determinar las fortalezas y debilidades en la gestión de proyectos, el nivel de funcionalidad de los sistemas de información automatizados, la adecuación de la configuración de la plataforma informática, el nivel de calidad de los

servicios prestados por la unidad encargada y la situación de los contratos con proveedores de productos y servicios, entre otros aspectos, todo ello en el ámbito del uso y aplicación de las TIC´s en la organización. Esto con la finalidad de brindar recomendaciones y propuestas de solución para lograr que las mismas brinden un apoyo óptimo a los procesos de negocio y, por ende, ayuden a alcanzar los objetivos establecidos.

Los objetivos de la auditoría de sistemas son los siguientes:

- Realizar una evaluación con personal multidisciplinario y capacitado en el área de sistemas, con el fin de emitir un dictamen independiente sobre la razonabilidad de las operaciones del sistema y la gestión administrativa del área de informática.
- Hacer una evaluación sobre el uso de los recursos financieros en las áreas del centro de información, así como del aprovechamiento del sistema computacional, sus equipos periféricos e instalaciones.
- Evaluar el uso y aprovechamiento de los equipos de cómputo, sus periféricos, las instalaciones y mobiliario del centro de cómputo, así como el uso de sus recursos técnicos y materiales para el procesamiento de información.
- Evaluar el aprovechamiento de los sistemas de procesamiento, sus sistemas operativos, los lenguajes, programas y paqueterías de aplicación y desarrollo, así como el desarrollo e instalación de nuevos sistemas.
- Evaluar el cumplimiento de planes, programas, estándares, políticas, normas y lineamientos que regulan las funciones y actividades de las áreas y de los sistemas de procesamiento de información, así como de su personal y de los usuarios del centro de información.
- Realizar la evaluación de las áreas, actividades y funciones de una empresa, contando con el apoyo de los sistemas computacionales, de los programas especiales para auditoria y de la paquetería que sirve de soporte para el desarrollo de auditorías por medio del computador. (Razo, 2002)

Planificación de Auditoria Informática

En esta etapa se crean los vínculos y las relaciones entre los auditores y personal que va a colaborar de la organización con el objetivo de determinar el alcance y objetivo de la auditoria.

Junto con el personal se realiza un bosquejo de la situación actual de la institución, de cómo se encuentra el sistema contable, los controles internos, seguridad de la información y otros elementos que le ayude y permita al auditor pueda elaborar el programa de auditoría que se va a realizar.

Elementos Principales de esta Fase:

- Conocimiento y Enfoque de la institución
- Objetivos y Alcance de la auditoría
- Análisis Preliminar del Control Interno
- Análisis de los Riesgos
- Planeación de la auditoría
- Elaboración de programas de auditoría

Conocimiento y Enfoque de la institución.

Como primer punto antes de realizar la planificación de auditoria, el equipo auditor debe indagar, investigar y analizar el enfoque de la institución a auditar, para con estas bases poder así elaborar el plan de auditoria de una forma objetiva y precisa.

En este análisis que se realiza a la institución se debe conocer: su naturaleza operativa, giro del negocio, su estructura organizacional, estatutos y reglamentos vigentes, disposiciones legales que la rigen, sistema informático contable que utiliza, volumen de sus procesos y, en si todo lo que sirva como base para poder comprender con exactitud el funcionamiento de la institución.

Para comprender y tener un enfoque adecuado de la institución, el auditor deberá establecer diferentes técnicas y mecanismos que deberá dominar y poner en práctica.

Análisis Preliminar del Control Interno

La función del análisis preliminar es muy importante ya que de su efectividad depende que la firma auditora obtenga la información precisa para poder evaluar y seleccionar la naturaleza y la extensión del plan de auditoría, y analizar los procedimientos a utilizar durante el proceso.

Es por ello que el auditor evalúa los controles internos con anterioridad, para tener conocimiento de las falencias existentes que indican que los controles no están operando efectivamente.

Análisis de los Riesgos

Al analizar los riesgos en la auditoria, se tiene la posibilidad de que el auditor presente una opinión errónea en su informe, esto se debe a que la información entregada al equipo esté afectada por una desviación material o desviación de alguna normativa específica.

La posibilidad de que exista algún tipo de error puede presentarse en distintos niveles, es por ello que se debe analizar de la manera más apropiada para así poder observar la implicación dentro de cada nivel o subproceso.

Y es así que se ha determinado tres tipos de riesgos existentes dentro de una auditoria, los cuales son:

- **El riesgo inherente**, Este tipo de riesgo tiene ver exclusivamente con la actividad económica o negocio de la empresa, independientemente de los sistemas de control interno que allí se estén aplicando. Si se trata de una auditoría financiera es la susceptibilidad de los estados financieros a la existencia de errores significativos; este tipo de riesgo está fuera del control de un auditor por lo que difícilmente se puede determinar o tomar decisiones para desaparecer el riesgo ya que es algo innato de la actividad realizada por la empresa. Entre los factores que llevan a la existencia de este tipo de riesgos esta la naturaleza de las actividades económicas, como también la naturaleza de volumen tanto de transacciones como de productos y/o servicios, además tiene relevancia la parte gerencial y la calidad de recurso humano con que cuenta la entidad. (Gerencie.com, 2017)

- **Riesgo de control:** Aquí influye de manera muy importante los sistemas de control interno que estén implementados en la empresa y que en circunstancias lleguen a ser insuficientes o inadecuados para la aplicación y detección oportuna de irregularidades. Es por esto la necesidad y relevancia que una administración tenga en constante revisión, verificación y ajustes los procesos de control interno. Cuando existen bajos niveles de riesgos de control es porque se están efectuando o están implementados excelentes procedimientos para el buen desarrollo de los procesos de la organización. Entre los factores relevantes que determina este tipo de riesgo son los sistemas de información, contabilidad y control. (Gerencie.com, 2017)
- **Riesgo de detección:** Este tipo de riesgo está directamente relacionado con los procedimientos de auditoría por lo que se trata de la no detección de la existencia de errores en el proceso realizado. La Responsabilidad de llevar a cabo una auditoria con procedimientos adecuados es total responsabilidad del grupo auditor, es tan importante este riesgo que bien trabajado contribuye a debilitar el riesgo de control y el riesgo inherente de la compañía. Es por esto que un proceso de auditoría que contenga problemas de detección muy seguramente en el momento en que no se analice la información de la forma adecuada no va a contribuir a la detección de riesgos inherentes y de control a que está expuesta la información del ente y además se podría estar dando un dictamen incorrecto. (Gerencie.com, 2017)

La información que es presentada en los estados financieros tiene importancia relativa, si existe el riesgo de una presentación errónea afecte con la toma de decisiones, por lo cual el auditor determina la materialidad para los estados financieros y los procesos que conlleva, con el propósito de determinar la naturaleza y el alcance de los procedimientos.

Ejecución de Auditoria Informática

La ejecución de la auditoría informática constituye la recopilación de la mayor cantidad de información necesaria, como son documentos y evidencias

que permitan al auditor fundamentar sus comentarios, sugerencias y recomendaciones, con respecto al manejo y administración de TI.

Para la recolección de información, se pueden aplicar las siguientes técnicas:

- Entrevistas
- Simulación
- Cuestionarios
- Análisis de la información documental entregada por el auditado
- Revisión y Análisis de Estándares
- Revisión y Análisis de la información de auditorías anteriores

Toda la información entra luego en un proceso de análisis, el cual debe ser realizado utilizando un criterio profesional por parte de los auditores y el equipo a cargo del proceso de Auditoría, toda la información recopilada debe ser clasificada de manera que nos permita ubicarla fácilmente y además permita, luego del análisis respectivo, justificar de manera correcta las recomendaciones.

La evidencia se clasifica de la siguiente manera:

- Evidencia documental.
- Evidencia física.
- Evidencia analítica.
- Evidencia testimonial.

Una vez que tenemos información real y confiable, procedemos a evaluar y probar la manera en la que han sido diseñados los controles en la organización, para el mejoramiento continuo de la misma, para esto el equipo de Auditoría utilizara medios informáticos y electrónicos que permitan obtener resultados reales. El equipo de auditores, para poder dar una opinión sobre un sistema o proceso informático, debe comprobar el funcionamiento de los sistemas de aplicación y efectuar una revisión completa de los equipos de cómputo

Control Interno

Los controles internos son métodos implementados por una empresa para garantizar la integridad de la información financiera y contable, cumplir los objetivos operativos y de rentabilidad y transmitir las políticas de gestión en toda la organización. Los controles internos funcionan mejor cuando se aplican a múltiples divisiones y se ocupan de las interacciones entre los distintos departamentos comerciales. No hay dos sistemas de controles internos idénticos, pero muchas filosofías centrales con respecto a la integridad financiera y las prácticas contables se han convertido en prácticas de gestión estándar. (Investopedia)

Clasificación de controles de TI

Al momento de realizar un proyecto de auditoría, se desarrollan una gran variedad de actividades de control para verificar la exactitud, integridad y autorización de las transacciones. Estas actividades pueden agruparse en dos grandes conjuntos de controles de los sistemas de información, los cuales son: controles de aplicación y los controles generales de la computadora. Sin embargo, estos dos conjuntos de controles se encuentran estrechamente relacionados, puesto que, los controles generales de la computadora son normalmente necesarios para soportar el funcionamiento de los controles de aplicación, además de la efectividad de ambos depende el aseguramiento del procesamiento completo y preciso de la información.

Controles de aplicación

Los controles de aplicación son procedimientos manuales o automatizados que operan típicamente a nivel de los procesos de la organización. Los controles de aplicación pueden ser de naturaleza preventiva o de detección y están diseñados para asegurar la integridad de la información que se procesa en ellos. Debido a lo cual, los controles de aplicación se relacionan con los procedimientos utilizados para iniciar, registrar, procesar e informar las transacciones de la organización. Estas actividades de control ayudan a asegurar que las transacciones ocurridas, estén autorizadas y completamente registradas y procesadas con exactitud.

Debido al tamaño y complejidad de varios sistemas, no siempre se los podrá revisar a todos, por lo que es necesario evaluar los sistemas de aplicación para considerar en el plan de auditoría los sistemas de aplicación que tienen un efecto significativo en el desarrollo de las operaciones de la organización, con el fin de realizar un análisis más profundo de estos sistemas. Existen varios parámetros que se deben considerar para calificar los sistemas de aplicación, siendo los siguientes:

- Importancia de las transacciones procesadas.
- Potencial para el riesgo de error incrementado debido a fraude.
- Si el sistema sólo realiza funciones sencillas, como acumular o resumir información o funciones más complejas, como la iniciación y ejecución de transacciones.
- Tamaño y complejidad de los sistemas de aplicación

Se debe incluir los controles implantados, para verificar la validez del ingreso de datos dentro de los sistemas, controles que podemos evaluar mediante el seguimiento manual de los informes de excepción o la corrección en el punto de entrada de datos. Debido al tamaño y complejidad de varios sistemas, no siempre se los podrá revisar a todos, por lo que es necesario evaluar los sistemas de aplicación para considerar en el plan de auditoría aquellos que tienen un efecto significativo en el desarrollo de las operaciones de la organización, con el fin de realizar un análisis más profundo de estos sistemas.

Controles Generales

Los controles generales son políticas y procedimientos que se relacionan con muchos sistemas de aplicación y, soportan el funcionamiento eficaz de los controles de aplicación, ayudando a asegurar la operación continua y apropiada de los sistemas de información. Los controles generales mantienen la integridad de la información y la seguridad de los datos. Es por esto que antes de realizar una evaluación de los controles de aplicación, normalmente se actualiza la comprensión general de los controles del

ambiente de procesamiento de la computadora y se emite una conclusión acerca de la eficacia de estos controles.

Las actividades que se llevan a cabo para la evaluación de estos controles inician con entrevistas a la administración, luego de las cuales se tendrá una mejor capacidad para comprender y definir la estrategia y las pruebas que realizaremos sobre los controles. Posteriormente, se debe determinar si los controles generales de la computadora se diseñan e implementan para soportar el procesamiento confiable de la información, respecto a los controles que se han identificado, para lo cual se debe realizar lo siguiente:

- Evaluación del diseño de los controles, en la que se determinará que los controles evitan los riesgos para los que fueron diseñados.
- Determinar si los controles se han implementado, lo cual consiste en evaluar si los controles que se han diseñado y, se están utilizando durante el tiempo de funcionamiento de la organización.

Entorno de Control

El entorno de control marca la pauta del comportamiento en una organización, siendo la base de todos los demás elementos del control interno:

- Disciplina,
- Valores éticos,
- Capacidad,
- Estructura,
- Segregación de funciones y
- La filosofía como la Dirección distribuye la autoridad y la responsabilidad para organizar y desarrollar profesionalmente a las personas que integran la organización.

El control interno, consiste en un proceso multidireccional repetitivo y permanente, en el cual más de un componente influye en los otros y conforman un sistema integrado que reacciona dinámicamente a las condiciones cambiantes. (Romero J. , 2012)

Niveles de Efectividad

Los sistemas de control interno operan con distintos niveles de efectividad; puede ser juzgado efectivo en cada uno de los tres grupos, respectivamente, si el consejo de administración o junta y la gerencia tienen una razonable seguridad de que:

- Entienden el grado en que se alcanzan los objetivos de las operaciones de las entidades.
- Los informes financieros sean preparados en forma confiable.
- Se observen las leyes y los reglamentos aplicables.

Ambiente de Control

Consiste en el establecimiento de un entorno que se estimule e influencie la actividad del personal con respecto al control de sus actividades. Es la base de los demás componentes de control a proveer disciplina y estructura para el control e incidir en la manera como: (Romero J. , 2012)
Se estructuran las actividades del negocio.

- Se asigna autoridad y responsabilidad.
- Se organiza y desarrolla la gente.
- Se comparten y comunican los valores y creencias.
- La personal toma conciencia de la importancia del control.

Factores del Ambiente de Control:

- La integridad y los valores éticos.
- El compromiso a ser competente.
- Las actividades de la junta directiva y el comité de auditoría.
- La mentalidad y estilo de operación de la gerencia.
- La estructura de la organización.
- La asignación de autoridad y responsabilidades.
- Las políticas y prácticas de recursos humanos.

El ambiente de control se determina por el conjunto de circunstancias que en marcan el accionar de una entidad, organización o empresa, desde una perspectiva de control interno y que son determinantes para el

cumplimiento de las metas y objetivos de la organización en que los principios y políticas actúan, sobre las conductas y los procedimientos organizacionales.

El sistema de control interno está relacionado directamente con las actividades operativas y de procedimiento dentro de la organización y, existen por razones empresariales fundamentales y, a que estos fomentan la eficiencia, reducen el riesgo de pérdida de valor de los activos y, ayudan a garantizar la fiabilidad de los estados financieros y el cumplimiento de las leyes y normas vigentes.

El ambiente de control se puede definir como un proceso, efectuado por el personal de una organización, diseñado para conseguir objetivos específicos. La definición es amplia y cubre todos los aspectos de control de un negocio, pero al mismo tiempo, permite centrarse en objetivos específicos.

Evaluación de Riesgos

Es la identificación y análisis de riesgos relevantes para el logro de los objetivos y la base para determinar la forma en que tales riesgos deben ser mejorados. Así mismo, se refiere al mecanismo necesario para identificar y manejar riesgos específicos asociados con los cambios, tanto los que influyen en el entorno de la organización como en su interior.

En toda entidad, es indispensable el establecimiento de objetivos tanto globales de la organización como de actividades relevantes, obteniendo con ello una base sobre la cual sean identificados y analizados los factores de riesgo que amenazan su oportuno cumplimiento.

La evolución de riesgos debe ser una responsabilidad ineludible para todos los niveles que están involucrados en el logro de los objetivos. Esta actividad de autoevaluación debe ser revisada por los auditores internos para asegurar que tanto el objetivo, enfoque, alcance y procedimiento han sido apropiadamente llevados a cabo.

Toda entidad enfrenta una variedad de riesgos provenientes de fuentes externas e internas que deben ser evaluados por la gerencia quien, a su vez, establece objetivos generales y específicos e identifica y analiza los riesgos de que dichos objetivos no se logren o afecten su capacidad para salvaguardar sus bienes y recursos, mantener ventaja ante la competencia.

Construir y conservar su imagen, incrementar y mantener su solidez financiera, crecer, etc.

Objetivos

Su importancia es evidente en cualquier organización, ya que representa la orientación básica de todos los recursos y esfuerzos y proporciona una base sólida para un control interno efectivo. La fijación de objetivos es el camino adecuado para identificar factores críticos de éxito. (Romero J. , 2012)

Las categorías de los objetivos son las siguientes:

- Objetivos de Cumplimiento. Están dirigidos a la adherencia a leyes y reglamentos, así como también a las políticas emitidas por la administración.
- Objetivos de Operación. Son aquellos relacionados con la efectividad y eficacia de las operaciones de la organización.
- Objetivos de la Información Financiera. Se refieren a la obtención de información financiera confiable.

El logro de los objetivos antes mencionados está sujeto a los siguientes eventos:

- Los controles internos efectivos proporcionan una garantía razonable de que los objetivos de información financiera y de cumplimiento serán logrados, debido a que están dentro del alcance de la administración.
- En relación a los objetivos de operación, la situación difiere de la anterior debido a que existen eventos fuera de control del ente o controles externos. Sin embargo, el propósito de los controles en esta categoría está dirigido a evaluar la consistencia e interrelación entre los objetivos y metas en los distintos niveles, la identificación de factores críticos de éxito y la manera en que se reporta el avance de los resultados y se implementan las acciones indispensables para corregir desviaciones.

Los riesgos de actividades también deben ser identificados, ayudando con ello a administrar los riesgos en las áreas o funciones más importantes; las causas en este nivel pertenecen a un rango amplio que va desde lo obvio hasta lo complejo y con distintos grados de significación, deben incluir entre otros aspectos los siguientes: (Romero J. , 2012)

La estimación de la importancia del riesgo y sus efectos.

- La evaluación de la probabilidad de ocurrencia.
- El establecimiento de acciones y controles necesarios.
- La evaluación periódica del proceso anterior.

Actividades de Control

Son aquellas que realiza la gerencia y demás personal de la organización para cumplir diariamente con las actividades asignadas. Estas actividades están expresadas en las políticas, sistemas y procedimientos. Las actividades de control tienen distintas características. Pueden ser manuales o computarizadas, administrativas u operacionales, generales o específicas, preventivas. Sin embargo, lo trascendente es que, sin importar su categoría o tipo, todas ellas están apuntando hacia los riesgos (reales o potenciales) en beneficio de la organización, su misión y objetivos, así como la protección de los recursos propios o de terceros en su poder. (Romero J. , 2012)

Las actividades de control son importantes no solo porque en sí mismas implican la forma correcta de hacer las cosas, sino debido a que son el medio idóneo de asegurar en mayor grado el logro de objetivos. (Romero J. , 2012)

Información y Comunicación

Están diseminados en todo el ente y todos ellos atienden a uno o más objetivos e control. De manera amplia, se considera que existen controles generales y controles de aplicación sobre los sistemas de información.

- **Controles Generales:** Tienen como propósito asegurar una operación y continuidad adecuada, e incluyen al control sobre el centro de procesamiento de datos y su seguridad física, contratación y mantenimiento del hardware y software, así como la operación propiamente dicha. También se relacionan con las funciones de

desarrollo y mantenimiento de sistemas, soporte técnico y administración de base de datos.

- **Controles de Aplicación**: Están dirigidos hacia el interior de cada sistema y funcionan para lograr el procesamiento, integridad y confiabilidad, mediante la autorización y validación correspondiente. Desde luego estos controles cubren las aplicaciones destinadas a las interfases con otros sistemas de los que se reciben o entregan información.

Los sistemas de información y tecnología son y serán sin duda un medio para incrementar la productividad y competitividad. Ciertos hallazgos sugieren que la integración de la estrategia, la estructura organizacional y la tecnología de información es un concepto clave para el nuevo siglo. (Romero J. , 2012)

Con frecuencia se pretende evaluar la situación actual y predecir la situación futura sólo con base en la información contable. Este enfoque es simplista, por su parcialidad, sólo puede conducir a juicios equivocados.

Para todos los efectos, es preciso estar consciente de que la contabilidad nos dice, en parte, lo que ocurrió, pero no lo que va a suceder en el futuro. Los sistemas producen reportes que contienen información operacional, financiera y de cumplimiento que hace posible conducir y controlar la organización.

La información generada internamente, así como aquella que se refiere a eventos acontecidos en el exterior, es parte esencial de la toma de decisiones, así como en el seguimiento de las operaciones. La información cumple con distintos propósitos a diferentes niveles. (Romero J. , 2012)

Supervisión y Seguimiento

En general, los sistemas de control están diseñados para operar en determinadas circunstancias. Claro está que para ello se tomaron en consideración los objetivos, riesgos y las limitaciones inherentes al control; sin embargo, las condiciones evolucionan debido tanto a factores externos como internos, provocando con ello que los controles pierdan su eficiencia.

Como resultado de todo ello, la gerencia debe llevar a cabo la revisión y evaluación sistemática de los componentes y elementos que forman parte de los sistemas de control. Lo anterior no significa que tenga que revisarse todos los componentes y elementos, como tampoco que deba hacerse al mismo tiempo.

La evaluación debe conducir a la identificación de los controles débiles, insuficientes o innecesarios, para promover con el apoyo decidido de la gerencia, su robustecimiento e implantación. Esta evaluación puede llevarse a cabo de tres formas: durante la realización de las actividades diarias en los distintos niveles de la organización; de manera separada por personal que no es el responsable directo de la ejecución de las actividades (incluidas las de control) y mediante la combinación de las dos formas anteriores. Para un adecuado seguimiento (monitoreo) se deben tener en cuenta las siguientes reglas:

- El personal debe obtener evidencia de que el control interno está funcionando.
- Sí las comunicaciones externas corroboran la información generada internamente.
- Se deben efectuar comparaciones periódicas de las cantidades registradas en el sistema de información contable con el físico de los activos.
- Revisar si se han implementado controles recomendados por los auditores internos y externos; o por el contrario no se ha hecho nada o poco.
- Sí son adecuadas, efectivas y confiables las actividades del departamento de la auditoría interna.

Estándares y Normas Internaciones para Seguridad de la Información

El uso de estándares puede ofrecer un conjunto de potentes herramientas comerciales y de marketing para organizaciones de todos los tamaños. Puede usarlos para ajustar su rendimiento y administrar los riesgos

que enfrentan mientras opera de manera mas eficiente y sostenible te ayudan a ver como se podrían incorporar las mejores prácticas en la organización para la toma de decisiones.

A nivel internacional se toman como referencias para ser aplicadas en sus organizaciones las normas: COBIT 5 , ISO 27001, Itil, Coso, Magerit, ISO3100.

Para el desarrollo de este proyecto se tomarán como marco referencias las normas ISO 27001 y COBIT 5 las cuales se presenta en detalle a continuación:

ISO 27001-2013

Contenido de la ISO 27001- 2013

El SGSI es un proceso sistemático, organizado y documentado para implementar y gestionar la seguridad de la información en una organización buscando mantener la confidencialidad, integridad y disponibilidad.

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. (27001Academy, s.f.)

Es un estándar certificable, es decir, cualquier organización que tenga implantado un SGSI según este modelo puede solicitar una auditoría externa por parte de una entidad acreditada y, tras superar con éxito la misma, recibir la certificación en ISO 27001. (27001Academy, s.f.)

Trabaja en función a 8 principios de gestión:

- Orientación al cliente.
- Liderazgo.
- Participación del personal.
- Enfoque de procesos.
- Enfoque de sistemas de gestión.
- Mejora Continua.
- Enfoque de mejora continua.
- Relación mutuamente beneficiosa con el proveedor

Confidencialidad de los datos

Es cuando un usuario o empleado de la empresa garantice seguridad al momento de ingresar a la información no divulgando dicha información a personas ajenas a la empresa con ellos se busca conseguir una seguridad donde los que puedan acceder a los datos son los administradores del sistema o la misma gerencia.

Disponibilidad de Datos

La disponibilidad de datos es el acceder a la información de la empresa a tiempo o la hora que sea con el fin que los usuarios alteren, actualicen, respalden los datos útiles y no tener pérdidas financieras o de personal.

Integridad de Datos

La integridad de datos hace referencia a que los datos no pueden ser alterados por ningún tipo de personal, solo por alta dirección, para ello deben de tener un tipo de seguridad que ayude al manejo debido de los datos para beneficio propio de la empresa. (27001Academy, s.f.)

Beneficios de la ISO 27001 – 2013

Demuestra la garantía independiente de los controles internos y cumple los requisitos de gestión corporativa y de continuidad de la actividad comercial. Demuestra independientemente que se respetan las leyes y normativas que sean de aplicación

Proporciona una ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de la información es primordial verifica independientemente que los riesgos de la organización estén correctamente identificados evaluados y gestionados al tiempo que formaliza uno procesos, procedimientos y documentación de protección de la información.

Generalidades de la ISO 27001 – 2013

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa.

Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se

produzcan (es decir, mitigación o tratamiento del riesgo). (27001Academy, s.f.)

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente para lograr que se cumplan objetivos de las organizaciones y tener un regulador que ayude en todo momento a la detección de los problemas que se pueden suscitar y mitigarlos.

Ilustración 1 *Estructura de ISO 27001*

Fuente: 27001 Academy

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos). Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software, pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas

organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.

Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI). (27001Academy, s.f.)

Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, cortafuegos, anti-virus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc.

Ventajas de Implantación de la norma

Hay 4 ventajas comerciales esenciales que una empresa puede obtener con la implementación de esta norma para la seguridad de la información:

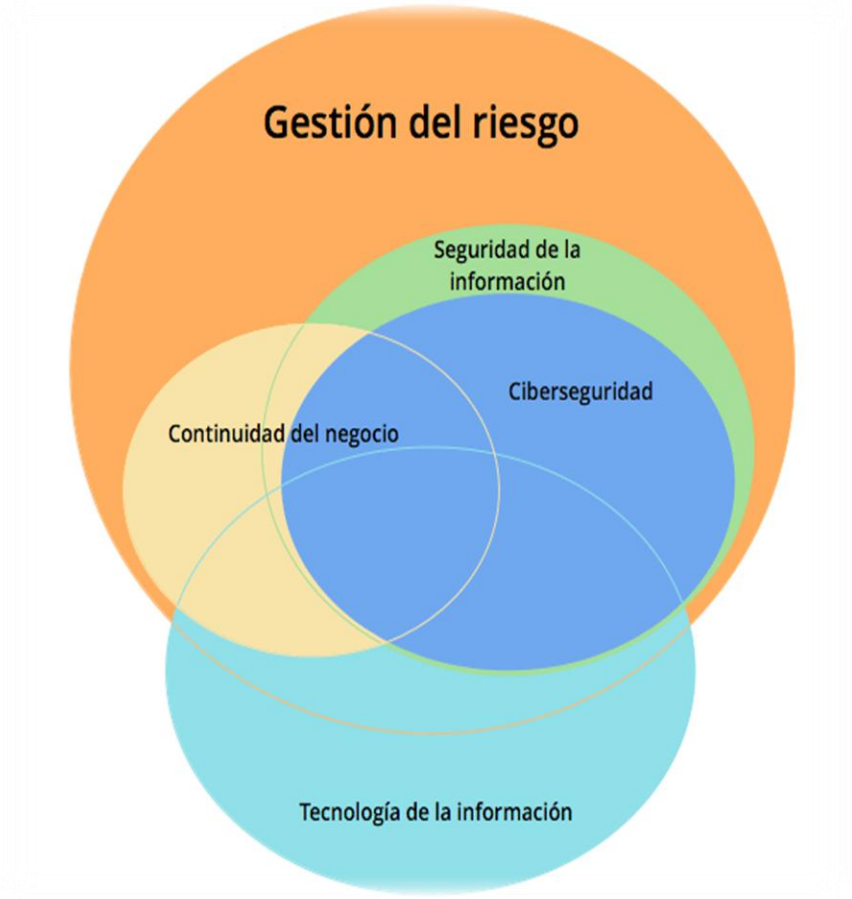
- **Cumplir con los requerimientos legale**s: cada vez hay más y más leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información. La buena noticia es que la mayoría de ellos se pueden resolver implementando ISO 27001 ya que ésta norma le proporciona una metodología perfecta para cumplir con todos ellos. (27001Academy, s.f.)
- **Obtener una ventaja comercial**: si su empresa obtiene la certificación y sus competidores no, es posible que usted obtenga una ventaja sobre ellos ante los ojos de los clientes a los que les interesa mantener en forma segura su información. (27001Academy, s.f.)
- **Menores costos**: la filosofía principal de ISO 27001 es evitar que se produzcan incidentes de seguridad, y cada incidente, ya sea grande o pequeño, cuesta dinero; por lo tanto, evitándolos su empresa va a ahorrar mucho dinero. Por tanto, la inversión en ISO 27001 es mucho menor que el ahorro que obtendrá. (27001Academy, s.f.)
- **Una mejor organización**: en general, las empresas de rápido crecimiento no tienen tiempo para hacer una pausa y definir sus

procesos y procedimientos; como consecuencia, muchas veces los empleados no saben qué hay que hacer, cuándo y quién debe hacerlo. La implementación de ISO 27001 ayuda a resolver este tipo de situaciones ya que alienta a las empresas a escribir sus principales procesos, lo que les permite reducir el tiempo perdido de sus empleados. (27001Academy, s.f.)

¿Dónde Interviene la gestión de Seguridad de la Información en una empresa?

Básicamente, la seguridad de la información es parte de la gestión global del riesgo en una empresa, hay aspectos que se superponen con la ciberseguridad, con la gestión de la continuidad del negocio y con la tecnología de la información: (27001Academy, s.f.)

Ilustración 2 *Gestión de Seguridad de la Información en una empresa*



Fuente: 27001 Academy

Implementación de ISO 27001

Para implementar la norma ISO 27001 en una empresa, se tiene que seguir estos 16 pasos:

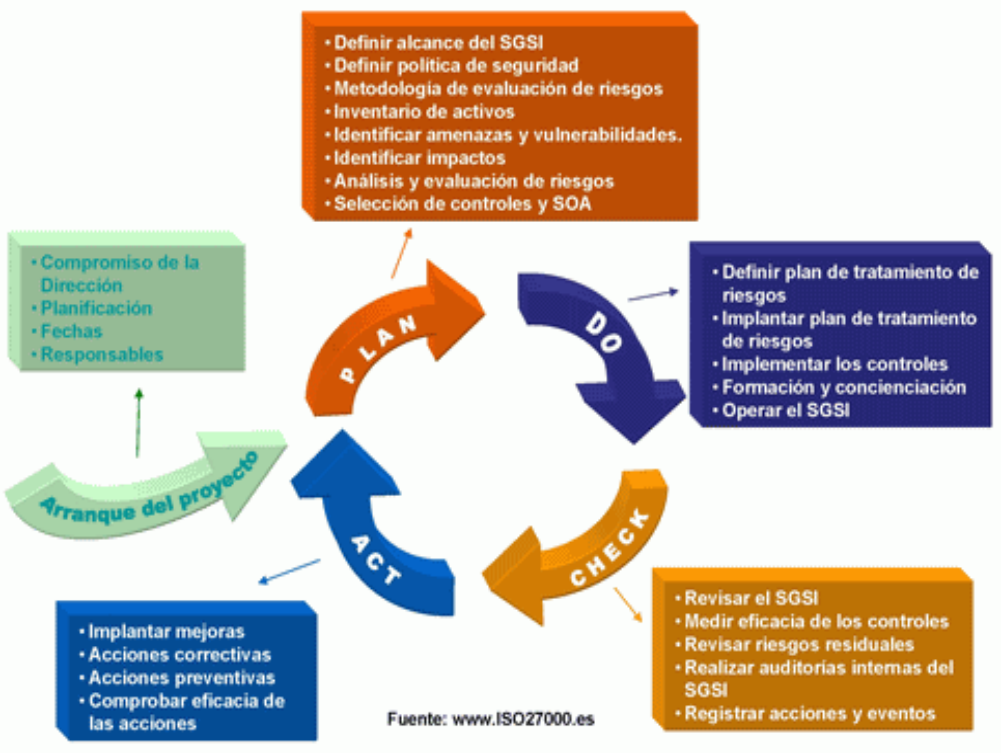
- Obtener el apoyo de la dirección
- Utilizar una metodología para gestión de proyectos
- Definir el alcance del SGSI
- Redactar una política de alto nivel sobre seguridad de la información
- Definir la metodología de evaluación de riesgos
- Realizar la evaluación y el tratamiento de riesgos
- Redactar el Plan de tratamiento de riesgos
- Definir la forma de medir la efectividad de sus controles y de su SGSI
- Implementar todos los controles y procedimientos necesarios
- Implementar programas de capacitación y concienciación
- Realizar todas las operaciones diarias establecidas en la documentación de su SGSI
- Monitorear y medir su SGSI
- Realizar la auditoría interna
- Realizar la revisión por parte de la dirección
- Implementar medidas correctivas

Ciclo Deming

CICLO PHVA ISO 27001:2013 El ciclo PHVA significa actuar sobre el proceso, resolviendo continuamente las desviaciones a los resultados esperados. El mantenimiento y la mejora continua de la capacidad del proceso pueden lograrse aplicando este ciclo en cualquier nivel de la organización y en cualquier tipo de proceso, ya que se encuentra asociado con la planificación, implementación, control y mejora del desempeño de los procesos. (27001Academy, s.f.)

- Planear: establecer los objetivos para obtener resultados.
- Hacer: implementar procesos para alcanzar resultados.
- Verificar: realizar seguimiento y medir los procesos.
- Actuar: realizar acciones para promover la mejora del desempeño.

Ilustración 3 *Ciclo Deming*



Fuente: www.ISO27001.es

Planificar

Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión. Es importante que defina los límites del SGSI ya que no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado). (27001Academy, s.f.)

Es importante disponer de un mapa de procesos de negocio, definir claramente los interfaces con el exterior del alcance, determinar las terceras partes (proveedores, clientes...) que tienen influencia sobre la seguridad de la información del alcance, crear mapas de alto nivel de redes y sistemas, definir las ubicaciones físicas, disponer de organigramas organizativos, definir claramente los requisitos legales y contractuales relacionados con seguridad de la información, etc. (27001Academy, s.f.)

La política del SGSI es normalmente un documento muy general, una especie de "declaración de intenciones" de la Dirección pero que:

Incluya el marco general y los objetivos de seguridad de la información de la organización;

- Tenga en cuenta los requisitos de negocio además de considerar los requerimientos legales o contractuales relativos a la seguridad de la información;
- Esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI;
- Establezca los criterios con los que se va a evaluar el riesgo;
- Esté aprobada por la dirección

Hacer

Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.
- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.

Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.

- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.
- Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.

Verificar

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión para:
    - Detectar a tiempo los errores en los resultados generados por el procesamiento de la información;
    - Identificar brechas e incidentes de seguridad;
    - Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto;
    - Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;
    - Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.
- Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.
- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.-.
- Realizar periódicamente auditorías internas del SGSI en intervalos planificados para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001:2005, el entorno legal y los requisitos y objetivos de

seguridad de la organización, están implementados y mantenidos con eficacia y tienen el rendimiento esperado. Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y posibles mejoras en el proceso del SGSI, a la política de seguridad o a los objetivos de seguridad de la información.

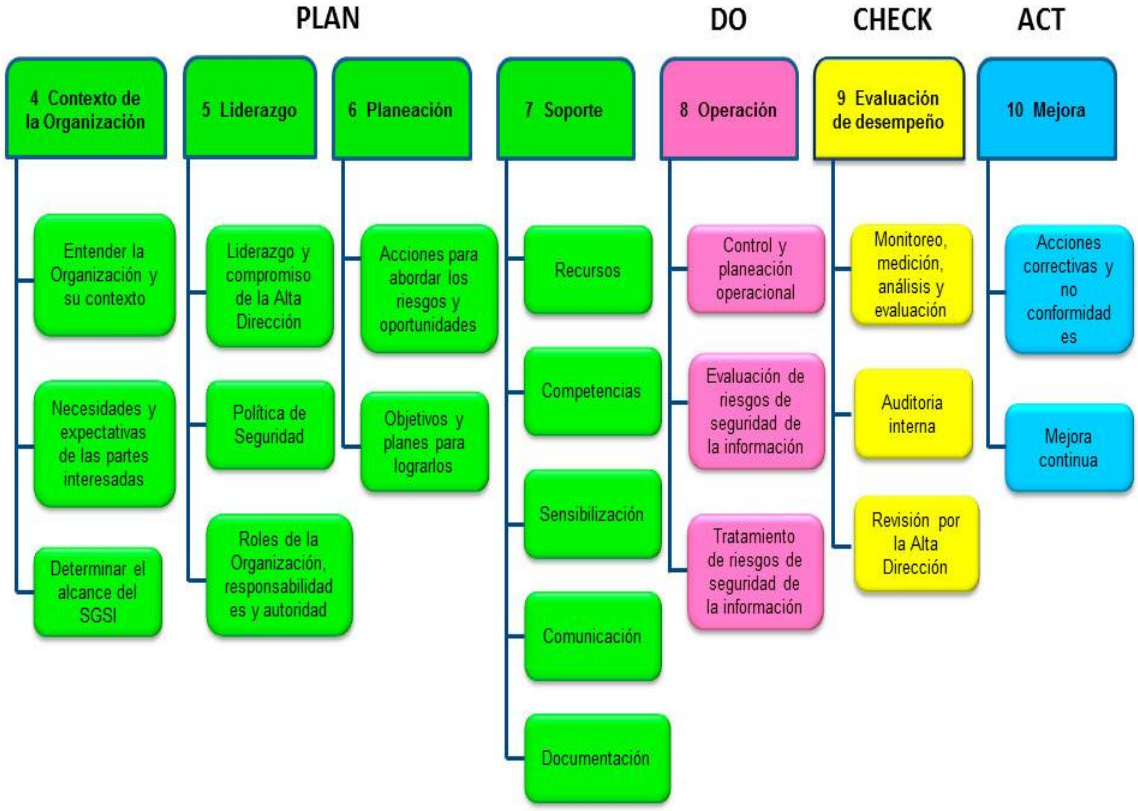
- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

Actuar

La organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas para prevenir potenciales no conformidades antes de que se produzcan y solucionar no conformidades detectadas y materializadas
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre. PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de actuar lleva de nuevo a la fase de planear para iniciar un nuevo ciclo de las cuatro fases. Téngase en cuenta que no tiene que haber una secuencia estricta de las fases, sino que, p. ej., puede haber actividades de implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado; o que se monitorizan controles que aún no están implantados en su totalidad.

Ilustración 4 *Ciclo PDCA en ISO 27001: 2013*



Fuente https://*trabajoscun.wordpress.com/category/*auditoria-de-sistemas/

COBIT 5

Conocimiento del COBIT

COBIT 5 es un marco de trabajo que permite comprender el gobierno y la gestión de las tecnologías de información (TI) de una organización, así como evaluar el estado en que se encuentran las TI en la empresa.

Control Objectives for Information and related Technology o COBIT 5 también se puede definir como un conjunto de herramientas de soporte empleadas por los gerentes para reducir la brecha entre los requerimientos de control, los temas técnicos y los riesgos del negocio. (ISACA, 2012)

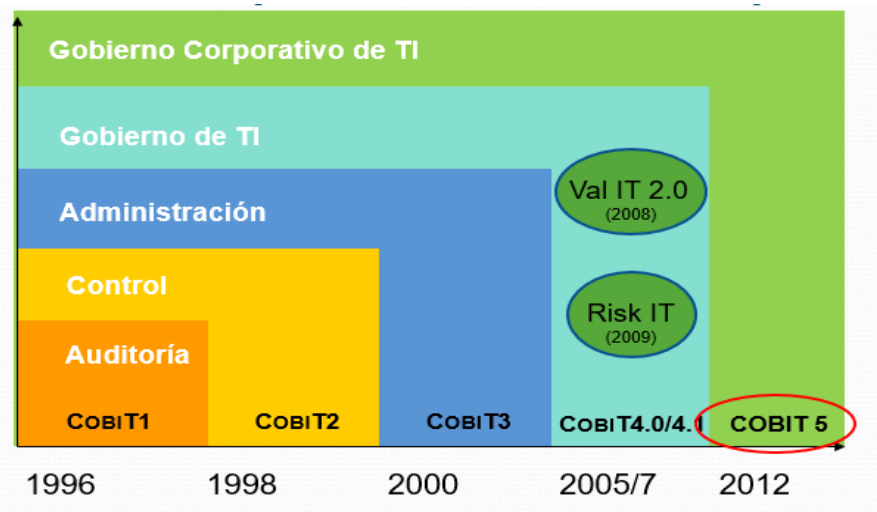
Mediante COBIT 5 se puede desarrollar una política clara que permite el control de las TI en la organización. La aplicación de este marco incide especialmente en el cumplimiento regulatorio y ayuda a incrementar el valor asociado al área de TI de la organización. (ISACA, 2012)

COBIT permite el desarrollo de políticas claras y mejores prácticas para la administración de TI. También ayuda a las organizaciones a gestionar los riesgos relacionados con TI y a asegurar el cumplimiento, la continuidad, seguridad y privacidad.

Para el desarrollo de la presente tesis de auditoria informática se están optando dos modelos internacionales siendo uno de ellos el COBIT del cual se realiza el análisis con la versión 5 ya que nos permite dar un enfoque integral, no solo abarca el área de Tecnología de la información, sino más bien abarca de principio a fin toda la empresa es un gobierno corporativo a diferencia del gobierno de TI.

Se adoptó el Modelo COBIT 5, ya que previamente se hizo una revisión a las otras versiones de COBIT en la cual se identificaron las siguientes características de cada versión anterior. (ISACA, 2012)

Ilustración 5 *Evolución del COBIT*



Fuente //www.isaca.org/COBIT/Documents/COBIT5-Introduction-Spanish.ppt

Versión 1.0: La primera edición del COBIT fue publicada en 1996 esta incluía la colección y análisis de fuentes internacionales reconocidas, con la

investigación y mejores prácticas llevaron al desarrollo de Objetivos del control.

Versión 2.0: En 1998 la segunda edición su cambio principal fue la adición de las guías de gestión. El control de los elementos de arquitectura de sistemas de desarrollo de mismo personal.

Versión 3.0: Fue posterior al 2003 que el marco de referencia de COBIT fue revisado y mejorado para soportar el incremento del control gerencial, introducir el manejo del desempeño y mayor desarrollo del Gobierno de TI.

Versión 4.0: Esquema de Gobernabilidad especifica cómo se debe utilizar los recursos, los proceso las políticas más la auditoria y la administración, recalca el cumplimiento ayudando a las organizaciones para aumentar los logros de TI considerando que posee un enfoque un poco más gerencial el cual ayuda con las alineaciones para simplificar las partidas emitidas del modelo COBIT.

Versión 5: Permite ayudar a las empresas a guiar la toma de decisiones basadas en las necesidades de todos los grupos de interés, la oferta de servicios disponibles, así como los costos y riesgos involucrados en la adopción de esta tecnología en la empresa. Un ejemplo claro, es que COBIT 5 puede guiar a las empresas a tomar decisiones sobre el gobierno del cómputo en la nube

Luego de este análisis se concluyó que la versión 5, provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Ayuda a las empresas a crear el valor óptimo desde TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. (ISACA, 2012)

Generalidades del COBIT

COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los

intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público.

Principios Básicos del Cobit

Del COBIT 5 se desprenden 5 principios básicos que son

Ilustración 6 *Principios básicos del COBIT*

Fuente: COBIT® 5, Figura 2. © 2012 ISACA

Principio 1. Satisfacer las Necesidades de las Partes Interesadas:

Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos. COBIT 5 provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI.

Dado que toda empresa tiene objetivos diferentes, una empresa puede personalizar COBIT 5 para adaptarlo a su propio contexto mediante la cascada de metas, traduciendo metas corporativas de alto nivel en otras metas más manejables, específicas, relacionadas con TI y mapeándolas con procesos y prácticas específicos.

Ilustración 7 *Objetivos de Gobierno Creación de Valor*

Fuente: COBIT® 5, Figura 3. © 2012 ISACA

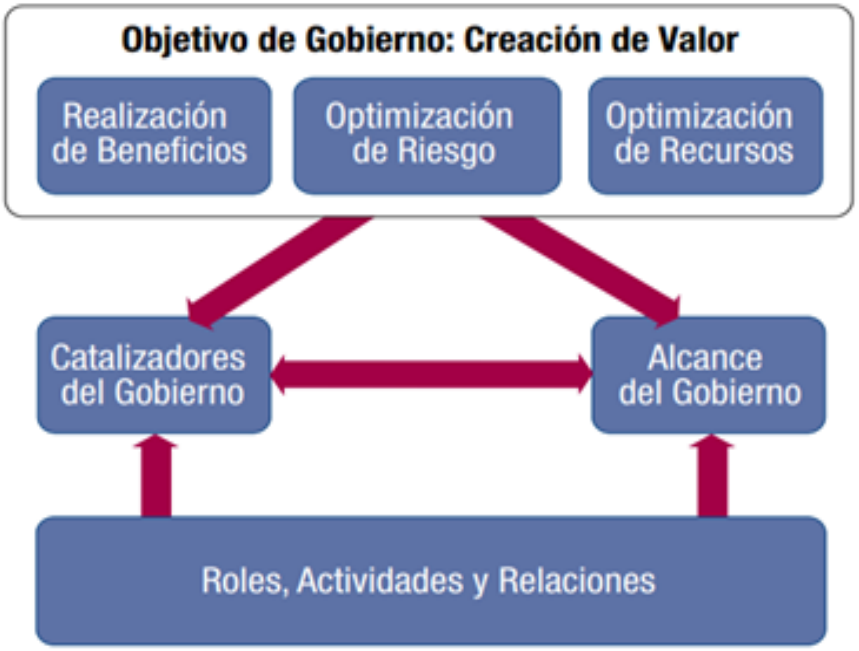
Principio 2: Cubrir la Empresa Extremo-a-Extremo:

COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo:

- Cubre todas las funciones y procesos dentro de la empresa; COBIT 5 no se enfoca sólo en la "función de TI", sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa.
- Considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo a todo y todos – internos y externos – los que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionadas.

Además del objetivo de gobierno, el otro elemento principal del enfoque de gobierno incluye catalizadores, alcance y roles, actividades y relaciones. (ISACA, 2012)

Ilustración 8 *Gobierno y Gestión en COBIT 5*



Fuente COBIT® 5, Figura 8. © 2012 ISACA

Principio 3: Aplicar un Marco de Referencia único integrado:

Hay muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las Ti de la empresa. (ISACA, 2012)

Principio 4: Hacer Posible un Enfoque Holístico:

Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos.

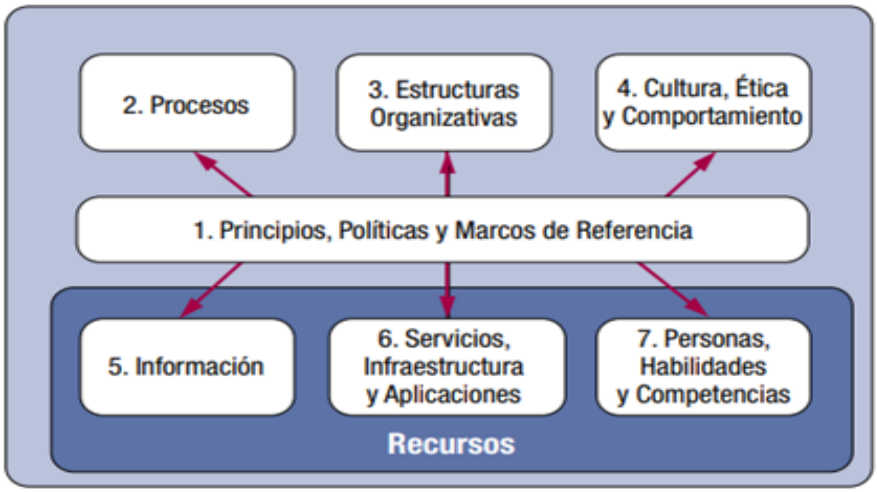
COBIT 5 define un conjunto de catalizadores (enablers) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa.

Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. (ISACA, 2012)

El marco de trabajo COBIT 5 define siete categorías de catalizadores:

- Principios, Políticas y Marcos de Trabajo
- Procesos
- Estructuras Organizativas
- Cultura, Ética y Comportamiento
- Información – Servicios, Infraestructuras y Aplicación
- Personas, Habilidades y Competencias

Ilustración 9 *Catalizadores Corporativos COBIT 5*



Fuente COBIT® Figura 12 . © 2012 ISACA

Los catalizadores pueden ser identificados como recursos corporativos en algunas organizaciones pueden ayudar en algunos aspectos como en la información (ISACA, 2012)

Principio 5: Separar el Gobierno de la Gestión:

El marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. La visión de COBIT 5 en esta distinción clave entre gobierno y gestión es:

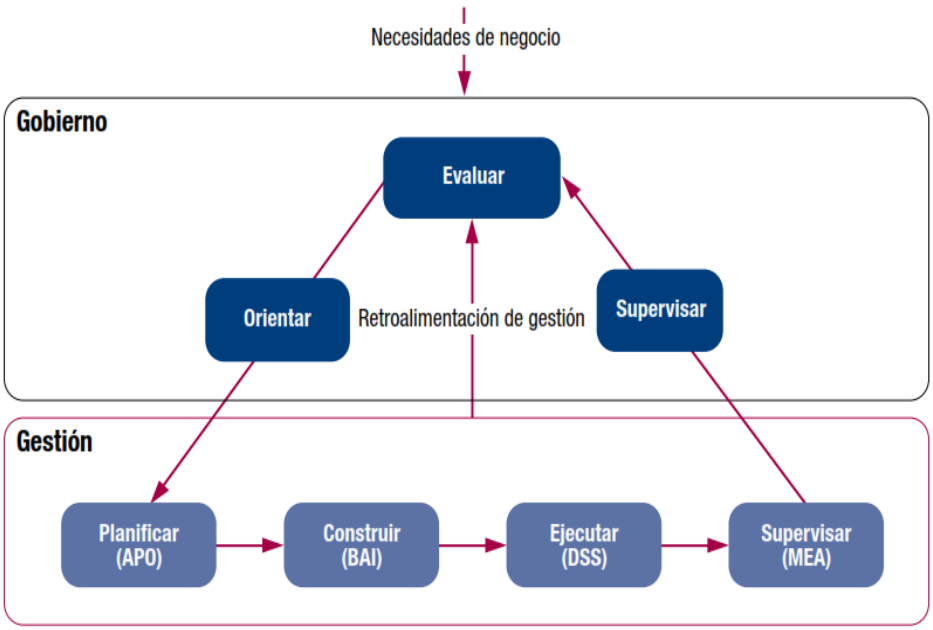
Gobierno: asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

En muchas corporaciones, el gobierno global es responsabilidad del comité de dirección bajo el liderazgo del presidente. Algunas responsabilidades de gobierno específicas se pueden delegar en estructuras organizativas especiales al nivel apropiado, particularmente en las corporaciones más grandes y complejas. (ISACA, 2012)

Gestión: Planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

COBIT 5 no es prescriptivo, pero sí defiende que las empresas implementen procesos de gobierno y de gestión de manera que las áreas fundamentales estén cubiertas, tal y como se muestra en la gráfica siguiente:

Ilustración 10 *Las áreas clave de Gobierno y Gestión COBIT 5*



Fuente COBIT® Figura 15 . © 2012 ISACA

El modelo de referencia de procesos de COBIT 5 divide los procesos de gobierno y de gestión de la TI empresarial en dos dominios principales de procesos:

- Gobierno Contiene cinco procesos de gobierno; dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión (EDM)
- Gestión Contiene cuatro dominios, en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar y supervisar (Plan, Build, Run and Monitor - PBRM), y proporciona cobertura extrema a extremo de las TI.

Los nombres de estos dominios han sido elegidos de acuerdo con estas designaciones de áreas principales, pero contienen más verbos para describirlos:

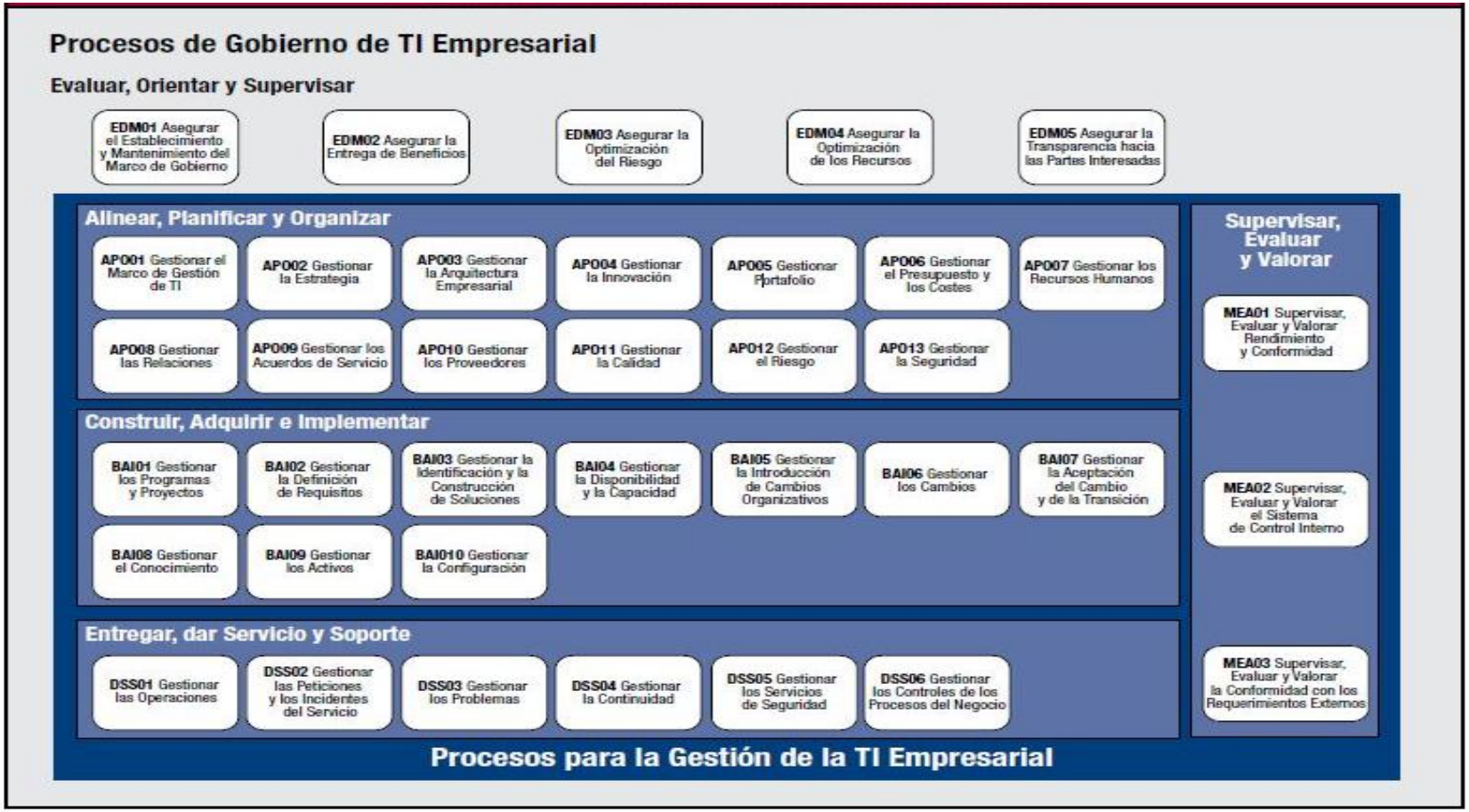
- Alinear, Planificar y Organizar (Align, Plan and Organise, APO)
- Construir, Adquirir e Implementar (Build, Acquire and Implement, BAI)
- Entregar, dar Servicio y Soporte (Deliver, Service and Support, DSS)
- Supervisar, Evaluar y Valorar (Monitor, Evaluate and Assess, (ISACA, COBIT 5 FRAMEWORK, 2012 ISACA)

Procesos de Gobierno y Gestión

COBIT presenta un conjunto de treinta y siete procesos de gobierno y gestión que pueden ser identificados cada uno de ellos los cuales se comprenden de cinco dominios:

- Evaluar Orienta y Supervisar
- Alinear planificar y organizar
- Construir adquirir e implementar
- Entregar dar servicio y soporte
- Supervisar evaluar y valorar

Ilustración 11 *Modelo de Referencia de procesos de COBIT*



Fuente COBIT® Figura 16 . © 2012 ISACA

Cascada de metas de COBIT 5

Las necesidades de las partes interesadas deben transformarse en una estrategia corporativa factible. La cascada de metas transforma las metas individuales requeridas por los partes interesados con la Ti. Esta traducción permite establecer metas específicas en todos los niveles y en todas las áreas de la empresa en apoyo de los objetivos generales y requisitos de las partes interesadas y así, efectivamente, soportar la alineación entre las necesidades de la empresa y las soluciones y servicios de TI.

Ilustración 12 *Visión de la Cascada de metas de COBIT 5*

Fuente COBIT® Figura 4 . © 2012 ISACA

Se presenta en la ilustración 13 los objetivos del gobierno en relación con las metas corporativas financieras.

Ilustración 13 *Metas corporativas del COBIT 5 con relación a los objetivos de gobierno*

Dimensiones de CM	Meta Corporativa	Relaciòn con los Objetivos de Gobierno		
		Realizaciòn de Beneficios	Optimizaciòn de Riesgos	Optimizaciòn de Recursos
Financiera	1. Valor para las Partes interesadas de las Inversiones de Negocio	P		S
	2. Cartera de productos y servicios competitivos	P	P	S
	3. Riesgos de negocio gestionados (Salvaguarda de activos)		P	S
	4. Cumplimiento de leyes regulaciones externas		P	
	5. Transparencia Financiera	P	S	S

Fuente COBIT® Figura 5 . © 2012 ISACA

Para un mejor entendimiento de la ilustración es factible mencionar que las metas han sido analizadas por COBIT determinando la P(prioritaria) y S (secundaria) por ende podemos identificar que una mayor cantidad de metas corporativas son sensibles a una optimización de los riesgo.

Las dimensiones de metas de información y tecnología en correlación con las metas de la gerencia financiera son las que se presentan en la ilustración 14

Ilustración 14 *Metas Relacionadas con el TI COBIT 5*

Dimensiòn del CMI TI	Meta de Informaciòn y Tecnologìa Relacionada	
Financiera	01	Alineamiento de Ti y estrategia de negocio
	02	Cumplimiento y soporte de la Ti al cumplimiento del negocio de las leyes y regulaciones externas
	03	Compromiso de la direcciòn ejecutiva para tomar decisiones relacionadas con Ti
	04	Riesgos de negocio relacionados con las Ti gestionados
	05	Realizaciòn de beneficios del portafolio de inversiones y servicios relacionados con las Ti
	06	Transparencia de los costos, beneficios y riesgos de la Ti

Fuente COBIT® Figura 6. © 2012 ISACA

Para una mejor comprensión se emítela relación que poseen entre metas corporativas y metas de Ti.

Ilustración 15 *Conexión metas corporativas y relación de metas con TI*

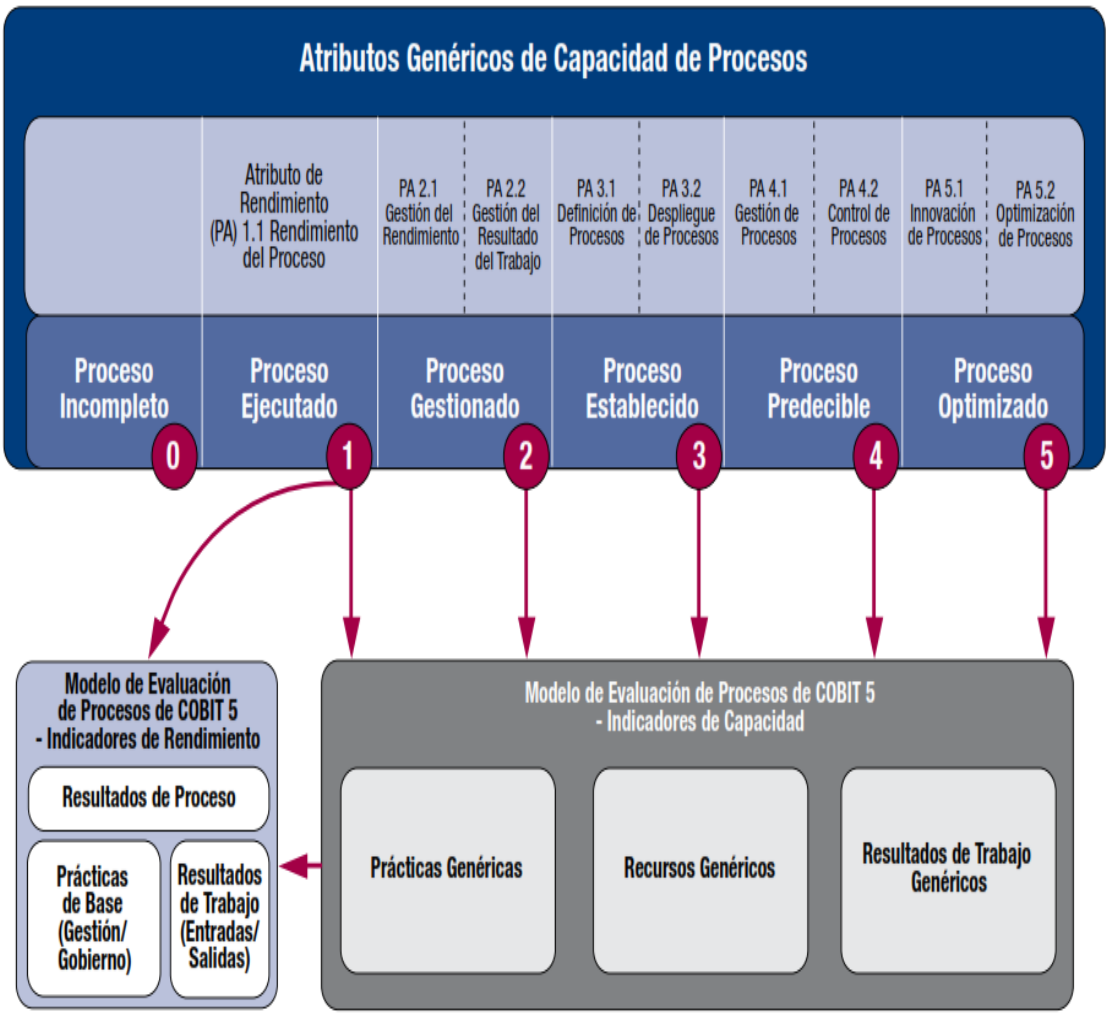
		Valor para las partes interesadas de las inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activo)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera
Meta relacionada con las Ti		**1**	**2**	**3**	**4**	**5**
		Financiera				
Financiera	Alineamiento de Ti y estrategia de negocio	P	P	S		
	Cumplimiento y soporte de Ti al cumplimiento del negocio de las leyes y regulaciones externas			S	P	
	Compromiso de la direccion ejecutiva para tomar decisiones relacionas con Ti	P	S	S		
	Riesgo de negocio relacionados con Ti gestionados		p	S		
	Realizacion de beneficios del portafolio de inversiones y servicios relacionados con las Ti	P	P			
	Trasparencia de los costos, beneficios y riesgos de Ti	S		S		P

Fuente COBIT® Figura 22. © 2012 ISACA

Modelo de Capacidad de los procesos

Según (ISACA, 2012, pág. 41) el modelo alcanzará los mismos objetivos generales de evaluación de procesos y apoyo a la mejora de procesos, es decir, que proporcionará un medio para medir el desempeño de cualquiera de los procesos de gobierno o de gestión y permitirá identificar áreas de mejora.

Ilustración 16 *Resumen de Modelo de Capacidad de procesos de COBIT 5*



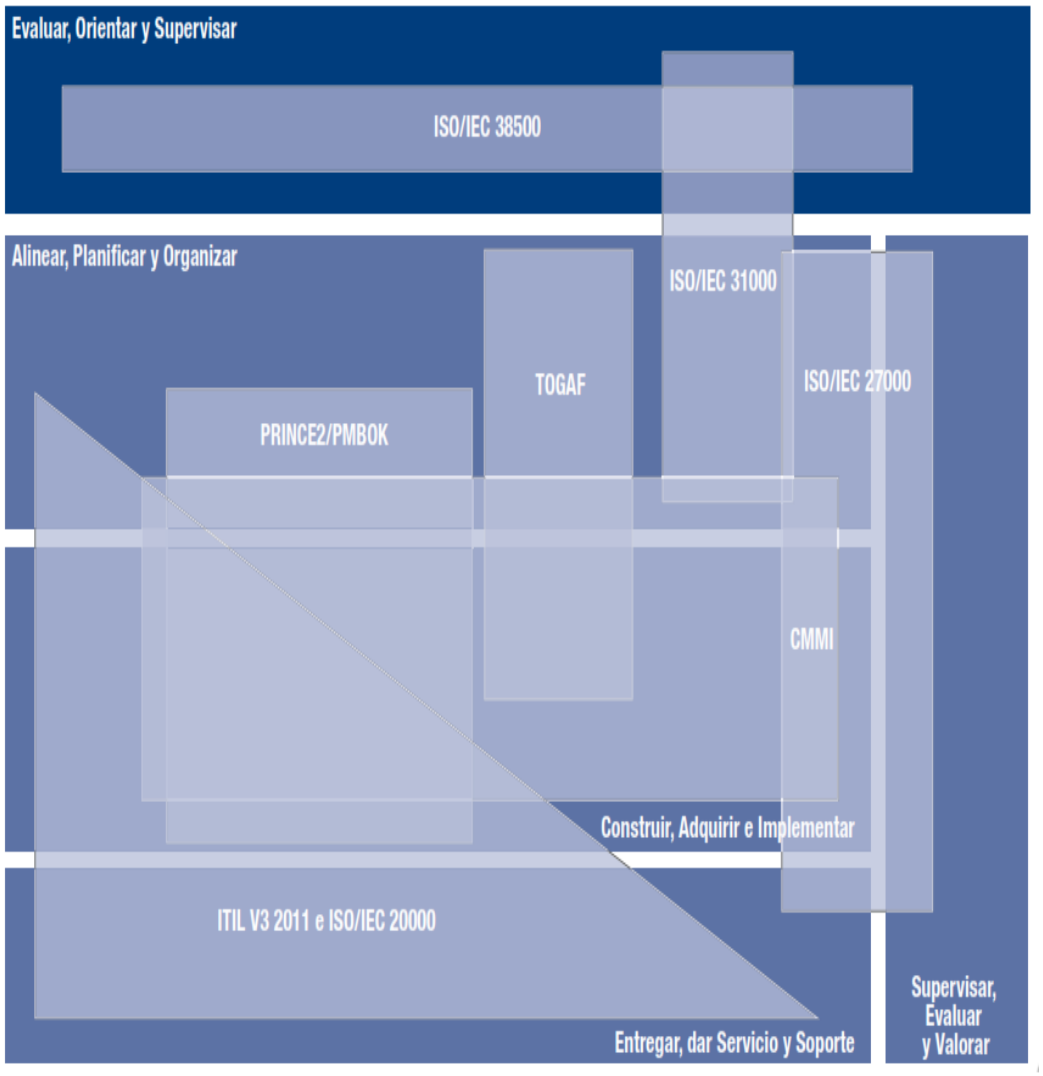
Fuente COBIT® Figura 19. © 2012 ISACA

Integración de Normas COBIT 5 e ISO 27000

COBIT 5 es un marco integrador de normas comúnmente aceptados por las organizaciones, para logar la integración de las necesidades a nivel corporativo o de gobierno con las necesidades relacionadas con TI.

En la ilustración siguiente se representa la relativa coincidencia entre COBIT 5 y los estándares y marcos de referencias.

Ilustración 17 *Integración del COBIT 5 con otros Estándares y Marcos de Trabajo*



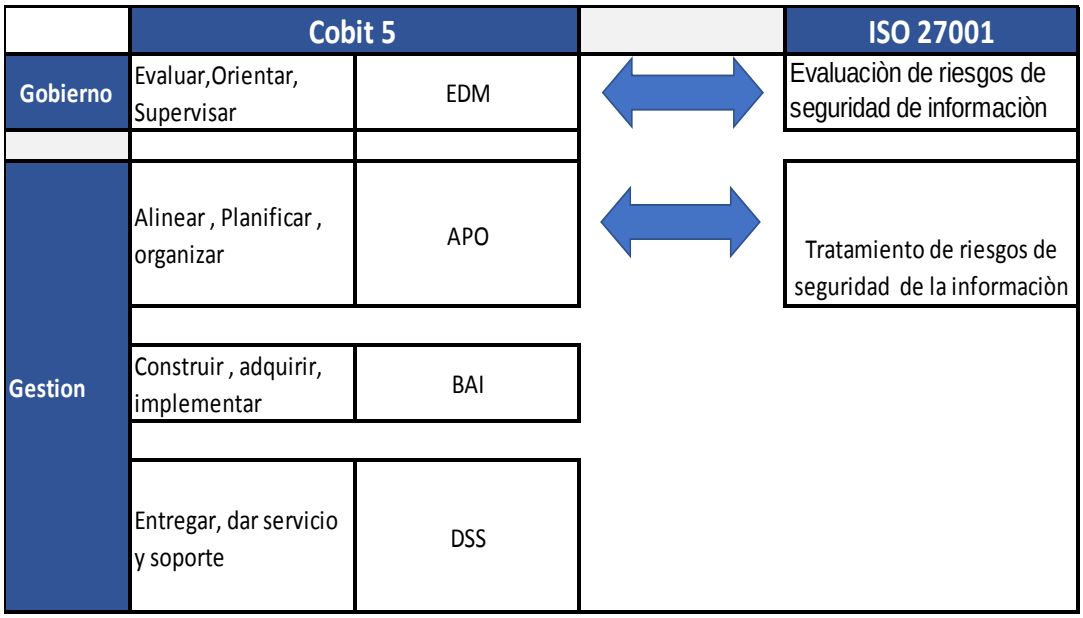
Fuente COBIT® Figura 25. © 2012 ISACA

Podemos identificar que en la ilustración 18 se presenta los procesos que según la norma COBIT se poseen de riesgos basado en los 5 dominios del COBIT 5 y que se encuentran relacionas con la ISO27001 que hace guardar relación con la gestión corporativa.

- Evaluar, orientar supervisar (EDM) (ISACA, 2012)
- Alinear, planificar y organizar (APO) (ISACA, 2012)

COBIT 5 incluye objetivos de riesgos, pero podemos integrarla con la ISO 270001 para gestionar de una forma efectiva y eficiente los riesgos de TI.

Ilustración 18 *Acoplamiento de COBIT e ISO 27001*



Fuente Elaboración de las autoras

Área Financiera en la Empresa

La gestión financiera es el proceso de análisis y toma de decisiones sobre las insuficiencias financieras de una organización, tratando de utilizar los recursos financieros, asegurando que sean suficientes contribuyendo de esta manera al cumplimiento de los objetivos propuestos.

Una buena organización financiera es la base para que nuestro negocio tenga beneficios. Si queremos que nuestra empresa crezca es imprescindible conocer todas las posibilidades que nos ofrece. A continuación, realizaremos un breve análisis para saber en qué consiste el departamento financiero. (Ramos, 2017)

La gestión financiera es la destinación apropiada del capital de trabajo dentro de un equilibrio de los criterios de riesgo y rentabilidad, gracias a sus aportes, a la minimización de costos, al empleo efectivo de los recursos colocados a la disposición de la gerencia y la generación de fondos para el desempeño empresarial. La gestión financiera es la que se encarga de convertir a la visión y misión en operaciones monetarias (ORTIZ, 2005)

Planificación Financiera

Gitman (2007) expone que la planificación financiera es una parte importante en las operaciones de la organización, debido a que proporciona esquemas para guiar, coordinar y controlar las actividades de esta con el fin de lograr sus objetivos. Además, señala que el proceso de planificación financiera comienza con planes financieros a largo plazo, o estratégicos, que a su vez conducen a la formulación de planes y presupuestos a corto plazo u operativos. (Giltman, 2007)

La planificación financiera se piensa en todas las actividades que pueden realizarse en el futuro, se integran las políticas y decisiones que los directivos pueden adoptar ante determinadas situaciones, se fijan estándares en cuanto a la actuación futura, se concretan las actividades, se compromete al personal con las ventas. El presupuesto es una herramienta de planificación financiera, en él se determina si los recursos están disponibles para ejecutar las actividades. (Burbano)

Se establece en si, que la planificación financiera plantea la manera en la cual se van a alcanzar metas financieras. Por ende, un plan financiero son las acciones que se realizaran en un futuro. La mayoría de las decisiones tienen tiempos de ejecución largos, lo que significa que la implementación debe lleva mucho tiempo.

Organización Financiera

De según Chávez (2003) la organización financiera plantea un análisis de la parte operacional de las finanzas, al considerar los fines que persiguen las cifras; al encasillar en fondo de una forma adecuada, instrumentamos la plataforma que guía la actividad financiera. Al hablar de organización financiera se hace referencia a la formación de los departamentos o unidades (departamentalización), la asignación de autoridad y responsabilidad (línea de autoridad) las características que conforman el personal de la organización (cultura organizacional) y el objetivo que se persigue al diseñar la estructura (propósito de la organiza. (Chavez, 2003)

La organización financiera como la asignación eficaz de los recursos humanos, económicos y financieros para el logro pleno de los propósitos

empresariales. Para asignar la elaboración del presupuesto en el tiempo establecido y garantizar la participación de los diferentes niveles organizacionales, deben definirse las actividades para asignar a los participantes, así como precisar normas aplicables al flujo de información, secuencia a seguir y coordinación. (Burbano)

Responsabilidades del área

Gestión de los costes

Una vez que tenemos definidos y controlados los costes, hay que gestionarlos. Para ello se suelen emplear los ingresos y los costes diferenciales a través del margen de contribución para tomar decisiones relacionadas con seguir fabricando un producto, cerrar una fábrica, etc. (Fajardo, 2010)

Presupuestos

Otra de las funciones relevantes es la de elaborar el presupuesto. En primer lugar, debe decidir si el presupuesto va a ser base cero o no.

Una vez decidido, este departamento controlará los presupuestos de ventas, de producción, de compras, de mano de obra directa, de gastos de estructura, etc. Con esto ya se pueden reelaborar los presupuestos de tesorería, la cuenta de resultados y el balance, comprobar desviaciones para sus posibles correcciones. (Fajardo, 2010)

CAPITULO II

METODOLOGIA

Metodología

Actualmente la tecnología en las empresas constituye un recurso clave para resguardar la información que se genera logrando constituirse en un proceso integrador ente la organización y las TI.

Las metodologías para la seguridad de sistemas buscan establecer y mejorar para el reconocimiento de las amenazas sean visibles y se materialicen en hechos que se logren reducir de una forma razonable beneficiando a la empresa.

En este capítulo se expone los aspectos metodológicos de la investigación seleccionada, se llevará a cabo el estudio y se definirá el enfoque y el diseño de este proceso de investigación, considerando las características que posee nuestro proyecto de estudio de manera ordenada y eficaz para alcanzar a definir el objetivo de la investigación planteada.

Diseño de la investigación

En el presente proyecto desarrollado a BanEcuador, utilizaremos el diseño no experimental ya que se busca analizar en el ambiente natural el fenómeno a investigar y no se busca cambiar ni manipular la información, para poder definir riesgos que se puedan estar suscitando en la empresa y poder emitir recomendaciones para minimizar los riesgos o desaparecerlos.

El diseño no experimental, el cual tiene como propósito, realizar una observación del evento tal cual como ocurre, para en lo posterior, efectuar un análisis de este, de acuerdo con (Hernandez, Fernanfez, & Baptista, 2004)

Cuando el investigador se limita a observar los acontecimientos sin intervenir en los mismos entonces se desarrolla una investigación no experimental (Grajales, 2000)

En este tipo de diseños no experimentales, nos indica que la información obtenida es de primera mano, por consiguiente, mediante la técnica cualitativa de la observación evidenciaremos las situaciones posibles

de debilidades en su sistema Core Bancario Cobis para posteriormente analizarlo.

En la presente investigación, la información reunida pertenece a un solo fenómeno de estudio que se desarrollará en BanEcuador B.P en un solo período en el año.

En base a las mejores prácticas, en cuanto a gestión tecnológica, los procesos, así como su definición, administración y ejecución, forman parte de un conjunto de fortalezas que permiten que una empresa se desarrolle y evolucione, proporcionalmente, conforme su estado de madurez, dinamismo y adaptabilidad se encuentren mejor enriquecidos, desarrollados e implementados.

En cuanto a la infraestructura tecnológica que administra y mantiene. La Gestión de tecnología de la información de BanEcuador B.P , cuenta con varios procesos tecnológicos ejecutados por la dirección y las cuatro áreas que la conforman, gestión de desarrollo y mantenimiento de aplicaciones, gestión de gestión y control, gestión de producción y operaciones, gestión de infraestructura tecnología.

Tipo de investigación

Para esta investigación, se utilizó como tipo de investigación, el estudio de caso el cual nos permitirá identificar como se está desarrollando en la empresa el manejo de los riesgos presentados en sus sistemas y como esto afecta en la toma de decisiones enfocados en un área de estudio como es la Gerencia Financiera.

> Robert K.Yin, uno de los autores tomados como referencia principal en la utilización del Método de Estudio de Casos, indica que este método es empleado para el estudio de un fenómeno en su entorno natural, se analiza e interpreta un caso en particular, con la finalidad de obtener un conocimiento profundo del mismo.
>
> (Bernal , 2010) señala que el Estudio de Casos se centra en describir y explicar el fenómeno estudiado y considera a esta metodología como un tipo de investigación que puede ser empleada con buenos resultados en diferentes ramas de estudio.

En el diseño de este estudio de caso realizaremos un levantamiento de información donde se conocerá como inicio la empresa, su organigrama, la Gerencia Financiera, Gerencia de Tecnología, Sistema Core Bancario.

Para el desarrollo de la recolección de información realizaremos entrevista estructurados puntuales para determinar cuáles son los procesos críticos de la Gerencia Financiera, se determinarán en conjunto con el gerente amenazas riesgos presentados en relación de las TI.

Se realiza una relación de las metas como lo presenta el marco integrador del COBIT entre Gerencia Financiera y TI . Posterior se determinarán por separado los procesos que se consideran críticos de cada área regidos por los 37 procesos presentados en el marco COBIT.

Una vez identificados los procesos se les medirá su nivel de madurez para que en el momento de analizar los riesgos a los que están los procesos críticos encontrados en el área guardar la relación de importancia entre los procesos financiera como las Ti para la toma de decisiones.

Enfoque de investigación

Para este proyecto de investigación se ha definido el método de investigación cualitativa debido a que se estudia la realidad en su contexto natural.

Este enfoque ha sido también referido como investigación naturalista e interpretativa, en el cual incluye una variedad de concepciones, visiones, técnicas y estudios no cuantitativos, existen diversos marcos interpretativos, como el interaccionismo, el constructivismo, la psicología, la teoría crítica, etc. (Grinnell Jr., 2005, pág. 45)

Entre las características de este enfoque cualitativo se menciona en el libro Metodología de la Investigación que se pueden desarrollar preguntas e hipótesis antes, durante y después que se recolectan y analizan datos. (Hernandez, Fernanfez, & Baptista, 2004)

Método de investigación cualitativa

Los Métodos y técnicas en la investigación cualitativa son diversos y cuentan con varios procedimientos para la obtención de información, la misma

que será utilizada para en lo posterior emitir criterios, interpretar datos, explicar, dar una conclusión y recomendación final. (MUNARRIZ)

Los estudios cualitativos pueden desarrollar preguntas e hipótesis antes, durante o después de la recolección y el análisis de los datos. Con frecuencia, estas actividades sirven, primero, para descubrir cuáles son las preguntas de investigación más importantes, y después, para refinarlas y responderlas. La acción indagatoria se mueve de manera dinámica en ambos sentidos: entre los hechos y su interpretación, y resulta un proceso más bien "circular" y no siempre la secuencia es la misma, varía de acuerdo con cada estudio en particular. (Hernandez, Fernanfez, & Baptista, 2004)

En el caso del proceso cualitativo, la muestra, la recolección y el análisis son fases que se realizan prácticamente de manera simultánea.

Características adicionales del enfoque cualitativo

- El investigador o investigadora plantea un problema, pero no sigue un proceso claramente definido. Sus planteamientos no son tan específicos como en el enfoque cuantitativo y las preguntas de investigación no siempre se han conceptualizado ni definido por completo.
- Bajo la búsqueda cualitativa, en lugar de iniciar con una teoría particular y luego "voltear" al mundo empírico para confirmar si ésta es apoyada por los hechos, el investigador comienza examinando el mundo social y en este proceso desarrolla una teoría coherente con los datos, de acuerdo con lo que observa, frecuentemente denominada teoría fundamentada (Esterberg, 2002), con la cual observa qué ocurre. Dicho de otra forma, las investigaciones cualitativas se basan más en una lógica y proceso inductivo (explorar y describir, y luego generar perspectivas teóricas). Van de lo particular a lo general. Es decir, procede caso por caso, dato por dato, hasta llegar a una perspectiva más general.

- En la mayoría de los estudios cualitativos no se prueban hipótesis, éstas se generan durante el proceso y van refinándose conforme se recaban más datos o son un resultado del estudio.
- El enfoque se basa en métodos de recolección de datos no estandarizados ni completamente predeterminados. No se efectúa una medición numérica, por lo cual el análisis no es estadístico. La recolección de los datos consiste en obtener las perspectivas y puntos de vista de los participantes (sus emociones, prioridades, experiencias, significados y otros aspectos subjetivos). También resultan de interés las interacciones entre individuos, grupos y colectividades. El investigador pregunta cuestiones abiertas, recaba datos expresados a través del lenguaje escrito, verbal y no verbal, así como visual, los cuales describe y analiza y los convierte en temas que vincula, y reconoce sus tendencias personales (Todd, 2005).
- Por lo expresado en los párrafos anteriores, el investigador cualitativo utiliza técnicas para recolectar datos, como la observación no estructurada, entrevistas abiertas, revisión de documentos, discusión en grupo, evaluación de experiencias personales, registro de historias de vida, e interacción e introspección con grupos o comunidades.
- El proceso de indagación es más flexible y se mueve entre las respuestas y el desarrollo de la teoría. Su propósito consiste en “reconstruir” la realidad, tal como la observan los actores de un sistema social previamente definido. A menudo se llama holístico, porque se precia de considerar el “todo” sin reducirlo al estudio de sus partes.
- El enfoque cualitativo evalúa el desarrollo natural de los sucesos, es decir, no hay manipulación ni estimulación con respecto a la realidad (Corbetta, 2003).

- La investigación cualitativa se fundamenta en una perspectiva interpretativa centrada en el entendimiento del significado de las acciones de seres vivos, sobre todo de los humanos y sus instituciones (busca interpretar lo que va captando activamente).
- Postula que la “realidad” se define a través de las interpretaciones de los participantes en la investigación respecto de sus propias realidades. De este modo convergen varias “realidades”, por lo menos la de los participantes, la del investigador y la que se produce mediante la interacción de todos los actores. Además, son realidades que van modificándose conforme transcurre el estudio y son las fuentes de datos.
- Por lo anterior, el investigador se introduce en las experiencias de los participantes y construye el conocimiento, siempre consciente de que es parte del fenómeno estudiado.
- Las indagaciones cualitativas no pretenden generalizar de manera probabilística los resultados a poblaciones más amplias ni necesariamente obtener muestras representativas; incluso, regularmente no buscan que sus estudios lleguen a replicarse.
- El enfoque cualitativo puede concebirse como un conjunto de prácticas interpretativas que hacen al mundo “visible”, lo transforman y convierten en una serie de representaciones en forma de observaciones, anotaciones, grabaciones y documentos. Es naturalista e interpretativo (Hernandez, Fernanfez, & Baptista, 2004, págs. 9-10)

Diferencias entre Enfoque Cuantitativo y Cualitativo

Tabla 1 *Diferencia entre enfoque Cuantitativo y Cualitativo Parte 1*

Definición	Enfoque Cuantitativo	Enfoque Cualitativo
Punto de partida	Hay una realidad que conoce.	Hay una realidad que descubrir, construir e interpretar.
Realidad a estudiar	Existe una realidad objetiva única. El mundo es concebido como externo al investigador.	Existen varias realidades subjetivas construidas en la investigación, las cuales varían en su forma y contenido entre individuos, grupos y culturas. En mundo es construido por el investigador
Naturaleza de la realidad	La realidad no cambia por las observaciones y mediciones realizadas.	La realidad si cambia por las observaciones y la recolección de datos
Objetividad	Busca ser objetivo.	Admite subjetividad.
Metas de la investigación	Describir, explicar y predecir los fenómenos (causalidad). Generar y probar teorías.	Describir, comprender e interpretar los fenómenos, a través de las percepciones y significados producidos por las experiencias de los participantes.
Lógica	Se aplica la lógica deductiva. De lo general a lo particular.	Se aplica la lógica inductiva. De lo particular a lo general.

Tabla 2 *Diferencia entre enfoque Cuantitativo y Cualitativo Parte 2*

Definición	**Enfoque Cuantitativo**	**Enfoque Cualitativo**
Posición personal del investigador	Neutral. El investigador "hace a un lado sus propios valores y creencias. La posición de investigador es "imparcial" intenta asegurar procedimientos rigurosos y "objetivos" de recolección y análisis de los datos.	Explicita. El investigador reconoce sus propios valores y creencias, incluso son parte del estudio.
Planteamiento del problema	Delimitado, acotado especifico. Poco flexible	Abierto, libre, no es delimitado o acotado. Muy flexible.
Población-muestra	El objetivo es generalizar los datos de una muestra a una población (de un grupo pequeño a uno mayor).	Regularmente no se pretende generalizar los resultados obtenidos en la muestra a una población.
Muestra	Se involucra a muchos sujetos en la investigación porque se pretende generalizar los resultados.	Se involucra a unos cuantos sujetos porque no se pretende generalizar los resultados del estudio.
Naturaleza de los datos	Datos numéricos.	Textos, narraciones, significados, etcétera.

Tabla 3 *Diferencia entre enfoque Cuantitativo y Cualitativo Parte 3*

Definición	Enfoque Cuantitativo	Enfoque Cualitativo
Tipo de datos	Datos confiables y duros.	Datos profundos y enriquecedores.
Recolección de datos	Se basa en instrumentos estandarizados.	Está orientada a proveer de mayor entendimiento de los significados y experiencias de las personas.
Finalidad del análisis de los datos	Describir las variables y explicar sus cambios y movimientos	Comprender a las personas y sus contextos.
Reporte de resultados	Utilizan un tono objetivo impersonal, no emotivo.	Utilizan un tono personal y emotivo

Fuente: *Metodología de la investigación 5ta Edición. Hernández, Fernández & Baptista. Tabla 1.1*

Una vez definido diseño, tipo y enfoque de la investigación, podemos identificar que el método de estudio de caso es el más idóneo para este tipo de proyecto, ya que permite obtener una comprensión e interpretación profunda de los acontecimientos ocurridos dentro de BanEcuador.

Método de Estudio de caso

(Bernal , 2010), señala que el Estudio de Casos se centra en describir y explicar el fenómeno estudiado y considera a esta metodología como un tipo de investigación que puede ser empleada con buenos resultados en diferentes ramas de estudio.

En la siguiente table se presenta la clasificación de estudio de caso.

Tabla 4 *Clasificación de Estudio de Caso*

Concepto	Clasificación
Según el objetivo de la estrategia	Descriptivos Exploratorios Ilustrativos Explicativos
Con respecto al número de casos que conforman un estudio	Un caso único Múltiples o comparativos

Fuente: Robert K. Yin, 1994

Características y ventajas de estudio de caso

Se define 4 características que posee el Método de Estudio de Casos que son consideradas las principales.

Tabla 5 *Características y ventajas de estudio de caso*

Características	Descripción
Particularista	Se basa en la comprensión del caso como característica útil para descubrir y analizar situaciones únicas.
Descriptivo	Se consideran variables para la descripción de una situación o fenómeno.
Heurístico	Su finalidad es la de aclarar o confirmas algo que ya es conocido. Se considera para la toma de decisiones y propuestas iniciales de acción.
Inductivo	Se obtiene conclusiones generales a partir de premisas que contiene establecer una hipótesis

Fuente: Pérez Serrano, 1994

En la tabla 5 se presentan las características que posee esta metodología según la autora Pérez Serrano, permiten obtener un conocimiento más claro de la misma.

Las características particularistas y descriptivas son las más idóneas para el estudio de este proyecto, ya que, mediante la comprensión de un caso en particular, descubriremos y analizaremos hechos o eventos ocurridos en el BanEcuador, para posteriormente proceder a la descripción de las situaciones más relevantes que se identifiquen.

Alcance de la investigación

De acuerdo a (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 1997, pág. 69) afirman que existen 4 tipos de investigaciones que son la "*Exploratoria, descriptiva, correlacional o explicativa"*

Mediante el análisis previo hemos seleccionado el tipo de investigación descriptiva, "El propósito del investigador es describir situaciones y eventos. Una investigación descriptiva busca especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis". de acuerdo con (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 1997, pág. 71)

Una vez efectuada la descripción de los procesos de la Gerencia Financiera procederemos a conocer los principales procesos que definen como críticos según la perspectiva del área.

También hemos identificado que será necesario aplicar el tipo de investigación explicativa, (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 1997) menciona que en este tipo de investigación se procede a explicar de manera detallada los eventos tal cual como se observan y ocurren.

Nuestro trabajo de investigación se usara el tipo de estudio descriptivo con lo cual podremos tener de primera mano un análisis de cómo se están manifestando el fenómeno a tratar y las características que presenta en la empresa BanEcuador B.P a su Sistema Core Bancario Cobis en los procesos que se seleccionaran de la Gerencia Financiera con el cual podremos conocer sobre sus seguridades , características propias de este sistema , al conocer

esta parte del fenómeno se procederá a realizar un análisis explicativo determinando los amenazas y lo que esta ocasional al buen desempeño de la empresa.

Utilizar este tipo de metodología en nuestro proyecto, permitirá que obtengamos evidencia de la realidad de la empresa, utilizando las diferentes herramientas cualitativas, tales como entrevistas, observación y análisis de riesgos, con la finalidad de dar respuesta a posibles eventualidades que se presenten.

Población y muestra

El muestreo es el procedimiento por el cual, de un conjunto de unidades que formar el objeto de estudio (La población), se elige un número reducido de unidades (muestra) aplicando unos criterios tales que permitan generalizar los resultados obtenidos del estudio de la muestra a toda la población. (Corbetta, 2007, pág. 272)

En esta investigación la población es todas las áreas que comprenden la Gerencia Financiera de BanEcuador B.P la misma que está conformada por Subgerencia de Tesorería, Subgerencia de Contabilidad, Subgerencia de Control Financiero y por ende a cada uno de los analistas que integran la Gerencia en conjunto con la Gerencia de Tecnología de la Información y sus Subgerencias.

La muestra que se utilizará al gerente financiero, subgerentes del área y a cuatro analistas al azar de esta para en análisis poder determinar los procesos críticos de la gerencia Financiera.

Técnicas de recolección de información

Para el desarrollo de este proyecto de estudio utilizaremos las siguientes técnicas de recolección de información.

Dankhe (1986) define dos tipos de fuentes de información:

- ✓ Primarias
- ✓ Secundarias

Las fuentes primarias son aquellas obtenidas a través de la revisión, información de primera mano.

Se ha determinado que en este proyecto de investigación la técnica cualitativa a utilizar será la recolección de información primaria mediante entrevistas cualitativas, debido a que permite realizar un intercambio de información valiosa, entre el entrevistador y entrevistado.

Para lo cual se desarrollan preguntas puntuales dirigidas en primera instancia al Gerente Financiero como cabeza principal y como conocedor del desarrollo de todo el proceso de su área y posteriormente a los subgerentes que integran el área y a cuatro analistas claves del área a analizar.

Las fuentes secundarias consisten en una recopilación de información bajo los parámetros de COBIT 5 de los procesos críticos.

Por consiguiente, emplearemos información proporcionada en las entrevistas y documentación entregada por el BanEcuador B.P para el estudio de proyecto, acerca de los procesos de control (si los hubiere) del área Financiera que es la analizar.

Entrevista Cualitativa

Es empleada para obtener la información, a través, de una comunicación directa, íntima y abierta que mantiene el investigador con el entrevistado.

La recolección de información tiene como objetivo entender y analizar un fenómeno, evento o problema con la finalidad de responder a las preguntas del problema de investigación y proveer en lo posterior conocimiento a través del entendimiento del origen de dichas situaciones. (Hernandez, Fernanfez, & Baptista, 2004)

Taylor y Bogdan (1987) consideran que en las investigaciones donde la entrevista es utilizada como la principal técnica para la obtención de la información, será necesaria una entrevista a profundidad efectuando reuniones frecuentes con los investigados, en este con las autoridades de las áreas en análisis de BanEcuador B.P.

Para el desarrollo de este proyecto la entrevista cualitativa se basará en un conversatorio entre el entrevistado y el entrevistador con el objetivo de entender, por medio de palabras sencillas del sujeto entrevistado, situaciones o problemas de un caso en particular.

Etapas de entrevista cualitativa

- Búsqueda de información general, cuyo análisis de datos nos irá centrando los campos a explorar. Es decir, antes de comenzar la observación. Es el caso de la entrevista abierta, semejante a una conversación cara a cara con los informantes seleccionados, donde se requiere información general sobre el tema de estudio.
- Indagación de datos que nos ayuden a comprender situaciones producidas durante la observación. Se trata de la entrevista semi-estructurada, donde se recoge información a partir de las preguntas planteadas en el análisis de los datos, de las notas de campos, documentos, etc.
- Recabar información, quizá más comprometida, que pudiera crear algún conflicto si se realizara en el proceso de observación. En esta situación se plantean las contradicciones aparecidas en los datos. Se corresponde con la entrevista semiestructurada. (MUNARRIZ)

Características principales de la entrevista cualitativas

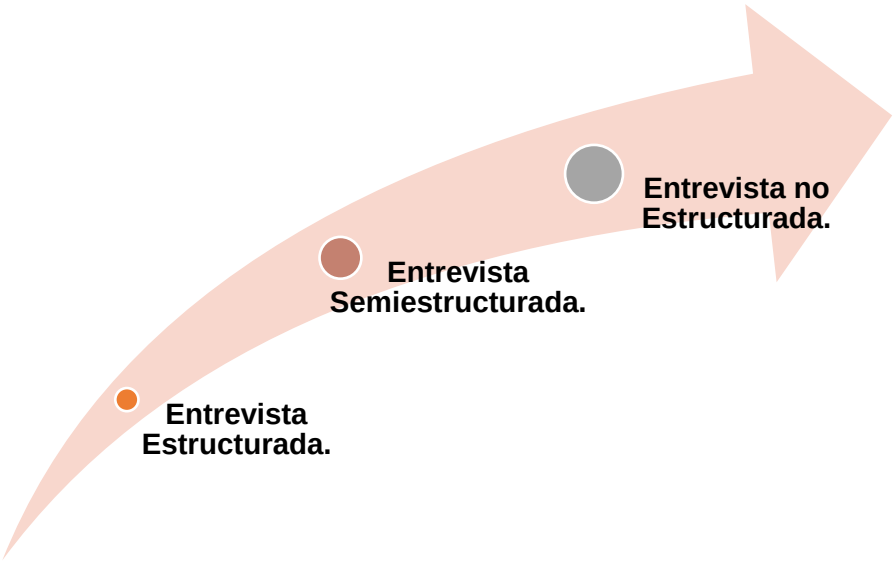
- Las entrevistas son efectuadas en diferentes fases o etapas dependiendo de la necesidad del investigador.
- El guion de preguntas para realizar la entrevista es adaptado al sujeto entrevistado.
- Los datos recolectados a través de la entrevista cualitativa son tomados de la realidad, experiencia y opinión expresada por los entrevistados.
- Tanto el entrevistador como el entrevistado intervienen en la coordinación y manejo de la conversación.

Tipos de entrevistas cualitativas

(Corbetta, 2007) señala que la clasificación de la entrevista depende de la recolección de información que se espera realizar, es decir, si no se desea profundizar sobre un tema se debe efectuar un cuestionario con preguntas de tipo cerrada; por otro lado, si se desea conocer profundamente sobre una situación o hecho especifico, lo más apropiado es efectuar una entrevista cualitativa, la misma que permite al entrevistado explicar con

libertad su percepción sobre las cosas ya que la entrevista es una conversación abierta y flexible.

Ilustración 19 *Tipos de Entrevistas Cualitativas*



Fuente: Metodología y Técnica de Investigación (Corbetta, 2007).

- **Entrevista Estructurada**: el entrevistador mantiene un guion de preguntas, las mismas que serán abordadas de una manera secuencial a cada uno de los entrevistados, con la finalidad de obtener información acerca de algún hecho en particular. En la mayoría de las ocasiones las posibles respuestas a estas preguntas planificadas serán de tipo cerrado; es decir, podrán ser afirmativas, negativas o de una respuesta muy concreta y exacta. (Corbetta, 2007)
- **Entrevista Semiestructurada:** se llevan a cabo a través de un guion de preguntas que pueden ser sujetas a cambio en el transcurso de la conversación con el entrevistado, con la finalidad de abordar el tema o temas que se consideren importantes.

Para este tipo de entrevistas, las posibles respuestas son de carácter abierto; por esta razón el entrevistador puede plantear las preguntas como él considere oportuno y en los términos en que le parezca conveniente para recabar todo tipo de información valiosa, garantizando de esta manera una

libertad tanto para el entrevistado como el entrevistador de poder abordar los temas principales y de relevancia que consideren. (Corbetta, 2007)

Entrevista no estructurada: Como hemos mencionado tanto para las entrevistas estructuradas o semiestructuradas el entrevistador prepara de antemano preguntas o temas que serán abordados durante el tiempo de la entrevista.

Por otro lado las entrevistas no estructuradas no mantienen un guion o planeación sobre preguntas o temas específicos a tratar, más bien el entrevistador planteará los temas que necesita conocer durante el lapso que dure la plática con el entrevistado, dejando que éste se sienta cómodo tomando siempre la iniciativa durante la entrevista e intervendrá únicamente cuando algún tema en particular desee que se profundice. (Corbetta, 2007)

Para nuestro proyecto se utilizará las entrevistas estructuradas para conocer con peguntas puntuales las necesidades de la Gerencia Financiera.

Observación de campo

Este tipo de investigación es también conocida como investigación in situ ya que se realiza en el propio sitio donde se encuentra el objeto de estudio. Ello permite el conocimiento más a fondo del investigador, puede manejar los datos con más seguridad y podrá soportarse en diseños exploratorios, descriptivos y experimentales, creando una situación de control en la cual manipula sobre una o más variables dependientes (efectos).

Encuesta

La encuesta es un instrumento de la investigación de mercados que consiste en obtener información de las personas encuestadas mediante el uso de cuestionarios diseñados en forma previa para la obtención de información específica. (Marta Alelú Hernández)

Es una técnica de investigación que consiste en una interrogación verbal o escrita que se le realiza a las personas con el fin de obtener determinada información necesaria para una investigación. (Marta Alelú Hernández)Cuando la encuesta es verbal se suele hacer uso del método de la entrevista; y cuando la encuesta es escrita se suele hacer uso del instrumento del cuestionario, el cual consiste en un documento con un listado

de preguntas, las cuales se les hacen a las personas a encuestar. (Marta Alelú Hernández)

Características principales de las encuestas

- Las encuestas son una de las escasas técnicas de que se dispone para el estudio de las actitudes, valores, creencias y motivos. (Marta Alelú Hernández)
- Las técnicas de encuesta se adaptan a todo tipo de información y a cualquier población. (Marta Alelú Hernández)
- Las encuestas permiten recuperar información sobre sucesos acontecidos a los entrevistados. (Marta Alelú Hernández)
- Las encuestas permiten estandarizar los datos para un análisis posterior, obteniendo gran cantidad de datos a un precio bajo y en un período de tiempo corto. (Marta Alelú Hernández)

Análisis de Datos

Entrevista

Las entrevistas serán utilizadas para los gerentes subgerentes y los analistas en primera instancia para determinar los procesos críticos del área financiera en este análisis se usurarán entrevistas de tipo estructuradas. Y como valla surgiendo el desarrollo de la investigación serán entrevistas con el Gerente Financiero o Gerente de Ti que se llevaran a cabo con las matrices que se presentan en el COBIT para el levantamiento de información

Observación de Campo

Se realizarán las visitas ín situ para poder verificar el desenvolvimiento de las áreas en análisis y recolectar información relevante a la empresa y sus manuales de procesos.

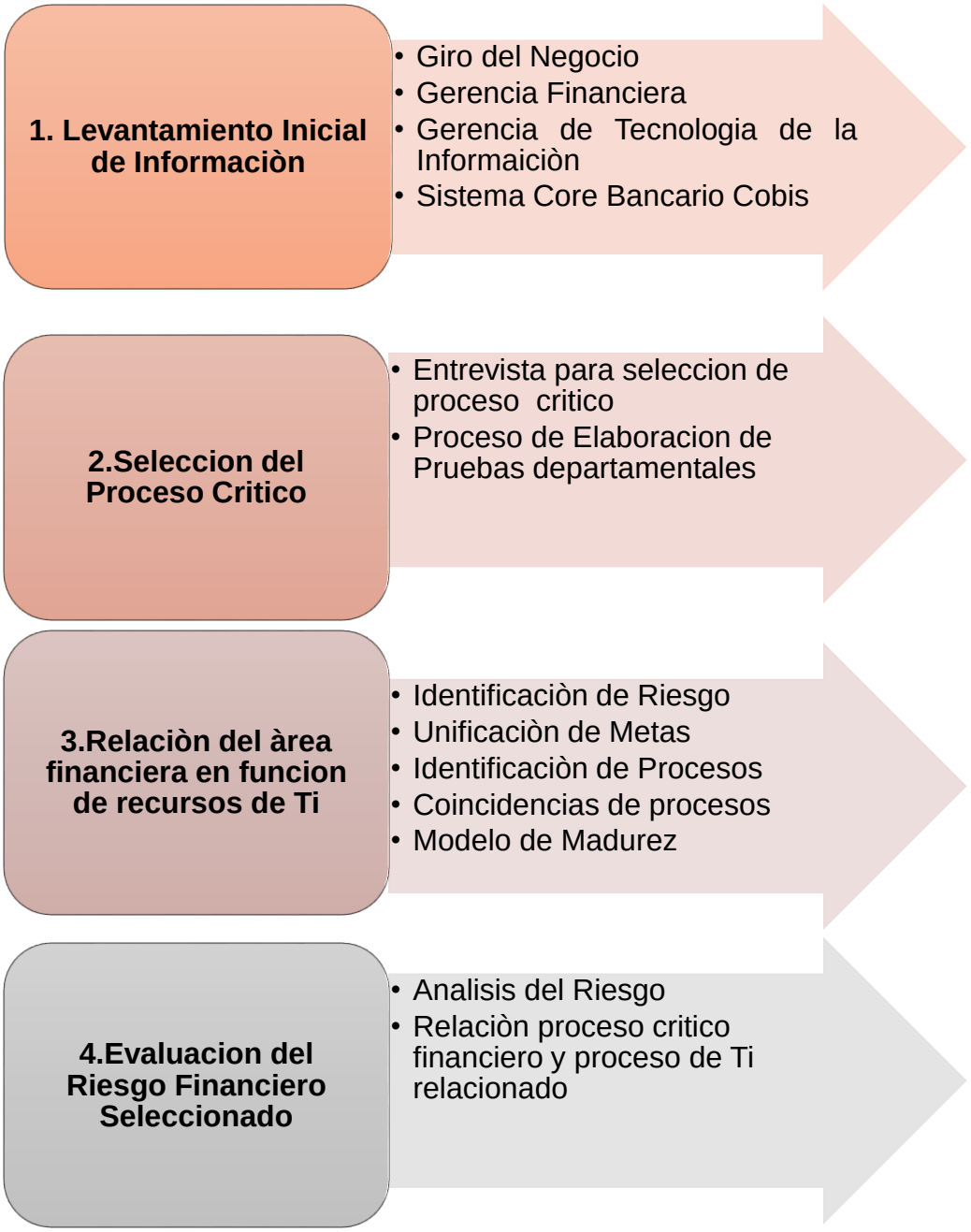
Encuestas

Se determinan según la etapa en que se vallan desarrollando el análisis del caso con estándares de copulación de información para medir metas análisis de procesos y evaluación de riesgo.

Una vez determinadas las principales características, ventajas del Método de Estudio de Casos y habiendo seleccionado y determinado la

técnica de entrevista cualitativa, para recolección de información, procederemos a realizar una estructura que utilizaremos para el estudio de este proyecto.

Ilustración 20 *Desarrollo de etapas de Estudio de caso en BanEcuador B.P*



Fuente: Elaboración de las autoras

Como se puede evidenciar en la ilustración 20 en nuestro proyecto de investigación se realizará entrevistas al Gerente Financiero, los subgerentes y analistas de área como expertos de las dificultades que se presentan para evaluarlas mediante el marco integrador de COBIT e ISO27001 con la finalidad de reconocer la relación que se pose entre la gerencia financiera que guardan relación con las Ti para dar una mayor importancia a la estrategia de esta en la empresa.

CAPITULO III

DESARROLLO

Podemos definir qué gestión de seguridad de información es el compendio de políticas, proceso, controles soportados en marcos de referencias y normativas comúnmente aceptadas.

Para desarrollar con mejor eficiencia la metodología de estudio que se busca aplicar en BanEcuador B.P es necesario conocer el entorno actual del mismo: organización, área financiera, área de TI y Sistema Core Bancario Cobis que se detallara a continuación.

Levantamiento Inicial de Información

Organización

La creación de BanEcuador B.P fue anunciada por el presidente de la República, economista Rafael Correa, el 9 de mayo de 2015, en el Enlace Ciudadano 423, en Iluman, cantón Otavalo. Lo presentó como un banco público, articulado a la institucionalidad y a los objetivos nacionales; con un enfoque inclusivo, créditos adaptados a las condiciones de los sectores productivos y, con horarios adecuados a las actividades de los productores, comerciantes y campesinos.

Cuatro días después, el 13 de mayo de 2015, con el Decreto Ejecutivo 677, BanEcuador B.P se incorpora a la vida económica del Ecuador. El 11 de marzo de 2016, el presidente Correa emite un nuevo Decreto Ejecutivo, que establecía la forma y plazo en que el BNF transferiría los activos, pasivos y patrimonio a BanEcuador. En cumplimiento de ese compromiso, el viernes 6 de mayo de 2016, el BNF hizo una pausa en su atención, y realizó los ajustes finales.

¡Así, el 9 de mayo de 2016, BanEcuador B.P , con su enfoque de desarrollo integral, abrió sus puertas al mundo! Se marca un hito en la Historia: la economía popular, rural y urbana, que produce, comercializa y presta servicios, es atendida por BanEcuador, que detecta sus prioridades en territorio, para interactuar con ellos, y articularse a políticas y programas

complementarios a los servicios financieros. Siempre con atención oportuna, sentido de compromiso y la calidez que merecen todos los ecuatorianos.

BanEcuador B.P está integrado por la matriz en Quito, 7 Coordinaciones zonales y 168 agencias a nivel nacional. **Ver Anexo 1**

Misión: Brindar productos y servicios financieros innovadores, eficaces y sostenibles social y financieramente, aportando en la inclusión y mejora de la calidad de vida de los pequeños y medianos productores urbanos y rurales, fortaleciendo la asociatividad.

Visión: Ser un banco líder y referente regional en servicios financieros inclusivos que aportan al desarrollo productivo rural y urbano.

Para el cumplimiento de la misión y el logro del a visión BanEcuador B.P ha establecido como guías de conducta de todos quienes hacen la institución los siguientes principios y valores:

- **Responsabilidad** Cumplir de manera oportuna con todas las funciones y obligaciones a fin de optimizar los tiempos de respuesta frente a las diversas exigencias, alcanzar las metas planteadas y contribuir al crecimiento institucional.
- **Compromiso:** Identificarse con la institución y los ciudadanos a fin de contribuir al crecimiento y posicionamiento del Banco y apoyar las iniciativas productivas de los ciudadanos, mediante el trabajo y el esfuerzo continuo, para fomentar la inclusión y el desarrollo integral del país.
- **Honestidad:** Actuar con integridad, ética y transparencia, sin ocultar información, ni incurrir en acciones indebidas que afecten a la ciudadanía y a la institución.
- **Respeto**: Aceptar la diversidad étnica y cultural, sus manifestaciones, así como las opiniones de los miembros de la entidad, ciudadanos y demás grupos de interés, a fin de crear relaciones que permitan mantener un buen ambiente de trabajo y la consecución de objetivos en todos los ámbitos.

- **Vocación de servicio**: Servir al país, especialmente al sector rural y urbano marginal, de forma eficiente y oportuna, mediante la entrega de servicios financieros incluyentes, que contribuyan a mejorar la calidad de vida y a disminuir la pobreza.

Estructura Organizacional

Por ser una estructura amplia de difícil visualización se presentará como adjunto en el **Anexo 2**

BanEcuador B.P cuenta con 3 Gerencias, 3 Subgerencias Generales con la misma jerarquía que responde a la gerencia general. Dentro de la Subgerencia general de servicios corporativos se encuentra la gerencia financiera la cual busca administrar de manera eficiente y efectiva los recursos financieros instituciones en función de la normativa vigente y de conformidad con los lineamientos del directorio y la gerencia general de BanEcuador B.P Gerencia Financiera

La gerencia financiera se encarga de administrar de manera eficiente y efectiva los recursos financieros institucionales, en función de la normativa vigente. Consta de las siguientes subgerencias que son las responsables de estos procesos en el banco:

- Subgerencia de Tesorería
- Subgerencia de Contabilidad
- Subgerencia de Control Financiero y Presupuesto

Responsable; Gerente Financiero

Atribuciones y responsabilidades:

- Asesorar a las autoridades, funcionarios y servidores en temas de su competencia;
- Supervisar el cumplimiento de las políticas financieras emanadas por la autoridad de conformidad con lo dispuesto en las leyes, normas y reglamentos pertinentes;
- Dirigir los mecanismos, instrumentos y procedimientos específicos de control interno previo y posteríos, de conformidad con los lineamientos legales y técnicos vigentes;

- Ejecutar los procesos relacionados con los ingresos y egresos institucionales;
- Presentar informes de pagos y de gastos previstos en el presupuesto;
- Validar y ejecutar el proceso de pagos de la nómina institucional;
- Realizar la programación, formulación, aprobación, ejecución, seguimiento, evaluación y liquidación del presupuesto institucional, así como las modificaciones presupuestarias aprobadas por la máxima autoridad, en coordinación con la Subgerencia de Planificación y Monitoreo;
- Realizar oportunamente las solicitudes de pago de las obligaciones económicas de la institución de conformidad a las aprobadas respectivamente;
- Administrar y delegar la custodia, registro, renovación y ejecución, de ser el caso, de valores y documento en garantía;
- Dirigir, revisar, validar y aprobar los estados financieros, análisis de cuentas, informes contables, conciliaciones bancarias. Informes impositivos, entre otros;
- Observar y ejercer las atribuciones y obligaciones específicas determinadas en los artículos 76 y 77, numeral 3 de la Ley Orgánica de la Contraloría General del Estado Proponer la aprobación de constitución de depósitos e inversiones en entidades financieras del país y del exterior en base a la normativa vigente,
- Identificar y negociar líneas de préstamos y créditos de entidades financieras del país y del exterior; Negociar documentos resultantes de operaciones de comercio exterior,
- Proponer la aprobación para la adquisición, conservación o enajenación de contratos a término, opciones de compra venta y futuras;
- Administrar los préstamos y aceptar los créditos de entidades financieras del país y del exterior;

- Formular, dirigir y proponer la titularización con respaldo de la cartera de crédito;
- Aprobar alianzas con entidades públicas y privadas para la implantación de procesos financieros relativos a la operación de la entidad, y,
- Las demás que le asigne la autoridad competente.

Gestión de Tesorería

Misión:

Gestionar los recursos financieros de la Institución para garantizar un óptimo nivel de liquidez de conformidad con el direccionamiento estratégico y las políticas del directorio y la Gerencia General.

Responsable: Subgerencia de Tesorería

Atribuciones y Responsabilidades:

- Asesorar a las autoridades, funcionarios y servidores en temas de su competencia;
- Gestionar y controlar los recursos financieros de la Institución de acuerdo a normativa legal vigente;
- Proponer políticas, procesos y procedimientos para la adecuada gestión de recursos financieros de la entidad;
- Mantener un adecuado portafolio de inversiones en la institución, controlando los excedentes temporales de liquidez, atendiendo las conveniencias institucionales de acuerdo a las leyes pertinentes;
- Presentar el flujo de caja institucional como herramienta de liquidez;
- Controlar la posición de encaje y liquidez de la institución a nivel nacional;
- Controlar el capital operativo del Banco a nivel nacional;
- Establecer estrategias y políticas para el manejo diario de la liquidez institucional;
- Gestionar los proyectos de crédito o fondeo para obtener recursos, redescuentos, desembolsos y anticipos de fondos; y, controlar el

servicio de la deuda de organismos financieros nacionales e internacionales;

- Presentar informes financieros periódicos de los programas de crédito financiados con recursos externos, internos y administración, son la utilización y disponibilidad de los recursos;
- Controlar la emisión y negociación de títulos valores;
- Constituir depósitos en entidades financieras del país y del exterior;
- Establecer el cálculo para el pago del costo financiero, diferencial cambiario (cuando aplique) y alícuotas de capital, que se deban cancelar por recursos utilizados;
- Establecer el plan de Fondeo Institucional, en su ámbito de acción, a través de obligaciones financieras o titulación de cartera, en base a requerimientos de la Institución, políticas de la Administración y movimiento de mercado financiero; y controlar su ejecución conforme la asignación presupuestaria a nivel territorial;
- Controlar y administrar el presupuesto de captaciones asignado a cada área, zonal. Sucursal, agencia;
- Establecer estrategias basado en los reportes de captaciones (del público y obligaciones financieras) a nivel nacional,
- Coordinar con el área correspondiente la programación y entrega del stock de efectivo que cada sucursal y/o agencia mantiene en las bóvedas;
- Coordinar con las demás Gerencias la entrega de información a los organismos externos de control y/o proveedores de recursos financieros;
- Efectuar la gestión de inversión de los excedentes de liquidez y la intermediación de recursos financieros e los mercados bursátiles y extra bursátiles de conformidad con la política institucional, calce la liquidez y las autorizaciones de las instancias competentes;
- Suscribir conjuntamente con los funcionarios autorizados, toda clase de documentos en las operaciones que se realicen entre BanEcuador

B.P. y el Banco Central del Ecuador y la Corporación Financiera Nacional u otras entidades financieras de redescuentos;

- Establecer informes y reporte relacionados con el área para conocimiento de las autoridades interna y entidades de control;
- Administrar y controlar los ingresos y desembolsos de los programas que el gobierno Nacional establezca;
- Adquirir, conservar o enajena contratos a términos, opciones de compra venta y futuros;
- Dar cumplimiento obligatorio a las Normas de control interno; y,
- Las demás que le asigne la autoridad competente.

Productos y servicios:

- Reporte diario a tesorería de la institución.
- Reporte de tases pasivas (nominal y TEA) Banco Central del Ecuador.
- Manual de tesorería.
- Reporte consolidado de pool de fondos.
- Registro de garantías y valores
- Reporte de asignación de recursos financieros.
- Reporte mensual del cumplimiento de metas de captaciones de depósitos monetarios, ahorros y a plazo a nivel nacional.
- Estructuras de información para Superintendencia de Bancos.
- Reporte diario de cupos de permanencia de valores a nivel
- Reporte mensual consolidado de comisiones por convenios
- Reporte mensual de cancelación y/o renovación de invenciones bajo los lineamientos respectivos.
- Reporte de Flujo de Caja
- Reporte de pagos generales y a proveedores.
- Reporte de reposición de fondos por servicios bancarios, saldos deudores y acreedores.
- Reporte de fondos en administración de terceros.
- Informe de proceso de contratación a través de crédito externo u otros mecanismos de similar naturaleza;

- Informe del proceso de emisión de títulos valores y cumplimento de normativa interna y externa previa a la colocación en el mercado bursátil;
- Reporte de utilización, compromiso y pago de obligaciones financieras (crédito externo y fondos de administración);
- Reporte de venta, redención y saldo por colocar de las emisiones de títulos y valores del Banco;
- Reporte de Inversión: compra de títulos valores sector público o privado.
- Reporte de Conciliación Bono de Desarrollo Humano.
- Informe de costo financiero para las sucursales y agencias.
- Reporte de préstamos de entidades financieras del país y del exterior, y de colocación de títulos valores;
- Pólizas de acumulación y/o depósitos a largo plazo
- Plan Anual de fondeo de Recursos a través de otras operaciones diferentes a la captación del público.

Gestión de Contabilidad

Misión:

Generar información contable actualizada, confiable y oportuna para la toma de decisiones de los niveles directivos; bajo criterios técnicos y legales.

Responsable: Subgerencia de Contabilidad

Atribuciones y responsabilidades:

- Asesorar a las autoridades, funcionarios y servidores en temas de su competencia;
- Generar, ajustar y validar los Estados Financieros Consolidados para ser presentados intensamente o a los organismos de control y demás entidades autorizadas, conforme la periodicidad requerida;
- Controlar y propender la trasparencia, consistencia, confiabilidad, razonamiento y suficiencia de las cifras contenidas en los estados financieros y de sus notas;

- Suscribir y refrendar con su firma los Estado Financieros y Comprobantes contables que así corresponda dentro de la entidad, así como para la presentación de estos a los organismos de control;
- Generar, controlar y presentar la información consolidada de tipo fiscal del Banecuador B.P. hacia los organismos pertinentes;
- Elaborar y dar seguimiento a las declaraciones fiscales;
- Válidas las plantillas contables para los diferentes módulos y administrar el sistema contable en lo que al ámbito de su competencia corresponde;
- Supervisar y vigilar el cumplimento de la normativa legal emitida por las entidades de control;
- Revisar y supervisar diariamente que las transacciones contables generadas a nivel nacional cumplan con las disposiciones legales emitidas por los organismos competentes,
- Dirigir, disponer y controlar la elaboración de las conciliaciones con el Banco Central del Ecuador, Cuenta Corriente Única y otros;
- Supervisar el cumplimento del catálogo de cuentas emitido por el órgano de control, así como el establecimiento de cuentas analíticas para todos los hechos económicos del Banco, además de los procedimientos que respalden el registro contable, con el adecuado seguimiento de su correcta aplicación,
- Verificar el correcto registro y sustento de las cuentas por cobrar y por pagar;
- Analizar y validar la parametrizaciòn contable en el core bancario;
- Elaborar instructivos del sistema contable (cierre semestral, cierre del ejercicio anual, registro de asientos manuales y de ajustes, entre otros), y,
- Las demás que le asigne la autoridad competente.

Productos y servicios:

- Estados Financieros Consolidados.
- Estructuras Superintendencia de Bancos.

- Declaraciones fiscales
- Comprobantes, anexos y auxiliares contables.
- Registros de roles de pago del personal.
- Registro de liquidación de haberes
- Retenciones y declaraciones fiscales
- Informes de asesoría técnico contable-financiera a las unidades del banco a nivel nacional.
- Reglamentos, manuales, procedimientos instructivos contables.
- Informe sobre el Estado de saldos diarios de depósitos y encaje bancario.
- Catálogos de cuentas de la institución
- Archivos y expedientes contables físicos y electrónicos
- Informe de validación de información consolidada de tipo fiscal de BanEcuador B.P.
- Reporte de parametrizaciòn de modelos contables aplicados al core bancario.
- Conciliaciones bancarias.
- Reporte de seguimiento y depuración de cuentas.

Gestión de Control Financiero y Presupuestario

Misión:

Establecer, controlar, actualizar el proceso del sistema contable a nivel nacional, así como ejecutar y liquidar el presupuesto del BanEcuador B. P. procurando la utilización óptima de los recursos financieros, con sujeción a la normativa legal vigente.

Responsable: Subgerencia de Control Financiero y Presupuestario

Atribuciones y Responsabilidades:

- Asesorar a las autoridades, funcionarios y servidores en temas de su competencia;

- Dirigir la emisión y aplicación de directrices y procedimientos necesarios para el establecimiento de controles presupuestarios a nivel nacional;
- Informar el cumplimiento y aplicación de disposiciones relacionadas con el control presupuestario impartido por la Administración Central, la Ley General de Instituciones del sistema Financiero y los Organismos de Control;
- Elaborar y presentar a la instancia correspondiente estrategias para reducir costos financieros, operativos y de inversión, y en general, para maximizar la gestión financiera de la institución;
- Analizar y evaluar permanentemente la situación de la Institución y establecer estrategias viables de acción a ser consideradas por las autoridades del Banco para su implementación;
- Establecer modelos de evaluación de rentabilidad de productos y servicios de BanEcuador B.P.
- Evaluar el cumplimento y aplicaciones de disposiciones relacionadas con el presupuesto que sean de carácter financiero, impartidas por la Administración Central, la ley General de Instituciones del Sistema Financiero y de los Organismos de Control;
- Diseñar y establecer el modelo de rentabilidad que permita determinar la eficiencia de las áreas, agencias o sucursales
- Resolver las consultas de las zonales, sucursales y agencia relacionadas con el sistema contable, presupuesto y la ejecución presupuestaria;
- Desarrollar modelos de simulacro presupuestaria de acuerdo a los requerimientos y normativa de la Institución;
- Supervisar las actividades técnicas y operativas del sistema de contabilidad;
- Realizar el costeo de productos, proceso, con el fin de entregar a la Gerencia de Tesorería el insumo para fijación del tarifario;

- Formular la normativa para el control y administración del presupuesto de inversión y operativo;
- Analizar y proponer negociaciones de documentos restantes de operaciones de comercio exterior;
- Definir e implementar el esquema de aplicación de tasas de interés y comisiones por servicios de la institución tomando como insumo el análisis de costo de Control financiero, coordinando su aplicación a nivel nacional con la Gerencia de operaciones y Gerencias Comerciales;
- Elaborar los informes que contengan información correspondiente para el desarrollo del Comité de Activos y Pasivos (ALCO); y,
- Las demás que le asigne la autoridad competente.

Productos y servicios:

- Oficios con anexos para Banco Central y Superintendencia de Bancos
- Matriz de costeo de comisiones y servicios bancarios y financieros.
- Estructuras a entidades de control y anexos.
- Informe de ejecución y liquidaciones presupuestaria
- Informe de análisis y control del presupuesto de operación e investigación.
- Certificados presupuestarios.
- Proyecto de manual de presupuesto
- Instructivo del gasto actualizado
- Modelo de fijación de tasas y tarifas para productos y servicios.
- Infirmes técnicas de control financiero y presupuestario de acuerdo a los requerimientos de las áreas del Banco y de los diferentes organismos de control.
- Manual de operación del sistema contable y presupuestario.
- Documentos de operaciones de comercio exterior negociados
- Registros de depósito en entidades financieras del país y del exterior.
- Informe semanal para el comité de Activos y Pasivos (ALCO).
- Contratos a término, opciones de compra venta y futuros.

Gerencia de Tecnología de la Información

La gerencia de la Tecnología de la Información provee y administra soluciones tecnológicas con herramientas de vanguardia y altos estándares de calidad que soporten permanentemente la actividad del banco en operaciones activas y pasivas, así como la continuidad de dichos servicios. Consta de las siguientes subgerencias que son las responsables de estos procesos en el banco:

- Subgerencia de Desarrollo y Mantenimiento de aplicaciones
- Subgerente de Gestión Y Control
- Subgerente de Producción y Operaciones
- Subgerente de Infraestructura Tecnológica

Responsable: Gerente de tecnología de la Información y Comunicación

Atribuciones y Responsabilidades:

- Asesorar a las autoridades, funcionarios y servidores en temas de su competencia;
- Proveer y administrar los servicios informáticos que la Instituciones requiera;
- Definir los estándares y arquitectura para los servicios informáticos;
- Definir y ejecutar los procesos y proyectos de tecnología que contribuyan a la presentación de los servicios informáticos;
- Definir lineamientos para control de los proyectos y procesos de tecnología de información
- Administrar funcionalmente a las unidades de tecnología ubicadas en las oficinas zonales del Banco;
- Validar los modelos de solución para el desarrollo y mantenimiento de aplicaciones, mantenimiento evolutivo y correctivo de los sistemas actuales;
- Supervisar las actividades de desarrollo, implementación y migración de datos;

- Validar la implementación y diseño de scripts;
- Validar propuestas de mejora y seguimiento de políticas internas, procesos y procedimientos de gestión de las subgerencias a su cargo;
- Aprobar la salida a producción de las soluciones o aplicaciones informáticas;
- Emitirlos lineamientos para la administración de proyectos tecnológicos y de infraestructura de Tics;
- Proponer cambios a la infraestructura, aplicaciones y bases de datos de Tics;
- Supervisar y validar los procedimientos e integridad de los respaldos de datos almacenados;
- Aprobar los manuales de usuario para los sistemas del Banco;
- Monitorear y controlar las actividades de soporte técnico a los usuarios en los servicios informativos, y,
- Las demás que le asigne la autoridad competente.

Gestión de Desarrollo y Mantenimiento de Aplicaciones

Misión:

Desarrollar nuevos sistemas y aplicativos que soporten y permitan hacer uso de la información tecnológica que el Banco produce en forma diaria y que agreguen valor a los proseos de negocios del Banco, además de realizar el mantenimiento correctivo y evolutivo a los aplicativos existente, para que cumplan con los requerimientos institucionales.

Responsable: subgerencia de Desarrollo y Mantenimiento de Aplicaciones

Atribuciones y Responsabilidades:

- Asesorar a las autoridades, funcionarios y servidores en temas de su competencia;
- Generar informes de factibilidad técnicos para la adquisición o para el desarrollo de nuevos sistemas informáticos;
- Analizar, diseñar y establece modelos de solución para el desarrollo y mantenimiento de aplicaciones y/o mantenimiento evolutivo y

correctivo de los sistemas actuales, de acuerdo a las especificaciones dadas dentro de las diferentes plataformas tecnológicas del banco;

- Planificar y ejecutar las actividades de desarrollo, implementación y migración de datos enmarcados en un concepto de calidad y conforme a la prioridad establecida por las distintas áreas de negocio del Banco,
- Entregar el código fuente de las soluciones informativas nuevas o mantenimiento de las existentes a la Subgerencia de Gestión y Control, para que se ejecute el control de calidad y pruebas de aceptación;
- Diseñar e implementar scripts de migración de datos;
- Brindar soporte técnico al área de Mesa de Ayuda, Producción y Operaciones, en las actividades de resolución de incidentes;
- Diseñar y proponer mejoras a las Políticas y Metodología relacionada con el ciclo de vida de software, de manera conjunta con la subgerencia de gestión y Control;
- Mantener actualizada la documentación técnica de los sistemas productivos; y,
- Las demás que asigne la autoridad competente.

Productos y Servicios:

- General informe de factibilidad para adquisición o construcción in-house de soluciones informáticas.
- Políticas y metodología del ciclo de vida del software.
- Generar y actualizar Manuales técnicos de los sistemas del Banco;
    a. Sistema core Bancario Cobis – 25 módulos y componentes (módulos de activas, módulo de pasivas, módulos financieros, modos de canales, módulos de seguridades y módulos de integración),
    b. Interoperación con el sistema Core de servicios Cash management (Transaccionalidad on line),

c. Sistemas satélites provistos por el Banco Central del Ecuador, sistemas de inteligencia de negocios (sistemas de lavado de activos, sistema de originacion de los créditos con dispositivos móviles, entre otros).

- Desarrollo de nuevos sistemas informáticos.
- Mantenimiento correctivo y evolutivo de los sistemas actuales, que automatizan los procesos operáticos del Banco:
    d. Sistema Core bancario Cobis – 25 módulos y componentes (módulo de activas, módulos de pasivas, módulos financieros, módulos de canales electrónicos, módulos de seguridad y módulos de integración),
    e. Interoperación con el sistema Core de Servicios Cash Management (Transaccionalidad on line),
    f. Sistemas satélites provistos por el Banco Central del Ecuador, sistemas de créditos con dispositivos móviles, otros sistemas satélites.
- Informe periódico de medición y evaluación de desempeño del Core Bancario.

Gestión de Gestión y control

Misión:

Establecer y mantener un Sistema de Gestión y Control con un enfoque estándar, formal y continuo para los procesos de: administración de proyectos y procesos informáticos, gestión de cambios, aseguramiento de la calidad, seguimiento y control, de las disposiciones de organismos de control y normativas de regulación relacionadas con tecnologías de información.

Responsable: Subgerencia de Gestión y Control

Atribuciones y Responsabilidades:

- Asesorar a las autoridades, funcionarios y servidores en temas de su competencia;
- Analizar, definir e implementar los procesos de gestión de Tecnología de Información;

- Realizar el seguimiento, control de procesos, normas y políticas internas y las impartidas los Organismos Externos y de control;
- Administrar el proceso para la implementación de los cambios que incluya comunicar el estado de los cambios implantados en producción a los interesados;
- Gestionar la salida a producción de las soluciones o aplicaciones informáticas;
- Presentar procesos para la aprobación de salidas a producción de las soluciones o aplicaciones informáticas;
- Coordinar la prueba funcional con los usuarios, a fin realizar la certificación de un cambio, previo a su paso a producción;
- Administrar el proceso de gestión de proyectos tecnológicos;
- Evaluar el levantamiento de información de los requerimientos funcionales previo al desarrollo de estos;

Productos y Servicios:

- Procesos operativos de Tecnología
- Informe de seguimiento de proyectos.
- Informe sobre observaciones impartidas por los organismos internos y externos de control.
- Información actualizada sobre el proceso de gestión de proyectos de Tecnología de Información.
- Informe sobre requerimiento certificados en calidad.
- Manuales de Usuario de los sistemas del Banco e Informe de aplicación:
    a. Sistema Core Bancario Cobis – 25 módulos y componentes (módulos de activas, módulos de pasivas, módulos financieros, módulos de canales, módulos de seguridad y módulos de integración),
    b. Interoperación con el sistema Core de Servicios Cash Management,

c. Sistemas satélites provistos por el Banco central del Ecuador, sistemas de inteligencia de negocios (sistema de lavado de activos, sistema de originaciòn de créditos con dispositivos móviles, otros sistemas satélites.

Gestión de Producción y Operaciones

Misión:

Administrar, operar y monitorear los ambientes productivos de los Centros de Procesamiento y levantamiento de datos de la Institución para garantizar la continuidad de los servicios informáticos. Desplegar los sistemas informáticos, realizar la Gestión de configuración, monitorear las cartas de servicios, gestionar versionamientos, administrar las bases de datos.

Responsable: Subgerencia de Producción y Operaciones.

Atribuciones y Responsabilidades:

- Asesoramiento a las autoridades, funcionarios y servidores en tenas de su competencia;
- Definir y gestionar las políticas, procesos y procedimientos de gestión, operación y monitoreo de los Centros de cómputos de la Institución, el control de acceso a los mismos y la ejecución de mantenimientos preventivos y correctivos de las facilidades de infraestructura física;
- Definir y gestionar las políticas, procesos y procedimientos para la ejecución de procesos batch;
- Registrar la ejecución de los cambios autorizados a la infraestructura, aplicaciones y bases de datos de tecnología de la información;
- Definir y gestionar las políticas, procesos y procedimientos del repositorio y control de versiones de software autorizado en producción y otros ambientes controlados;
- Definir y gestionar las políticas, procesos y procedimientos de planificación, gestión, capacidad y desempeño de las bases de datos;
- Definir y gestionar las políticas, procesos y procedimientos para monitorear el desempeño de los recursos de tecnología y bases de

datos, con la finalidad de poner a punto las necesidades actuales de procesamiento, contingencia, carga de trabajos actuales y proyectados;

- Definir y gestionar las políticas, procesos de los procedimientos de respaldo y su almacenamiento;
- Definir y gestionar las políticas, procesos y procedimientos de despliegue y liberación de aplicaciones;
- Identificar, registra y clasificar los problemas, dentro de su ámbito de acción, que provoquen la degradación o interrupción en los servicios informáticos, determinando la causa raíz de su ocurrencia y coordinar su solución definitiva; y,
- Las demás que le asigne la autoridad competente.

Productos y Servicios

- Manuales para el procesamiento batch.
- Manuales del repositorio y control de versiones de software autorizado en producción y otros ambientes controlados.
- Manuales de monitoreo del desempeño de los recursos de tecnología y bases de datos.
- Manuales de administración de la configuración de recursos tecnológicos de los Centros de Cómputo.
- Manuales de los procesos de respaldo y su almacenamiento.
- Manuales de despliegue y liberación de aplicaciones.
- Informe semestral de ejecución de procesos batch.
- Informe semestral de cambios aplicados a producción.
- Informe semestral de cambios aplicados a producción, de versionamiento y despliegue.
- Informe semestral de seguimiento a SLA y cartas de servicio, y cumplimiento de proveedores.
- Informe semestral de gestión de configuración.
- Informe semestral de respaldos realizados, numero de cintas utilizadas, y pruebas de recuperación realizadas.

Gestión de Infraestructura Tecnológica

Misión:

Proporcionar y garantizar la disponibilidad de la infraestructura tecnológica y de telecomunicaciones, y gestionar la mesa de servicios de Tecnología.

Responsable: Subgerencia de Infraestructura Tecnológica

Atribuciones y Responsabilidades:

- Asesorar a las autoridades, funcionarios y servidores en temas de su competencia;
- Diseñar y ejecutar el plan de mantenimientos preventivo y correctivo de infraestructura tecnológica;
- Dimensionar y gestionar la infraestructura para ambientes de producción, pruebas, desarrollo y otros, de acuerdo a las necesidades del Banco;
- Administrar y ejecutar la seguridad para la infraestructura tecnológica conforme a las políticas emitidas por la Gerencia de Riesgos;
- Identificar, monitorear, corregir y reportar vulnerabilidades e incidentes de seguridad sobre la infraestructura tecnológica y telecomunicaciones;
- Colaborar en la implementación del Plan de Contingencia tecnológica con base al Plan de Continuidad del Negocio, garantizando la continuidad de los servicios críticos identificados y definidos por la Gerencia de Riesgos;
- Gestionar la Mesa de Servicios Tecnología; y,
- Las demás que le asigne la autoridad competente.

Productos y Servicios

- Manuales para instalación, configuración y mantenimiento de infraestructura tecnológica y telecomunicaciones.
- Informe disponibilidad de la infraestructura tecnológica y telecomunicaciones.

- Procedimientos de seguridad tecnológica, en concordancia con las políticas de seguridad de la información emitidas por la Gerencia de Riesgos.
- Informe de monitoreo, detección y solución de vulnerabilidades e incidentes de seguridad de tecnología de la Información.
- Reporte de satisfacción de usuarios sobre requerimientos e incidentes tecnológicos.
- Informe de gestión de capacidad.

Parámetros de Calidad

Los parámetros de calidad que busca la gerencia de tecnología de la información para los requerimientos de la información en la toma de decisiones son:

- Oportuna
- Confiable
- Utilizable

Política interna de Seguridad de Información

Esta política se implementó desde la creación del banco en conjunto con los analistas de cada área basados a parámetros mínimos aplicados:

- Gestión de riesgos
- Seguridad física y ambiental
- Gestión de la continuidad de los servicios
- Control de acceso
- Gestión de incidentes de seguridad

Actualmente BanEcuador B.P no posee una certificación internacional que norme las seguridades en la empresa.

Sistema Core Bancario Cobis

Cobis provee a las instituciones financieras las herramientas que permiten realizar de una manera eficiente su operación diaria. Bajo una plataforma tecnológica abierta y software avanzado que cubren los diferentes requerimientos en el complejo mundo de las instituciones financieras, el cual comprende todo el manejo operativo de misión crítica y de estrategia de

negocios de los bancos requieren para el manejo y control total de las operaciones de la institución. (COBIS)

Desde la creación de BanEcuador B.P se ha implementado el sistema Core Bancario Cobis hasta la actualidad.

Los módulos de Cobis son:

- Cobis core
- Cobis clientes
- Cobis contabilidad
- Cobis cuentas corrientes
- Cobis cámara y remesas
- Cobis cuentas de ahorros
- Cobis firmas electrónicas
- Cobis servicios bancarios
- Cobis ip (procesamiento de documentos)
- Cobis if (image fólder)
- Cobis crédito
- Cobis cartera
- Cobis garantías
- Cobis depósitos a plazo
- Cobis mesa de dinero y cambios
- Cobis comercio exterior
- Cobis work flow
- Cobis branch
- Cobis branch explorer
- Cobis (reportes a las entidades de control) rec
- Cobis (sistema de administración contable) sidac

En la Gerencia Financiera se Utilizan los módulos de Cobis contabilidad y Cobis (sistema de administración contable) Sidac.

Selección de Proceso Critico

Entrevista para selección de procesos críticos

Se nos fue proporcionado por BanEcuador B.P los manuales de procesos de la Gerencia Financiera, y de cada una de su subgerencia para poseer un mejor entendimiento de cada uno de los procesos que maneja el área.

Posterior como herramienta de levantamiento de información se realizó una entrevista estructura al Gerente Financiero, Subgerentes de Tesorería, Contabilidad, Control Financiero y Presupuesto al igual que a cuatro analistas de las áreas para poder determinar cuáles son los procesos críticos.

Preguntas Realizadas

Tabla 6 *Preguntas para definir procesos críticos*

	Preguntas
1	¿Cuántos procesos maneja su área?
2	¿Qué proceso considera más fácil o
3	difícil?
4	¿Qué proceso considera más
5	sensible?
	¿Qué proceso considera critico en la actualidad?
	¿Tiene conocimiento que poseen un manual de procesos?

Fuente Elaboración de las autoras

El resultado de la entrevista realizada arrojo tres procesos en la Gerencia Financiera que se consideran críticos:

Tabla 7 *Procesos críticos Financieros*

Proceso	Definición
Elaboración de Pruebas Departamentales	Generar información confiable, oportuna y adecuada que finalmente se verá reflejada en los Estados financieros de BanEcuador B.P.
Gestión de Viáticos	Atender los requerimientos de acreditación de valores a los servidores públicos del banco por concepto de viáticos en comisión de servicios hasta el registro contable de los gastos por este concepto.
Control de Pago Proveedores	Cumplir con las normas de control interno establecidas por la Contraloría

Fuente: Elaboración de las autoras

A continuación, se presenta un detalle de los procesos críticos encontrados en la Gerencia Financiera

Elaboración de Pruebas Departamentales

En términos generales, se realiza una evaluación de este proceso a los principales actores involucrados, esto es, Área requirente, Subgerente de Contabilidad, Responsable de Ejecutar Prueba Departamental, Analista Financiero Zonal, Analista de contabilidad Matriz y Especialista de Contabilidad.

El resultado de esta revisión arroja las principales dificultades del proceso en varios aspectos; generar el estado de cuentas mensual, regularizar las transacciones inconsistentes, consolidar las pruebas departamentales a nivel zonal y después a nivel nacional, realizar el informe de pruebas departamentales.

En dicho informe se hace referencia a debilidades de seguridad por la diversa manipulación de dicho informe final. Es una preocupación de la Gerencia Financiera contar con la seguridad de la información de su área, el

cumplimiento de los procedimientos formales para reducir las vulnerabilidades a los procesos internos en unión a su herramienta tecnológica.

Gestión de Viáticos

Como segundo proceso critico se identificó la gestión de viáticos, dentro de la misma entrevista a los Analistas del Área Financiero con el Analista de Contabilidad. Indicó que al revisar la documentación este completa y con sus respectivos sustentos, no se estaría cumpliendo con este procedimiento ya que la información como sustento se la recibe de forma escaneada para poder agilitar el pago, la documentación original llega días posteriores lo que no permite tomar correctivos a tiempo.

Control de Pago Proveedores

Al analizar el tercer proceso crítico, expuesto dentro de la entrevista con los involucrados en este proceso, se indicó que, al revisar la certificación de fondos, el formulario de desglose de utilización de fondos y verificación de la disponibilidad presupuestaria. Carece de sustento físico que garantices la autenticidad de la utilización de fondos.

Por la importancia de proceso con BanEcuador B.P para la toma de decisiones, el Gerente Financiero, selecciona el proceso de Elaboración de Pruebas departamentales para realizar un análisis detallado de identificación de vulnerabilidades, gestión de riesgos y procesos que guarden relación con las TI según la norma COBIT la cual está asociada con la ISO 27001.

Proceso de Elaboración de Pruebas Departamentales

La Elaboración de Pruebas Departamentales se define como un proceso que inicia con el resultado de la conciliación de las cuentas contables y termina con la entrega de las pruebas departamentales a la Subgerencia de Contabilidad en los tiempos establecidos.

Las actividades principales de la Elaboración de Pruebas Departamentales son:

- Generar estado de cuenta
- Analizar y conciliar partidas
- Regularizar la transacción inconsistente

- Elaborar la prueba departamental
- Revisar prueba departamental
- Realizar análisis de consistencia, confiabilidad, soporte y variación de saldos
- Validad informe de pruebas departamentales

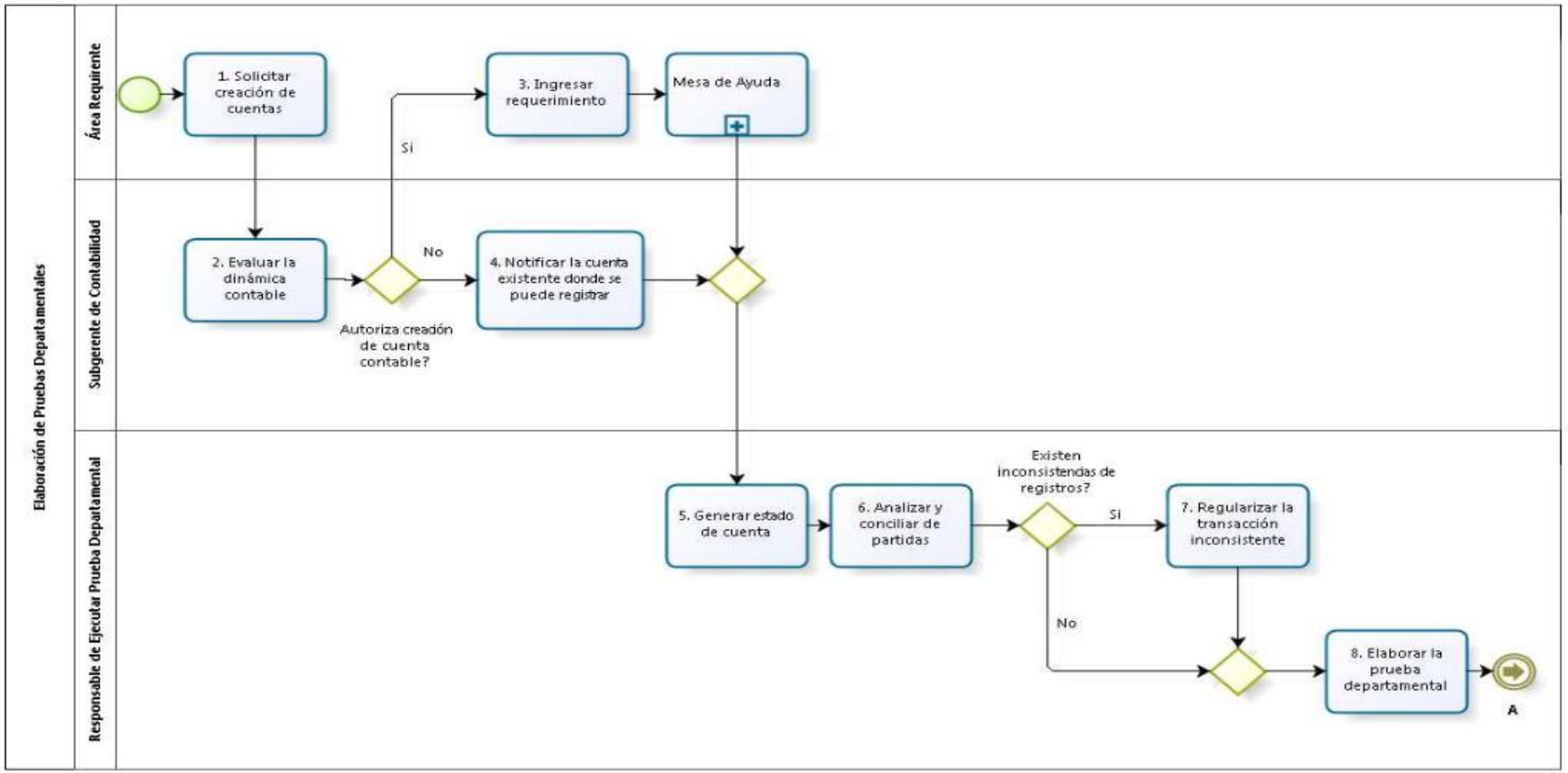
Las reglas de este subproceso son:

- Se deberá realizar el cuadre diario de las cuentas bajo responsabilidad de cada una de las Gerencias del Banco,
- Los saldos de las partidas que no se regularizaron dentro del mismo mes, se trasladaran a la prueba departamental que será cargada en el repositorio correspondiente.
- Las partidas pendientes que se registren en la prueba departamental deberán ser regularizadas hasta el 15 del siguiente mes.
- Las pruebas departamentales de fin de mes tendrán dos fechas de corte:
    - Al 26 o el día anterior laborable de cada mes; y será entregado el siguiente día laborable
- La fecha de entrega de pruebas departamentales a la Subgerencia de Contabilidad será:
    - Primer corte. - Hasta el 28 de cada mes.
    - Segundo Corte. - Hasta el tercer día hábil del siguiente mes, posterior al cierre del balance definitivo.
- Las pruebas departamentales se presentarán debidamente conciliadas con los saldos del balance.
- Las partidas que se depuren cada mes deberán contener el respaldo y sustento de los cruces y/o registro contable de la regularización realizada, en caso de evidenciarse inconsistencias, se aplicará sanciones estipuladas de acuerdo a lo establecido en el reglamento interno.

- La línea de supervisión del responsable de cuenta debe asegurar la veracidad de la información que conste en la prueba departamental.
- El envió de pruebas departamentales a la Subgerencia de Contabilidad, por parte de la línea de supervisión de la Gerencia responsable de las cuentas, implica aceptación de que la información presentada, así como también de su regularización.
- Una vez entregada las pruebas departamentales, cada responsable de las cuentas, debe realizar un seguimiento minucioso de la partida pendiente hasta su regularización o depuración en un tiempo máximo de dos días hábiles
- Las partidas que fueron depuradas en un mes no deberán aparecer en meses posteriores, en caso de evidenciarse información inconsistente en la prueba departamental, se aplicara sanciones estipuladas de acuerdo con lo establecido en el reglamento interno.

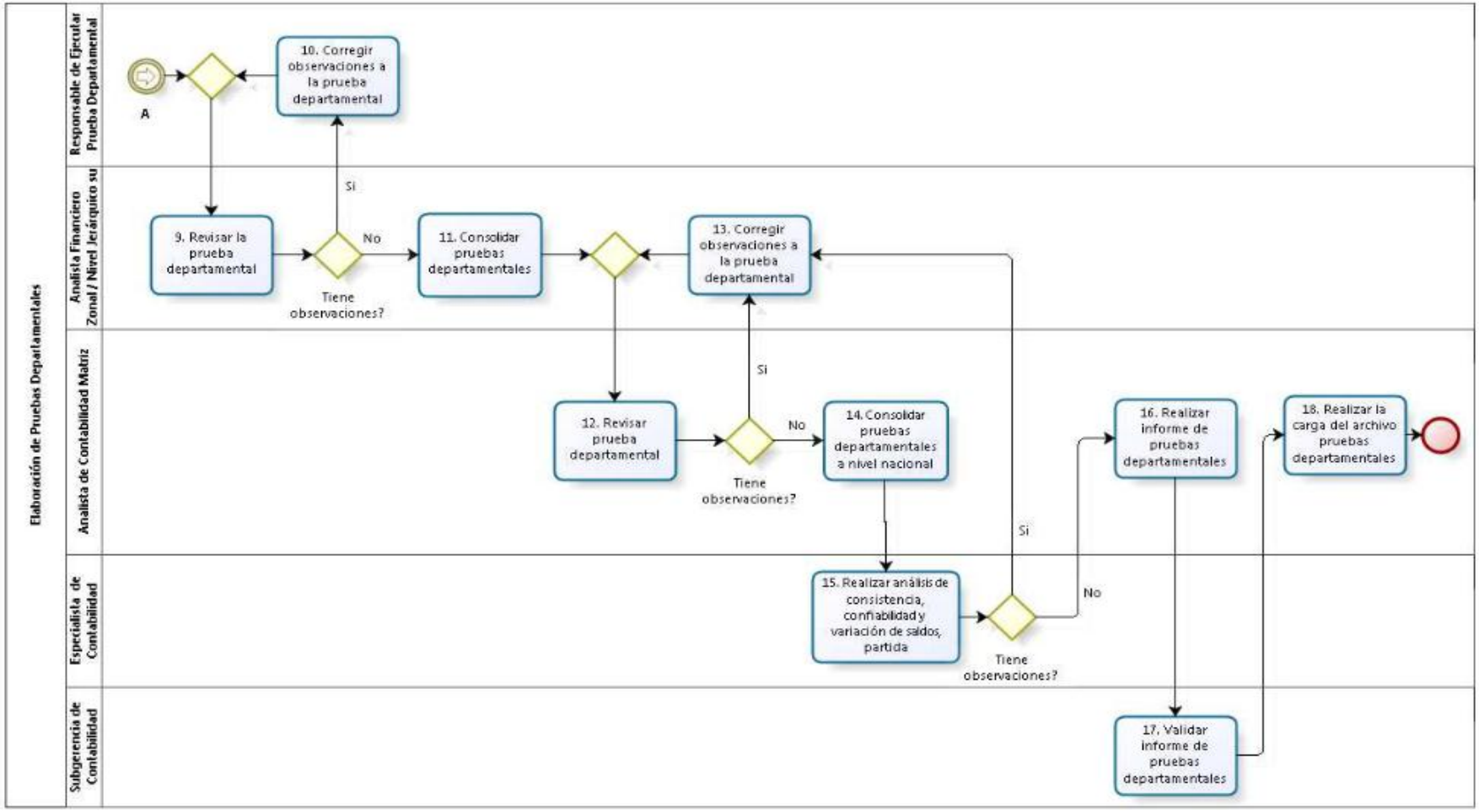
En diagrama de flujo corresponde para un mejor entendimiento de cada uno de los pasos y probabilidades que podrían darse en el transcurso del proceso identificando cada una de las áreas y personal involucrado en el mismo.

Ilustración 21 Diagrama de Flujo de Elaboración de Pruebas Departamentales Parte 1



Fuente: Manual de Proceso de Gestión Contable BanEcuador

Ilustración 22 *Diagrama de Flujo de Elaboración de Pruebas Departamentales Parte 2*



Fuente: Manual de Proceso de Gestión Contable BanEcuador

En el diagrama anterior se puede determinar que en el proceso de Elaboración de pruebas departamentales se considera como acción inicial solicitar creación de cuentas que después de ser analizado es evaluado la dinámica contable si no está creada se ingresa el requerimiento a mesa de ayuda.

Para poder entender posteriormente el nivel de riesgo del proceso seleccionado es importante analizar los riesgos del área en función a la Gerencia de TT. Por ser parte importante de este análisis se realizó una entrevista también con el área de Gerencia de TI para conocer su experiencia en los riesgos que se presentan en la organización a nivel general y especificando el interés en el área de Gerencia Financiera.

Relación del Área Financiera en Función de Recursos Ti

Identificación de Riesgos en Función de Recursos Ti

Se debe reconocer que para la Gerencia de TI la existencia de eventos que involucren el desempeño óptimo de los servicios computarizados e informáticos es una preocupación.

Actualmente BanEcuador B.P tiene la Gerencia de Riesgo, con la cual debería existir un mejor entendimiento entre la Gerencia de TI para obtener una adecuada administración de los riesgos encontrados.

Al poseer identificados los procesos críticos que fueron considerados por las partes interesadas del área en estudio, podemos determinar en conjunto con el Gerente Financiero mediante un esquema cuales son las principales amenazas encontradas que guarden relación con los recursos de TI.

Tabla 8 *Riesgos Financiero en Función de recursos de Ti*

Gerencia Financiera

Amenazas	**Vulnerabilidad**	**Riesgos financieros en función de Ti**
Acceso a usuarios no autorizados Manipulación de Información sin un control regido.	Divulgación de información confidencial. Acceso a información permitiendo actos maliciosos.	Acceso no controlado a la información confidencial.
Falta de codificación a los archivos encriptados.	Falta de aplicación de política de encriptado de información.	Perdida de confiabilidad en información para la toma de decisiones

Fuente Elaboración de las autoras

COBIT presenta en su marco integrador las metas corporativas y metas relacionadas con la TI buscando que la empresa reconozca que en la actualidad la información como un activo vital para el desarrollo óptimo de las actividades de la organización.

Para seguir con el análisis se debe definir metas con el área de Gerencia Financiera relacionadas con más metas determinadas como corporativas en el COBIT.

Después de haber definido los riesgos y amenazas que se detectaron en la tabla anterior, se le solicita al gerente financiero previo al conocimiento de que son las metas corporativas de COBIT definir 5 metas las cuales serán relacionadas entre sí, las misma que se presentan a continuación:

- Unificación de Información de la Gerencia Financiera
- Maximización de la Eficiencia de la Gerencia Financiera
- Aseguramiento de controles en la Gerencia Financiera
- Optimización de la productividad de la Gerencia Financiera
- Seguridad de la información de la Gerencia financiera

Ilustración 23 *Metas Corporativas con Enfoque Financiero*

Metas Corporativas		Metas de Gerencia Financiera
Valor para las partes interesadas de las inversiones de Negocio	⟷	Unificacion de Informacion de la Gerencia Financiera
Cartera de productos Servicios Competitivos	⟷	Maximizaciòn de la eficiencia de la Gerencia Financiera
Riesgo de Negocio Gestionados	⟷	Aseguramiento de controles de la Gerencia Financiera
Cumplimientos de leyes y regulaciones externas	⟷	Optimización de la productividad de la Gerencia Financiera
Transparencia Financiera	⟷	Seguridad de la información de la Gerencia financiera

Fuente Elaboración de las autoras

Al conocer las metas de la Gerencia Financiera es momento de que se integren con las metas relacionadas con TI que presenta COBIT para identificar cuáles son las metas que guardan relación entre si, se realizara el análisis propuesto en el modelo.

Unificación de Metas

En la siguiente ilustración se podrá observar la integración de las metas relacionadas con la Gerencia Financiera y Gerencia TI, se han identificado las relaciones P (principales) y S (secundarias).

Ilustración 24 *Meta relacionadas con Ti*

Meta relacionada con las Ti	Unificacion de Informacion de la Gerencia Financiera	Maximizaciòn de la eficiencia de la Gerencia Financiera	Aseguramiento de controles de la Gerencia Financiera	Optimización de la productividad de la Gerencia Financiera	Seguridad de la información de la Gerencia financiera
Alineamiento de Ti y estrategia de negocio	P	P	S		
Cumplimiento y soporte de Ti al cumplimiento del negocio de las leyes y regulaciones externas			S	P	
Compromiso de la direccion ejecutiva para tomar decisiones relacionas con Ti	P	S	S		
Riesgo de negocio relacionados con Ti gestionados		p	S		
Realizacion de beneficios del portafolio de inversiones y servicios relacionados con las Ti	P	P			
Trasparencia de los costos, beneficios y riesgos de Ti	S		S		P

Fuente Elaboración de las autoras

En la ilustración podemos identificar las metas de TI con mayor incidencia con la Gerencia Financiera es decir las detectadas como principales.

Las metas de la Gerencia Financiera unificación de la información de la Gerencia Financiera y Maximización de la eficiencia de la Gerencia Financiera guardan relación con la meta TI Alineamiento de ti y estrategia de negocio.

La meta de la Gerencia Financiera Optimización de la productividad de la Gerencia Financiera guarda relación con la meta TI Cumplimiento y soporte de Ti al cumplimiento del negocio de las leyes y regulaciones externas.

La meta de la Gerencia Financiera Unificación de Información de la Gerencia Financiera guarda relación con la meta TI Compromiso de la dirección ejecutiva para tomar decisiones

La meta de la Gerencia Financiera Maximización de la eficiencia de la Gerencia Financiera guarda relación con la meta TI Riesgo de negocio relacionados con Ti gestionados

Las metas unificación de la información de la Gerencia Financiera y Maximización de la eficiencia de la Gerencia Financiera guardan relación con la meta de Ti realización de beneficios del portafolio de inversiones y servicios relacionados con las TI.

Podemos darnos cuenta de que las necesidades de la Gerencia Financiera integra o se califican como principales con las metas de Ti esto nos da entender que para un esencial desenvolvimiento de la organización en el área financiera es relevante un correcto manejo de sus sistemas ya que son los que emiten la realidad monetaria que presenta las organizaciones y esto ayuda en la toma de decisiones en la misma.

Nuestros marcos referenciales para el análisis de los riesgos presentados en la organización de la Gerencia Financiera integrados y relaciones con la gerencia de Ti son el COBIT e ISO 27001 que previo a un análisis inicial en el marco teórico definimos en la ilustración 19.

La integración de estas normas internacionales basados en la información que COBIT nos presenta en donde se pude definir que de los 37 procesos integrados en 5 dominios estas dos normas se interrelacionan en los dominios de:

Evaluar Orientar y supervisar (EDM)

Alinear Planificar y Organizar (APO).

Para seguir con nuestro estudio debemos realizar una observación de campo en conjunto con el Gerente financiero para determinar de los 37 procesos que nos presenta el COBIT cuáles son los considerados principales basados a los riesgos y amenazas conocidos.

Identificación de Procesos

Identificación de procesos de la Gerencia Financiera en relación con TI

Al conocer los procesos críticos, la amenazas y las metas relacionadas es hora de definir cuáles son los procesos que se van a evaluar. Se determinará mediante las metas de la Gerencia financiera y los 37 procesos del COBIT el análisis para identificar los procesos que a consideración del área son los principales. El detalle del análisis se presenta en el **Anexo 2.**

En la ilustración siguiente se presentan los procesos ya seleccionados relacionados con la evaluación de las metas de la gerencia financiera y el acoplamiento de la ISO 27001. Los procesos de COBIT serán analizados desde la perspectiva del riesgo mediante evaluación.

Ilustración 25 Procesos seleccionados

Organización de TI	Dominios		Procesos	ISO 27001
Gobierno	Evaluar,Orientar, Supervisar	EDM	EDM03. Asegurar la optimizaciòn del riesgo	*Evaluaciòn de riesgos de seguridad de informaciòn * Tratamiento de riesgos de seguridad de la informaciòn
Gestiòn	Alinear , Planificar , organizar	APO	APO11 Gestionar la Calidad APO12 Gestionar el Riesgo APO13 Gestionar la seguridad	
	Construir , adquirir, implementar	BAI	BAI01 GEStionar los programas y proyectos	
	Entregar, dar servicio y soporte	DSS	DSS05. Gestionar los servicios de seguridad DSS06 Gestionar los controles de los procesos de negocios	

Fuente Elaboración de las autoras

De igual manera se deben identificar los procesos que en consideración con las Ti se encuentran en mayor criticidad. Estas fueron definidas mediante la matriz management awareness diagnostic y la matriz Raci que detalla la metodología del COBIT 5. Se estableció dar un peso al componente de

desempeño e importancia del 70% para encontrar los procesos más críticos, y siendo el 30% el peso otorgado al total de las preguntas. Donde 30 es el máximo valor y 6 el mínimo. Se considera en cada pregunta que la ponderación es de 5 el cual representa de mayor riesgo y el 1 de menor riesgo. Se considerará el nivel de criticidad mediante:

- 6-9 bien ejecutado
- 10-20 Medianamente ejecutado
- 21-30 Atención por Mejorar

Procesos Críticos de TI

Mediante el análisis de la información y ejecución de las preguntas al Gerente de Ti se puede desprender los resultados de lo proceso que para el área son ms críticos se presentan los resultados:

Ilustración 26 *Procesos críticos según TI parte 1*

	PROCESOS	CRITICIDAD
1	EDM01 Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	22
2	EDM02 Asegurar la Entrega de Beneficios	21
3	EDM03 Asegurar la Optimizacióndel Riesgo	25
4	EDM04 Asegurar la Optimizaciónde los Recursos	19
5	EDM05 Asegurar la Transparenciahacia las partes interesadas	18
6	APO1 Gestion de Marco de Gestion de Ti	21
7	APO02 Gestionar la Estrategia	16
8	APO03 Gestionar la Arquitectura Empresarial	20
9	APO04 Gestionar la Innovación	17
10	APO05 Gestionar el portafolio	16
11	APO06 Gestionar el Presupuesto ylos Costes	15
12	APO07 Gestionar los Recursos Humanos	18
13	APO08 Gestionar las Relaciones	19
14	APO09 Gestionar los Acuerdos de Servicio	16
15	APO10 Gestionar los Proveedores	17

Fuente: Elaboración de las autora

Ilustración 27 *Procesos críticos según Ti parte 2*

	PROCESOS	CRITICIDAD
16	APO11 Gestionar la Calidad	18
17	APO12 Gestionar el Riesgo	20
18	APO13 Gestionar la Seguridad	24
19	BAI01 Gestionar los Programas y Proyectos	16
20	BAI02 Gestionar la Definición de requisitos	14
21	BAI03 Gestionar la Identificación y la Construcción de Soluciones	14
22	BAI04 Gestionar la Disponibilidad y la capacidad	13
23	BAI05 Gestionar la introducción de cambios organizativos	13
24	BAI06 Gestionar los Cambios	16
25	BAI07 Gestionar la Aceptación del cambio y de la transicion	12
26	BAI08 Gestionar el Conocimiento	15
27	BAI09 Gestionar los Activos	12
28	BAI10 Gestionar la Configuración	13
29	DSS01 Gestionar las Operaciones	15
30	DSS02 Gestionar las Peticiones ny los incidentes del servicio	17
31	DSS03 Gestionar los Problemas	18
32	DSS04 Gestionar la Continuidad	18
33	DSS05 Gestionar los Servicios de Seguridad	20
34	DSS06 Gestionar los Controles de lo sprocesos del negocio	20
35	MEA01 Supervisar, Evaluar y Valorar Rendimientoy conformidad	19
36	MEA02 Supervisar, Evaluar y Valorar el sistema de control interno	18
37	MEA03 Supervisar, Evaluar y Valorar la conformidad con los requerimientos externos	19

Fuente: Elaboración de las autoras

Como podemos identificar para el área de TI surgen 5 procesos con mayores riesgos críticos que se presenta a continuación, pero las demás evaluaciones realizadas a cada uno de los 37 procesos pueden ser visualizados en el **anexo 3**

Ilustración 28 *Diagnostico de criticidad al proceso EDM01*

	PROCESO	**EDM01 Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno**					
	DESCRIPCION	Analizar y articular los requisitos para la gobernanza de TI empresarial, y establecer y mantener estructuras, principios, procesos y prácticas de habilitación eficaces, con claridad de responsabilidades y autoridad para lograr la misión, las metas y los objetivos de la empresa.					
No.	**PREGUNTA**	**VALOR**	**1**	**2**	**3**	**4**	**5**
1	En cuanto influye para el éxito de la empresa el proceso	5	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	4	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	5	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	4	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**22**					

Fuente: Elaboración de las autoras

Ilustración 29 *Diagnostico de criticada al proceso EDM02*

	PROCESO	EDM02 Asegurar la Entrega de Beneficios					
	DESCRIPCION	Optimice la contribución de valor a la empresa a partir de los procesos comerciales, los servicios de TI y los activos de TI resultantes de las inversiones realizadas por TI a un costo aceptable.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	4	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	5	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	4	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	4	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	21					

Fuente: Elaboración de las autoras

Ilustración 30 Diagnostico de criticidad al Proceso EDM03 Fuente:

	PROCESO	EDM03 Asegurar la Optimizacióndel Riesgo					
	DESCRIPCION	Asegúrese de que el apetito y la tolerancia al riesgo de la empresa se entiendan, articulen y comuniquen, y que se identifique y gestione el riesgo para el valor empresarial relacionado con el uso de la TI.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	5	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	4	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	5	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	5	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	5	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	25					

Fuente: Elaboración de las autoras

Ilustración 31 *Diagnostico de Criticada al Proceso APO01*

	PROCESO	APO01 Gestionar el Marco de Gestión de TI					
	DESCRIPCION	Aclare y mantenga el gobierno de la misión y visión de TI de la empresa. Implementar y mantener mecanismos y autoridades para administrar la información y el uso de TI en la empresa en apoyo de los objetivos de gobernabilidad en línea con los principios rectores y las políticas					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	4	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	4	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	3	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	5	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	4	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**21**					

Fuente: Elaboración de las autoras

Ilustración 32 *Diagnostico de criticidad del proceso APO13*

	PROCESO	APO13 Gestionar la Seguridad					
	DESCRIPCION	Definir, operar y monitorear un sistema para la gestión de la seguridad de la información.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	3	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	5	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	5	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	4	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	4	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	3	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**24**					

Fuente: Elaboración de las autoras

Coincidencias de procesos entre Gerencia Financiera y Gerencia de TI

Una vez identificados los proceso tanto de la gerencia financiera y la gerencia de TI se puede identificar que coinciden en dos procesos entre sí:

- EDM03 Asegurar la optimización del riesgo (ISACA, 2012)
- APO13 Definir, operar y supervisar un sistema para la gestión de la seguridad de la información (ISACA, 2012)

Si profundizamos el análisis a cada uno de estos procesos podemos indicar que:

En el proceso EDM03 Asegurar la optimización del riesgo es del primer domino de Evaluar, Orientar y Supervisar, constituye a la consecución de metas relacionadas con Ti aportadas por COBIT:

- 04 riesgo de negocios relacionados con las TI gestionados (ISACA, 2012)
- 06 transparencia de los costes beneficios y riesgos de TI

En el proceso APO13 Definir, operar y supervisar un sistema para la gestión de la seguridad de la información es del segundo dominio Alinear, Planificar y Organizar, constituye a la consecución de metas relacionadas con TI por COBIT:

- 04 riesgo de negocios relacionados con las TI gestionados
- 06 transparencia de los costes beneficios y riesgos de Ti
- 10 seguridad de la Información infraestructura para el procesamiento y aplicaciones

Comprobamos la relación entre el proceso crítico y su aportación en las metas de TI, nos confirma que la gerencia de Ti está vinculada con los riesgos del negocio, como lo había definido anteriormente. La Gerencia de Ti debe enfocarse al cumplimiento de propósitos relacionados:

Salvaguardar los riesgos relacionados de Ti no excedan la tolerancia del riesgo, reduciendo al mínimo en caso de existir posibles eventualidades.

Mantener el número de acontecimientos de incidentes de la seguridad de la información en niveles de riesgos tolerables para la organización

Modelo de madurez

El propósito del modelo del modelo de madurez de las capacidades es orientar a las empresas en la selección de estrategias luego de conocer el estado actual del mismo e identificando los puntos importantes que se deben evaluar para mejorar el proceso basados inicialmente en los riesgos detectados.

Para hacer la evaluación del estado de madurez se tomó como referencia el documento Self Assessment Guide Using COBIT 5 la cual nos indica los niveles de medición:

Ilustración 33 *Modelo De Madurez COBIT 5**I***

Modelo de Madurez Cobit 5	
Modelo de Capacidad	
0. Proceso Incompleto	El proceso no se ha implementado o no ha logrado conseguir su proposito
1. Proceso Desarrollado	El proeso alcanza su proposito
2. Proceso Gestionado	El proceso esta implementado y gestionado y sus productos estan adecuadamente establecidos, controlados y mantenidos
3. Proceso Establecido	El proceso esta implementado y se usa un proceso definido que permite obtener los resultados deseados
4. Proceso Predecible	El proceso opera dentro de los limites establecidos y alcana resultados deseados
5. Proceso en optimizaciòn	El proceso es predecible y se mejora continuamente para contribuir con las metas del negocio
Mediciòn	
	Escala
N: 0% al 15%	N: No se Alcanzo
P: >15% al 50%	P: Se alcanzo parcialmente
L: >50% al 85%	L: Alcanzado en gran Medida
F: >85% al 100%	F: Totalmente Alcanzado

Fuente Self Assessment Guide Using COBIT 5

Se le realizo el análisis de madurez a los dos procesos identificados por las áreas como críticos en común con el apoyo Gerente de TI con los siguientes resultados:

Ilustración 34 *Evaluación de Madurez al Proceso EDM03 Parte 1*

Proceso	Nivel 0	Nivel 1	Nivel 2		Nivel 3		Nivel 4		Nivel 5	
EDM03		PA1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Puntuacion de los proterios		L (77.5%)	P(35%)	P (16%)						
Nivel de Madurez Conseguido										

EDM03	Asegurar la Optimizacion del Riesgo							
	Proposito	Asegúrese de que el apetito y la tolerancia al riesgo de la empresa se entiendan, articulen y comuniquen, y que se identifique y gestione el riesgo para el valor empresarial relacionado con el uso de la TI.						
	Evaluar si se consiguen los siguientes resultados	Criterios	Cumple con los Criterios S/N	Comentarios	No alcanzados (0 -15%)	Parcialmente Alcanzados (15% -50%)	Alcanzados en Gran Medida (50% - 85%)	Totalmente Alcanzados (85 % -100%)
Nivel 0 Imcompleto	El proceso no se ha implementado, o no ha logrado conseguir su proposito							
Nivel 1 Ejecutado	PA 1.1 El proceso alcanza su proposito	Los resultados del proceso estan siendo logrados						
		EDM03-01. Los riesgos que guardan relacion con TI son reconocidos , definidos y comunicados	S	La gerencia de Ti conoce los riesgos que se encuentran expuestos		70%		
		EDM03-2. EL Apetito del riesgo relacionado con empresa y las Ti es identificado y gestionado.	S	Se posee un control del riesgo cada vez que surge		85%		

Fuente: Elaboración de las autoras

Ilustración 35 *Evaluación de Madurez al Proceso EDM03 Parte 2*

EDM03	Asegurar la Optimizacion del Riesgo							
	Proposito	Asegúrese de que el apetito y la tolerancia al riesgo de la empresa se entiendan, articulen y comuniquen, y que se identifique y gestione el riesgo para el valor empresarial relacionado con el uso de la TI.						
	Evaluar si se consiguen los siguientes resultados	**Criterios**	**Cumple con los Criterios S/N**	**Comentarios**	**No alcanzados (0 -15%)**	**Parcialmente Alcanzados (15% -50%)**	**Alcanzados en Gran Medida (50% - 85%)**	**Totalmente Alcanzados (85 % -100%)**
Nivel 2 Gestionado	PA 2.1 Gestion del desempeño	Como resultado de la plena consecuciòn de esre atributo						
		a. Se identifican los objetivos para la realizacion del proceso	S	La gerencia de TI conoce los objetivos de este proceso tiene responsabilidad compartida con la GR, pero se necesita una mejore relacion de como minimizar y afrontar los problemas.		35%		
		b. Se planifica y supervisa el desempeño del proceso	N					
		c. El desempeño del proceso se ajusta para cumplir los planes	N					
		d. Se definen , asignan y comunicanlas responsabilidades y autoridades para realizar el proceso	S					
		e. Se identifican ponen a disposicion asignan y utilizan los recursos e informacion necesarios para llevar a cabo el proceso	S					

Fuente: Elaboración de las autoras

Ilustración 36 *Evaluación de Madurez al Proceso EDM03 Parte 3*

EDM03	Asegurar la Optimizacion del Riesgo							
	Proposito	Asegúrese de que el apetito y la tolerancia al riesgo de la empresa se entiendan, articulen y comuniquen, y que se identifique y gestione el riesgo para el valor empresarial relacionado con el uso de la TI.						
	Evaluar si se consiguen los siguientes resultados	**Criterios**	**Cumple con los Criterios S/N**	**Comentarios**	**No alcanzados (0 -15%)**	**Parcialmente Alcanzados (15% -50%)**	**Alcanzados en Gran Medida (50% - 85%)**	**Totalmente Alcanzados (85 % -100%)**
Nivel 2 Gestionado	PA 2.2 Gestion del Producto del trabajo	Como resultado de la plena consecucion de este atributo						
		a.Se definen los requisitos para los productos de trabajodel proceso	N	Se posee una guia de los requisitos para verificar .		16%		
		b. se definen los requisitos para la documentacion y control de los productos de trabajo.	S					
		c. los productos de trabajo se identican, documentan y controlan adecuadamente.	N					
		d. Los productos de trabajo se revisan de acuerdo con los arreglos planificados y justados según sea necesario para cumplir con los requisitos	N					

Fuente: Elaboración de las autoras

Ilustración 37 *Evaluación de Madurez al Proceso APO13 Parte 1*

Proceso	Nivel 0	Nivel 1	Nivel 2		Nivel 3		Nivel 4		Nivel 5	
APO13		PA1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Puntuacion de los proterios		L (93%)	P(50%)	P (15%)						
Nivel de Madurez Conseguido										

APO13	Gestion de Seguridad							
	Proposito	Definir, operar y monitorear un sistema para la gestión de la seguridad de la información.						
	Evaluar si se consiguen los siguientes resultados	Criterios	Cumple con los Criterios S/N	Comentarios	No alcanzados (0 -15%)	Parcialmente Alcanzados (15% -50%)	Alcanzados en Gran Medida (50% - 85%)	Totalmente Alcanzados (85 % -100%)
Nivel 0 Incompleto	El proceso no se ha implementado o no ha logrado conseguir su proposito	En este nivel, hay poco o ninguna evidencia del cumplimiento del proposito del proceso						
Nivel 1 Ejecutado	PA 1.1 El proceso alcanza su proposito	Los siguientes resultados del proceso se estan cumpliendo						
		APO13--01 Se a cominucado en la empresa el plan de seguridad y encriptamiento de lainformacion	S	Se posee con un manual de encriptamiento de informacion difundido en toda la empresa				95%
		APO13-02 Se implementa las soluciones de seguridad	S	Cada vez que surge son implementado las soluciones				91%

Fuente: Elaboración de las autoras

Ilustración 38 Evaluación de Madurez al Proceso APO13 Parte 2

APO13	Gestion de Seguridad							
	Proposito	Definir, operar y monitorear un sistema para la gestión de la seguridad de la información.						
	Evaluar si se consiguen los siguientes resultados	Criterios	Cumple con los Criterios S/N	Comentarios	No alcanzados (0 -15%)	Parcialmente Alcanzados (15% -50%)	Alcanzados en Gran Medida (50% - 85%)	Totalmente Alcanzados (85 % -100%)
Nivel 2 Gestionado	PA 2.1 Gestion del desempeño	Como resultado de la plena consecucion de este atributo						
		a. Se identifican los objetivos para la realizacion del proceso	S	Se posee el conocimiento de que se debe realizar para el cumpliento de los objetivos		50%		
		b. Se planifica y supervisa el desempeño del proceso	N					
		c. El desempeño del proceso se ajusta para cumplir los planes	N					
		d. Se definen , asignan y comunican las responsabilidades y autoridades para realizar el proceso	S					
		e. Se identifican ponen a disposicion asignan y utilizan los recursos e informacion necesarios para llevar a cabo el proceso	S					

Fuente: Elaboración de las autoras

Ilustración 39 Evaluación de Madurez al Proceso APO13 Parte 3

APO13	Gestion de Seguridad							
	Proposito	Definir, operar y monitorear un sistema para la gestión de la seguridad de la información.						
	Evaluar si se consiguen los siguientes resultados	**Criterios**	**Cumple con los Criterios S/N**	**Comentarios**	**No alcanzados (0 -15%)**	**Parcialmente Alcanzados (15% -50%)**	**Alcanzados en Gran Medida (50% - 85%)**	**Totalmente Alcanzados (85 % -100%)**
Nivel 2 Gestionado	PA 2.2 Gestion del Producto del trabajo	Como resultado de la plena consecucion de este atributo						
		a.Se definen los requisitos para los productos de trabajo del proceso	S	Se conoce los requisitos pero no siempre se ejecutan	15%			
		b. Se definen los requisitos para la documentacion y control de los productos de trabajo.	N					
		c. Los productos de trabajo se identican, documentan y controlan adecuadamente.	N					
		d. Los productos de trabajo se revisan de acuerdo con los arreglos planificados y justados según sea necesario para cumplir con los requisitos	N					

Fuente: Elaboración de las autoras

Como resultado a el análisis realizado a los procesos EDM3 Asegura la optimización del riesgo (ISACA, 2012) posee un nivel de madurez de 77.5% que se define como nivel 1 y APO13 definir, operar y supervisar un sistema para la gestión de la seguridad de la información (ISACA, 2012) posee un nivel de madurez de 93% que se define como nivel 1 es decir los dos procesos se encuentran en ejecución.

Evaluación del Riesgo Financiero Seleccionado

El proceso de elaboración de pruebas departamentales consolida mucha información de las diferentes áreas no solo de zona, sino que también a nivel de matriz.

La información es ingresada en el Sistema Core Bancario Cobis, el área requirente solicita al subgerente de contabilidad la creación de la cuenta contable y se ingresa x el sistema posterior se notifica la existencia de la cuenta al solicitante, se regulariza la transacción inconsistente el analista financiero zonal revisa y emite recomendaciones en caso de existir, si no se consolidad todas las pruebas departamentales y se remiten al área contable a nivel de matriz la cual la revisa y remite a analista financiero zonal posterior un especialista contable realiza análisis de consistencias confiabilidad y variación de saldos , partidas y se envía una vez más al analista contable de matriz para la realización de informe de pruebas departamentales el cual se remite a la subgerencia de contabilidad para la validación del informe y se solicita que se carguen en el archivo compartido finalmente se realiza la carga del archivo en las carpetas compartidas.

Análisis de Riesgos

Se procede a realizar el análisis de los riesgos detectados en el proceso de elaboración de pruebas departamentales, sus principales causas y efectos a través de información previamente identificada.

Ilustración 40 *Análisis de Riesgo Financiero Institucional Causa Efecto*

Proceso	Elaboración de Pruebas departamentales
Riesgo	Riesgo Financiero Institucional
Tipo de Riesgo	Financiero
CAUSA	**EFECTO**
Estados de cuenta fácilmente manipulables	Información de cuentas incorrectas

Fuente: Elaboración de las autoras

Podemos identificar que en el riesgo financiero se desprende que los estados de cuenta son vulnerables a la manipulación de los usuarios que descarguen, permite modificaciones al momento de realizar el informe consolidado eleva el riesgo financiero de la institución y puede ocasionar tener información equivocada sobre los estados de las cuentas.

La probabilidad de que este riesgo ocurra es mensual

Ilustración 41 *Análisis de Riesgo Falta de acciones preventivas y correctivas en la consolidación de pruebas departamentales*

Proceso	Elaboración de Pruebas departamentales
Riesgo	Falta de acciones preventivas y correctivas en la consolidación de pruebas departamentales
Tipo de Riesgo	Cumplimiento
CAUSA	**EFECTO**
Falta de Calidad de Información financiera	Informe consolidado deficiente

Fuente: Elaboración de las autoras

De la tabla anterior se desprende que la falta de supervisión adecuada para consolidar la información que es enviada por las agencias eleva el riesgo de no poder ejecutar acciones preventivas y correctivas y no tener el estado exacto de las cuentas para así poder tomar las acciones correctas.

La probabilidad de que este riesgo ocurra es mensual

Ilustración 42 *Análisis de Riesgo Perdida de Información para la toma de decisiones*

Proceso	Elaboración de Pruebas departamentales
Riesgo	Perdida de Información para la toma de decisiones
Tipo de Riesgo	Tecnológico
CAUSA	**EFECTO**
Registro incompleto al descargar el estado de cuenta	La información carece de calidad

Fuente: Elaboración de las autoras

De la tabla anterior se desprende que la falta de control al momento de descargar las transacciones por día de una cuenta en específico dentro del sistema eleva el riesgo de perder datos para toma de decisiones y esto puede ocasionar principalmente que la calidad de la información La probabilidad de que este riesgo ocurra es mensual

Podemos llegar a la consideración que para evitar los riesgos de perdida de información para la toma de decisiones en la empresa se deben mejorar los controles, asegurar que el tratamiento de la información sea el correcto, evitar la manipulación de la información fuera del sistema, calidad de registro de información, accesos controlados de las gerencias financiera y de TI.

En el desarrollo de la evaluación al proceso seleccionado de la gerencia financiera se ha podido constatar que existe un riesgo que guarda relación con TI y es de alto impacto.

- Perdida de información para la toma de decisiones

Relación proceso critico financiero y proceso de TI relacionado

A continuación, se presenta la relación de los riesgos de tipo tecnológico del proceso de elaboración de pruebas departamentales contra procesos de ti relacionadas con la gestión gerencia financiera.

Ilustración 43 *Relación procesos critico financiero y proceso de TI relacionado*

Proceso critico de la Gerencia Financiera	**Proceso de Ti relacionado con la con la Gerencia Financiera**	
Elaboración de pruebas departamentales	EDM03- Asegura la optimización del riesgo	APO-13 Gestión de la Seguridad
Alcanza parcial ente el nivel 1 de riesgo	Alcanza totalmente el nivel 1 de riesgo	
Perdida de Información para la toma de decisiones	Gerencia Financiera	Gerencia de la Tecnología de la Información
	*Subgerencia de Tesorería *Subgerencia de Contabilidad *Subgerencia de Control *Financiero Presupuestario	*Subgerente de desarrollo y mantenimiento de aplicaciones *Subgerencia de Gestión y Control *Subgerencia de Producción y Operaciones *Subgerencia de Infraestructura Tecnológica

Claramente podemos identificar que el proceso seleccionado de la gerencia financiera elaboración de pruebas departamentales guarda relación con los procesos de la gerencia de TI. Sin embargo, los niveles de riesgo que determino el análisis son buenos con respecto al resultado. A pesar de que se alcanza el nivel 1 en riesgo es recomendable que todos los procesos de gobierno posean este nivel.

Se proponen acciones de mejora para la empresa:

- Maximizar los controles en las áreas con mayor incidencia de riesgo.
- Concientización de que los riesgos relacionados con la TI son de suma importancia para los actuales y futuros proyectos de la institución.
- Controles más recurrentes para verificar la encriptación de la información.
- Crear módulos para evitar descargar la información para trabajar fuera del sistema y controlar evitando la manipulación de información.
- Crear un plan de seguridad integral
- Verificación de manuales procesos para evitar el desconocimiento de debido control de los procesos.

Resumen de Investigación

Luego de llevar a cabo como primera instancia la revisión de documentos que facilito la empresa como organigrama , estatuto orgánico gestión organizacional por procesos, manual de procesos que son de conocimiento en las gerencias evaluadas como Financiera y de Tecnología de la Información de BanEcuador B.P se realiza el análisis respectivo , de acuerdo a la guía del marco de trabajo de COBIT 5 en conjunto a la ISO27001 , las cuales buscan que las organizaciones puedan obtener un valor óptimo de sus TI manteniendo un equilibrio de beneficios, recursos y riesgos asumidos, considerando que la TI sea gobernada y gestionada de forma holística tomando en consideración la organización y áreas de punta a punta.

El objetivo de la investigación es conocer los principales procesos críticos que se presentan en la Gerencia Financiera reconociendo que un área de mayor interés en la toma de decisiones ya que la misma emite informes financieros que son necesarios para verificar el cumplimiento de la meta de la organización.

Esta investigación se realizó en función de entrevistas, observación de campo y análisis facilitados por la norma COBIT 5 a las gerencias financiera y de tecnología de la información y a sus analistas.

La gerencia financiera en investigación expuso cuales son los principales procesos que a su consideración son los más sensibles en su área

y del el mismos presento un interés mayor en un proceso definido para ser analizado y conocer los riesgos que presenta.

Una vez analizado la situación actual de BanEcuador B.P y definido del tratamiento en la auditoria, así como las gerencias involucradas se detalla el trabajo realizado.

Mediante entrevista a la gerencia financiera en conjunto a su subgerencias y analistas se toma a conocimiento de los procesos que son considerados más críticos para comenzar.

Una vez identificado el proceso en interés, se identifica las riesgos y vulnerabilidades que presenta el mismo en función a la necesidad de la organización y de la TI.

Con el conocimiento detallado y para comenzar en la integración del COBIT se presenta al gerente financiero el conocimiento de la norma con la cual se considera evaluar el proceso y se solicita su participación para desarrollar metas basados en la necesidad de este proceso en análisis basados en TI.

Al ser el marco integrador del COBIT nuestra referencia de análisis este en primera instancia busca la unificación de las metas entre la organización y las TI, una vez determinadas las metas de la gerencia financiera se las relaciona con metas de TI para conocer las relaciones que guardan y así determinar su conexión.

El COBIT presenta 37 procesos a los cuales cada área se los relacionara con la meta que poseen y se distinguir los procesos que se presentan con mayor relevancia y necesarios para el análisis.

A los procesos identificados como relevantes en el proceso de análisis en las áreas se les hará una prueba evaluando su madurez es decir qué nivel de ejecución poseen.

Continuando con el análisis comenzamos a determinar con el gerente financiero y el análisis de observación de campo cuales son los riesgos en causa y efecto que provocan que el proceso seleccionado en el área siendo de interés presente dificultades en su ejecución.

Una vez determinamos realizamos una comparación entre los niveles de madurez de los procesos y los riesgos en causa efecto para lograr comprender las necesidades que posee el área financiera que necesita que Ti cubra para lograr minimizar los riesgos encontrados y poder maximizar las metas de la organización como partes integradoras.

CONCLUSIÒN

Conclusiones y recomendaciones

Conclusiones

En el proceso de esta investigación se reconocer que las TI ayudan a las empresas a mantener un equilibrio entre la generación de beneficios y la optimización de los grados de riesgos creando un valor optimo, para convertirlo en parte importante en la toma de decisiones.

Al culminar esta investigación de evaluación de los procesos críticos de la gerencia financiera con la integración los sistemas tecnológicos de información, de BanEcuador B.P, se han cumplido con los objetivos propuestos en el presente trabajo, por lo tanto, se exponen a continuación las siguientes conclusiones y recomendaciones en torno a la realización del proyecto.

- Planificar una auditoría informática al sistema de BanEcuador B.P.

Para el desarrollo de una Auditoría Informática de los Sistemas de Información de BanEcuador B.P es de vital importancia contar con la guía de un marco de referencia. Para esta investigación se ha escogido el modelo COBIT desarrollado por ISACA en conjunto con la ISO 27001, el cual a través de sus unificaciones de metas entre gobierno y Ti, evaluación de riesgos, modelo de madurez de los procesos formaron la estructura para evaluar el proceso crítico de la gerencia financiera.

- Aplicar el estándar COBIT e ISO 27001 en la evaluación de riesgos hasta determinar el nivel de madurez de los procesos seleccionados.

La determinación de los procesos críticos en el área financiera de BanEcuador B.P., se la desarrollo en el capítulo 3 selección de procesos críticos. Con la facilitación de los manuales de procesos, entrevista realizadas, observación de campo y en conjunto con técnicas complementarias basadas con la norma integradora del COBIT unificado con la ISO 27001 se determinaron las metas relacionadas entre la gerencia financiera y TI para unificar los procesos por su nivel de criticidad y medir

sus niveles de madurez dando un valor para definir la importancia de tomar decisiones para corregir los mismos y que no surjan próximas dificultades.

- Identificación de posibles debilidades que se posean realizando un análisis de riesgo.

La identificación de las vulnerabilidades en el sistema Core Bancario Cobis, las mismas que sirvieron de ante sala para la determinación de los riegos de más importancia para el área financiera en función de los recursos de TI en función al control propuestos por COBIT se logró identificar y valorar los riesgos dentro de BanEcuador B.P para tomar las medidas pertinentes y minimizar la materialización de los riesgos identificados.

- Emitir recomendaciones para minimizar los riesgos y obtener mayor confidencialidad e integridad de la información

Se define mediante la información realizado y documentado se pudo determinar que en la actualidad BanEcuador B.P posee niveles de madurez inferiores lo cual podría llegar a un problema mayor si no se proceden a elevar el nivel de integridad de la información en la organización.

Tal como se determinó en la hipótesis una institución pública debería contar con un estándar internacional como COBIT 5 e ISO 27001 para poder medir sus riesgos y mantener el equilibrio entre beneficio, riesgo y recursos. Se puede identificar que esto se cumple ya que es recomendado en una empresa se pueda medir el nivel de riesgo que poseen y así poder mejorar los mismos para aumentar sus niveles de seguridad de la información logrando estar en niveles internacionales y poder maximizar sus beneficios como organización.

En esta investigación podemos descartar:

- En el levantamiento de información pudimos ver de primera mano que la relación que se da entre la gerencia de riesgo y la gerencia de tecnología no es la más idónea al momento de detectar una dificultad

ya que se debe realizar un proceso un poco engorroso para poder buscar una posible solución al mismo.

- La gerencia financiera pese a existir un manual de encripta miento de información y por volumen de transacciones y ejecuciones diarias no realiza este control a toda la información o lo realiza días posteriores al mismo.
- La gerencia financiera cambio su criterio entorno a la gerencia de tecnología y le dio un peso mayor para alcanzar las metas del área.

Los hallazgos más importantes en esta investigación:

- Los analistas de finanzas no tienen el conocimiento pleno de todos los procesos que manejan y cada uno de sus pasos a seguir en ocasiones existe manipulación de información evitan pasar por los controles determinados ya que el sistema les permite trabajar descanso información y luego subirla en los mismo.
- En la unificación de metas se logra desprender varios componentes que sorprendieron a las gerencias por darse cuenta de que su integración surge de la necesidad el área y son necesarias para el alcance de objetivos corporativos.
- La identificación de procesos vulnerables sirvió para determinar los riesgos más importantes en función del recurso de Ti siendo así el principio de la identificación del grado de riesgos que presenta la empresa para la toma de decisiones y de cambio oportunos.
- El levantamiento de información pudo determinar que no existe un proceso documentado que sirva para la seguridad informática financiera.
- El control de permiso según jerarquía y responsabilidades no siempre es cumplido.

El trabajo de investigación cumplió con lo establecido determinar los procesos críticos financieros de la empresa cubriendo una de sus áreas con mayor nivel de importancia, y poder darles a conocer como con las normas

internacionales establecidas se puede obtener un mejor desarrollo para optimizar los riesgos que poseen logrando integrar a las TI en las estrategias fundamentales para la toma de decisiones de la organización , buscando llegar alcanzar la visión de BanEcuador B.P que son Ser un banco líder y referente regional en servicios financieros inclusivos que aportan al desarrollo productivo rural y urbano.

Recomendación

Se ponen a consideración recomendaciones que se consideran de importancia en BanEcuador B.P tomando como referencia la investigación realizada:

- La gestión financiera se sustenta en sistemas eficaces de información que hagan posible que los procesos se lleven con calidad y veracidad a la instancia final que lo requiera. La incorporación de un modelo de gestión de seguridad información financiera permitirá controlar las actividades relacionadas de la banca pública en relación con la seguridad requerida.
- A pesar de que se identificaron el proceso crítico es recomendable que se analices esos procesos que en la investigación que por diferencias de un solo porcentaje no fueron calificadas como criticas pero que están a muy poco de convertirse y así lograr evitar posibles riesgos futuros.
- Aumentar el nivel de madurez que actualmente se encuentran los controles en la gerencia financiera.
- Se debe realizar controles más seguidos de los permisos que se posee en los programas para cada analista del área ya que en oportunidades se promueven a los analistas y no se les desactiva los anteriores permisos pudiendo convertirse en riesgos de exceso de manipulación de información.

- La gerencia de riesgo debe crear procesos menos complejos para un entendimiento más amplio de como mitigar riesgos encontrados.
- Al tener que ser el área de riesgo quien emita como mitigar el riesgo en las áreas debería contarse con un especialista de cada área para que se emitan mejores criterios de como mitigar estas dificultadas ya que en el caso de tecnologías no todo son procedimientos manuales si controles destacados en softwares.
- Se debe capacitar a cada una de las áreas para que se tome conciencia de la importancia que posee las TI en la organización y puedan en conjunto minimizar los riesgos.

Bibliografía

27001, I. (s.f.). *Es.wikipedia.org*. Obtenido de Es.wikipedia.org: https://es.wikipedia.org/wiki/ISO/IEC_27001

27001Academy. (s.f.). *27001Academy*. Obtenido de 27001Academy: https://advisera.com/27001academy/es/que-es-iso-27001/

ACHA ITURMENDI, J. J. (1996). *http://econ.unicen.edu.ar.* Obtenido de http://econ.unicen.edu.ar: http://econ.unicen.edu.ar/monitorit/index.php?option=com_docman&task=doc_view&gid=552&tmpl=component&format=raw&Itemid=10

Agudelo, G., Aigneren, M., & Ruiz , J. (2008). *DISEÑOS DE INVESTIGACIÓN EXPERIMENTAL Y NO-EXPERIMENTAL.* Obtenido de bibliotecadigital.udea.edu.co: http://bibliotecadigital.udea.edu.co/bitstream/10495/2622/1/AgudeloGabriel_disenosinvestigacionexperimental.pdf

Apredizaje, S. N. (s.f.). *Senaintro.blackboard.com*. Obtenido de Senaintro.blackboard.com: https://senaintro.blackboard.com/bbcswebdav/institution/semillas/217219_1_VIRTUAL/OAAPs/OAAP1/aa1/oa_estandarseguridad/oc.pdf

Barros Marcillo Gabriela Fernanda, C. M. (2012). Obtenido de http://repositorio.espe.edu.ec/handle/21000/5197

Bernal , C. (2010). *Metodología de la Investiagación* (Tercera edición ed.). (O. Palma Fernandez , Ed.) Colombia: Pearson.

Biegler, J. (1980). *Procedimientos administrativos.*

BRAVO, M. V. (ABRIL de 2015). *Repositorio.espam.edu.ec.* Obtenido de Repositorio.espam.edu.ec: http://repositorio.espam.edu.ec/bitstream/42000/64/1/Mar%C3%ADa%20V%C3%ADctoria%20Rivera%20Ch%C3%A1vez%20-%20Mar%C3%ADa%20Fernanda%20Zambrano%20Bravo.pdf

Burbano. (s.f.). *Presupuesto nfoque de gestion planeacion y control de recursos .* Colombia: McGraw-Hill.

Chalmers, A. (1987). *Qué es esa cosa llamada ciencia?. Una valoración de la naturaleza y el estatuto de la ciencia y sus métodos. What is this thing called science?.* (5a. ed. ed.). Madrid.: Siglo XXI.

Chavez. (2003). *Finanzas teoria aplicada para empresas .* Ecuador: Abya Yala.

COBIS. (s.f.). *Accusys.com.ve.* Obtenido de Accusys.com.ve: http://www.accusys.com.ve/MODULOS%20COBIS.pdf

Committee of Sponsoring Organizations of the treadway Commission. (2013). *Control Interno - Marco Integrado.* ISBM 978.

Corbetta, P. (2007). *Metodologia y Tecnicas de investigacion Social .* España : McGraw.

Coronel Castro, K. M. (2012). *Auditoria de Sistemas.* Loja.

Diego Ibarra Navarrete, E. P. (2014). *Implementación de un sistema de control interno basa en coso.* Guayaquil.

Escamilla Dzul, M. (2013). *Aplicación básica de los meétodos científicos " Diseño no experimental".* Obtenido de sistema de universidad virtual: https://www.uaeh.edu.mx/docencia/VI_Presentaciones/licenciatura_en_mercadotecnia/fundamentos_de_metodologia_investigacion/PRES38.pdf

Estupiñán Gaitán, R. (2006). *Control Interno y Fraudes.* Bogotá: Ecoe - Ediciones.

Fajardo, O. (28 de noviembre de 2010). *Friendly Business.* Obtenido de Friendly Business: https://fbusiness.wordpress.com/2010/11/28/las-funciones-basicas-del-area-economico-financiero/

Fernandez Muñoz, R. (2005). TIC.

Friendly Business. (s.f.). Obtenido de Friendly Business: https://fbusiness.wordpress.com/2010/11/28/las-funciones-basicas-del-area-economico-financiero/

Gerencie.com. (8 de octubre de 2017). Obtenido de Gerencie.com: https://www.gerencie.com/tipos-de-riesgos-de-auditoria.html

Gestion de Seguridad de la Informacion. (2012). *iso27000.es.* Obtenido de iso27000.es: http://www.iso27000.es/glosario.html

Giltman. (2007). *Principios de administracion financiera.* Mexico: Pearson.

Grajales, T. (2000). *Tipos de investigación. On line)(27/03/2.000). Revisado el, 14.* Obtenido de Tipos de investigación. On line)(27/03/2.000). Revisado el, 14: http://tgrajales.net/investipos.pdf

Gregorio Rodriguez Gomez, J. G. (1996). *Metodologia de la Investigacion Cualitativa.* Granada, España: Aljibe.

Grinnell Jr., R. M. (2005). *Social Work Research and Evaluation: Quantitative and Qualitative Approaches.* New York: Cengage Learning.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (1997). *Metodologia de la investiacion* (Vol. primera edicion). Mexico: McGRAW - HILL INTERAMERICANA DE MÉXICO, S.A. de C.V. Obtenido de file:///C:/Users/Usuario/Downloads/metodologia%20de%20la%20investigacion%201era%20edicion-sampieri.pdf

Hernandez, R., Fernanfez, C., & Baptista, P. (2004). *Metodología de la Investigación.* Mexico DF: Mc Graw Hill.

IFRS Foundation. (2015). *NIIF para las Pymes.* Reino Unido.

INCONTEC. (2013). *NTC-ISO/IEC 27001.* Colombia.

International Organization for Standardization. (2016). *ISO/IEC 27000.*

Investopedia. (s.f.). *Investopedia.* Obtenido de Investopedia: https://www.investopedia.com/terms/i/internalcontrols.asp

ISACA. (2012). *COBIT 5 FRAMEWORK.* Estados Unidos.

ISO 27001:2013. (s.f.). *Ing. Manuel Collazos Balaguer*.

Laudon, K. C., & Laudon, J. P. (2012). Sistemas de Informacion Gerencial. En K. C. Laudon, & J. P. Laudon, *Sistemas de Informacion Gerencial* (pág. 40). Mexico: Pearson.

Ltd, A. E. (s.f.). *27001Academy*. Obtenido de 27001Academy: https://advisera.com/27001academy/es/que-es-iso-27001/

Luna, O. F. (2013). *Sistemas de control interno para organizaciones.* IICO (Instituto de Investigación en Accountability y Control). Recuperado el 2 de Diciembre de 2017

Luna, Y. B. (2012). *Auditoria Integral Normas y procedimientos.* Bogota, Colombia: Ecoe Ediciones.

Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. *International Journal of Morphology*.

MAR&Iacute, A., & A., A. L. (s.f.). *FUNDAMENTOS DE ISO 27001 Y SU APLICACIÓN EN LAS EMPRESAS.* Obtenido de Redalyc.org: http://www.redalyc.org/html/849/84921327061/

Marta Alelú Hernández, S. C. (s.f.). *Uam.es.* Obtenido de Uam.es: https://www.uam.es/personal_pdi/stmaria/jmurillo/InvestigacionEE/Presentaciones/Curso_10/ENCUESTA_Trabajo.pdf

Melo, I. (3 de octubre de 2014). *Auditoriaunidad1.blogspot.com.* Obtenido de Auditoriaunidad1.blogspot.com: http://auditoriaunidad1.blogspot.com/2014/

MUNARRIZ, B. (s.f.). Obtenido de http://ruc.udc.es/dspace/bitstream/handle/2183/8533/CC-02art8ocr.pdf

Muñoz, C. (2002). *Auditoria en Sistemas Computacionales.* Mexico: pearson Education.

ORTIZ. (2005). *Gerencia financiera y Diagnostico Financiero.* Colombia: McGraw-Hill.

Paredes, Y. C. (mayo de 2015). Obtenido de file:///C:/Users/Usuario/Downloads/CD-6237%20(1).pdf

Ramos, P. (5 de abril de 2017). *Profesion.es.* Obtenido de Profesion.es: https://www.profesion.es/departamento-financiero/

Razo, C. m. (2002). *Auditoria en Sistemas computacionales.* (G. T. Mendoza, Ed.) Mexico: Person Educaciòn. Recuperado el 2018, de https://cdryst.files.wordpress.com/2009/10/aussist.pdf

RIVAS, G. A. (1989). *http://econ.unicen.edu.ar.* Obtenido de http://econ.unicen.edu.ar: http://econ.unicen.edu.ar/monitorit/index.php?option=com_docman&task=doc_view&gid=552&tmpl=component&format=raw&Itemid=10

Romero, J. (31 de Agosto de 2012). *Control interno y sus 5 componentes según COSO.* Obtenido de Control interno y sus 5 componentes

según COSO: https://www.gestiopolis.com/control-interno-5-componentes-segun-coso/

Romero, S. C. (s.f.). *Auditoria Informática.* Obtenido de Sites.google.com: https://sites.google.com/site/aisadith/unidad-1

Romero, S. C. (s.f.). *Sites.google.com.* Obtenido de Sites.google.com: https://sites.google.com/site/aisadith/unidad-1

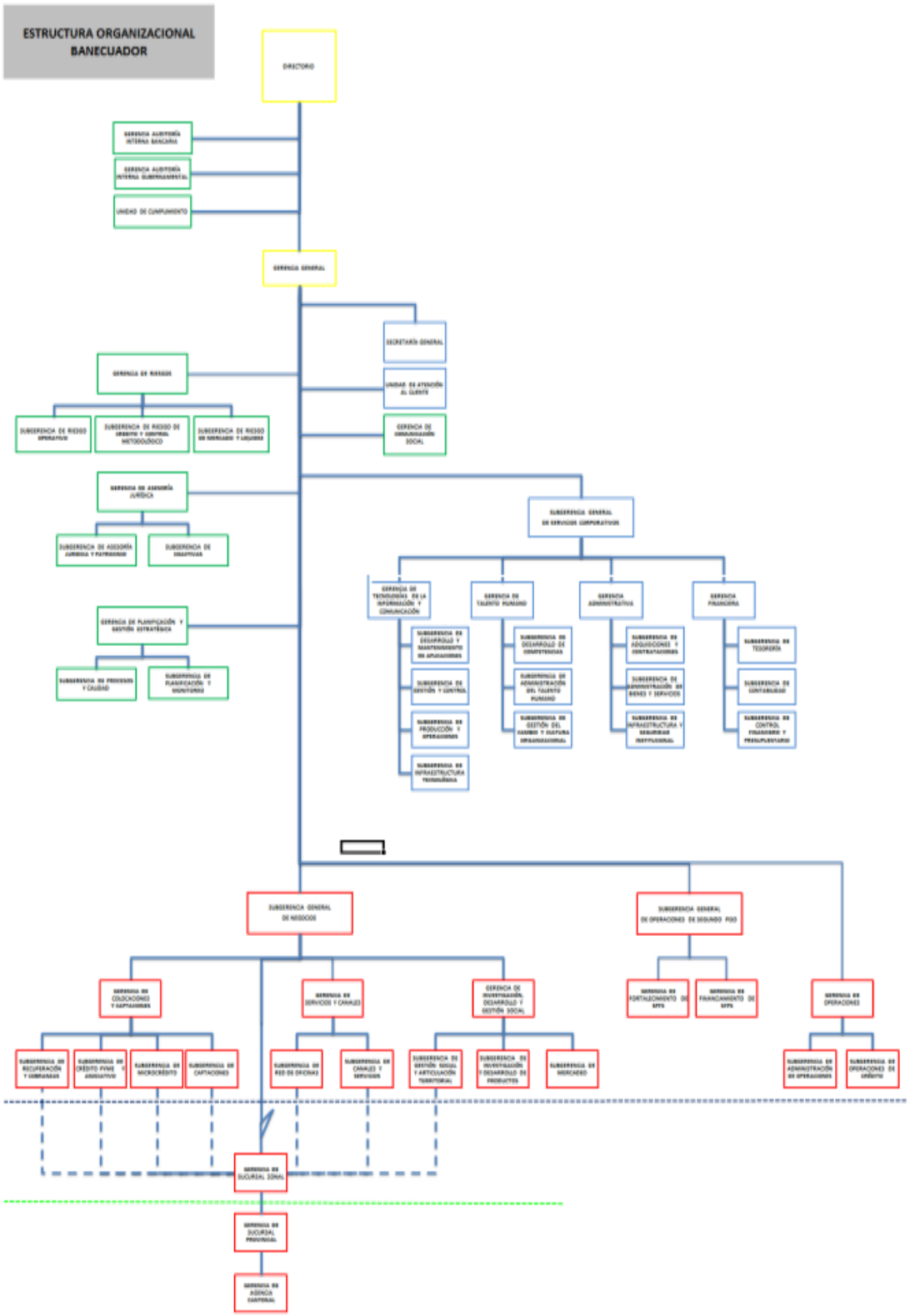
Rosas, R. (9 de febrero de 2012). *Axeleratum.com.* Obtenido de Axeleratum.com: http://axeleratum.com/2012/ipara-que-sirve-el-area-de-finanzas-en-la-empresa/

Tesis de Investigacion . (2013). Obtenido de http://tesisdeinvestig.blogspot.com/2013/06/tipos-de-investigacion-segun-tamayo-y.html

Walter, r. f. (2011). *Redalyc.org.* Obtenido de Redalyc.org: http://www.redalyc.org/pdf/4139/413940770004.pdf

ANEXOS

Anexo 1 Estructura Organizacional BANECUADOR B.P



ANEXO 2 Procesos Críticos Gerencia Financiera Parte 1

		Unificacion de Informacion de la Gerencia Financiera	Maximizaciòn de la eficiencia de la Gerencia Financiera	Aseguramiento de controles de la Gerencia Financiera	Optimización de la productividad de la Gerencia Financiera	Seguridad de la información de la Gerencia financiera
Evaluar , Orientar y Super visar	EDM01 Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	S		S		S
	EDM02 Asegurar la Entrega de Beneficios		S		S	
	EDM03 Asegurar la Optimizacióndel Riesgo		P	P		P
	EDM04 Asegurar la Optimizaciónde los Recursos			S		
	EDM05 Asegurar la Transparenciahacia las partes interesadas	S				
Alinear , Planificar y Organizar						
	APO01 Gestionar el Marco de Gestión de TI			S		
	APO02 Gestionar la Estrategia		S			
	APO03 Gestionar la Arquitectura Empresarial				S	
	APO04 Gestionar la Innovación	S				
	APO05 Gestionar el portafolio			S		
	APO06 Gestionar el Presupuesto ylos Costes					S
	APO07 Gestionar los Recursos Humanos			S		
	APO08 Gestionar las Relaciones					S
	APO09 Gestionar los Acuerdos de Servicio	S				
	APO10 Gestionar los Proveedores					
	APO11 Gestionar la Calidad	P	P			P
	APO12 Gestionar el Riesgo	P	P			P
	APO13 Gestionar la Seguridad	P		P	P	

ANEXO 2 Procesos Críticos Gerencia Financiera Parte 2

Construcción, Adquisición e Implementación	BAI01 Gestionar los Programas y Proyectos	P		P		P
	BAI02 Gestionar la Definición de requisitos				S	
	BAI03 Gestionar la Identificación y		S			
	BAI04 Gestionar la Disponibilidad y la capacidad	S				
	BAI05 Gestionar la introducción de cambios organizativos			S		
	BAI06 Gestionar los Cambios					
	BAI07 Gestionar la Aceptación del cambio y de la transicion	S				
	BAI08 Gestionar el Conocimiento				S	
	BAI09 Gestionar los Activos		S			
	BAI10 Gestionar la Configuración	S				
Entregar , dar Servicio y Soporte						
	DSS01 Gestionar las Operaciones			S		
	DSS02 Gestionar las Peticiones ny los incidentes del servicio				S	
	DSS03 Gestionar los Problemas	S				
	DSS04 Gestionar la Continuidad					
	DSS05 Gestionar los Servicios de Seguridad	P	P			P
	DSS06 Gestionar los Controles de lo sprocesos del negocio	P		P		
Supervisión, Evaluación y Verificación						
	MEA01 Supervisar, Evaluar y Valorar Rendimientoy conformidad	S				
	MEA02 Supervisar, Evaluar y Valorar el sistema de control interno			S		
	MEA03 Supervisar, Evaluar y Valorar la conformidad con los requerimientos externos		S			S

ANEXO 3 Procesos Críticos de la Gerencia TI

	PROCESO	EDM04 Asegurar la Optimizaciónde los Recursos					
	DESCRIPCION	Asegurar que las capacidades adecuadas y suficientes relacionadas con TI (personas, procesos y tecnología) estén disponibles para apoyar los objetivos de la empresa de manera efectiva a un costo óptimo.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	4	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	3	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	3	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	5	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**19**					

	PROCESO	EDM05 Asegurar la Transparencia hacia las partes interesadas					
	DESCRIPCION	Asegúrese de que el rendimiento de TI de la empresa y la medición e informe de conformidad sean transparentes, y que las partes interesadas aprueben los objetivos, las métricas y las medidas correctivas necesarias					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	5	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	2	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	2	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	4	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	2	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**18**					

	PROCESO	APO02 Gestionar la Estrategia					
	DESCRIPCION	Proporcione una visión holística del entorno empresarial y de TI actual, la dirección futura y las iniciativas necesarias para migrar al entorno futuro deseado. Aproveche los componentes y componentes básicos de la arquitectura empresarial, incluidos los servicios proporcionados externamente y las capacidades relacionadas para permitir una respuesta ágil, confiable y eficiente a los objetivos estratégicos.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	4	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	2	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	3	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	2	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	4	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**16**					

	PROCESO	APO03 Gestionar la Arquitectura Empresarial					
	DESCRIPCION	Mejore la alineación, aumente la agilidad, mejore la calidad de la información y genere ahorros de costos potenciales a través de iniciativas tales como la reutilización de componentes de bloques de construcción.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	5	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	3	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	3	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	5	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**20**					

	PROCESO	APO04 Gestionar la Innovación					
	DESCRIPCION	Mantener un conocimiento de la tecnología de la información y las tendencias de los servicios relacionados, identificar oportunidades de innovación y planificar cómo beneficiarse de la innovación en relación con las necesidades del negocio					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	4	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	2	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	3	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	3	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	4	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**17**					

	PROCESO	APO05 Gestionar el portafolio					
	DESCRIPCION	Evaluar, priorizar y equilibrar programas y servicios, gestionar la demanda dentro de los recursos y las limitaciones de fondos, en función de su alineación con los objetivos estratégicos, el valor y el riesgo de la empresa.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	3	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	2	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	4	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	3	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	3	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**16**					

	PROCESO	APO06 Gestionar el Presupuesto y los Costes					
	DESCRIPCION	Consulte a las partes interesadas para identificar y controlar los costos y beneficios totales dentro del contexto de los planes estratégicos y tácticos de TI, e inicie acciones correctivas cuando sea necesario.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	2	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	4	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	3	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	2	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	3	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**15**					

	PROCESO	APO07 Gestionar los Recursos Humanos					
	DESCRIPCION	Proporcionar un enfoque estructurado para garantizar una estructuración óptima, colocación, derechos de decisión y habilidades de recursos humanos. Esto incluye comunicar las funciones y responsabilidades definidas, los planes de aprendizaje y crecimiento y las expectativas de rendimiento, respaldados por personas competentes y motivadas.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	2	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	4	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	3	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	2	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	4	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	3	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**18**					

	PROCESO	APO08 Gestionar las Relaciones					
	DESCRIPCION	Administre la relación entre el negocio y las TI de una manera formal y transparente que asegure un enfoque en lograr un objetivo común y compartido de resultados empresariales exitosos en apoyo de los objetivos estratégicos y dentro de la restricción de presupuestos y tolerancia al riesgo					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	2	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	5	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	3	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	2	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	4	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	3	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**19**					

	PROCESO	APO09 Gestionar los Acuerdos de Servicio					
	DESCRIPCION	Alinee los servicios y niveles de servicio habilitados por TI con las necesidades y expectativas de la empresa, incluida la identificación, especificación, diseño, publicación, acuerdo y supervisión de servicios de TI, niveles de servicio e indicadores de rendimiento					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	2	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	2	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	3	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	2	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	4	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	3	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**16**					

	PROCESO	APO10 Gestionar los Proveedores					
	DESCRIPCION	Administre los servicios relacionados con TI proporcionados por todo tipo de proveedores para cumplir con los requisitos de la empresa, incluida la selección de proveedores, la gestión de relaciones, la administración de contratos y la revisión y el monitoreo del desempeño del proveedor para su efectividad y cumplimiento.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	3	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	3	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	3	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	4	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**17**					

	PROCESO	APO11 Gestionar la Calidad					
	DESCRIPCION	Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y los resultados empresariales relacionados, incluidos los controles, el monitoreo continuo y el uso de prácticas y estándares comprobados en esfuerzos de mejora continua y eficiencia.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	3	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	3	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	3	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	3	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	3	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**18**					

	PROCESO	APO12 Gestionar el Riesgo					
	DESCRIPCION	Identifique, evalúe y reduzca continuamente el riesgo relacionado con TI dentro de los niveles de tolerancia establecidos por la gerencia ejecutiva de la empresa.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	3	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	3	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	4	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	4	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	3	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**20**					

	PROCESO	BAI01 Gestionar los Programas y Proyectos					
	DESCRIPCION	Administre todos los programas y proyectos de la cartera de inversiones en alineación con la estrategia empresarial y de forma coordinada. Iniciar, planificar, controlar y ejecutar programas y proyectos, y cerrar con una revisión posterior a la implementación					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	3	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	3	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	3	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	3	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**16**					

	PROCESO	BAI02 Gestionar la Definición de requisitos					
	DESCRIPCION	Coordinar con las partes interesadas afectadas la revisión de las opciones factibles, incluidos los costos y beneficios relativos, el análisis de riesgos y la aprobación de los requisitos y las soluciones propuestas.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	2	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	3	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	2	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	3	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**14**					

	PROCESO	BAI03 Gestionar la Identificación y la Construcción de Soluciones					
	DESCRIPCION	Administre la configuración, la preparación de pruebas, las pruebas, la administración de requisitos y el mantenimiento de procesos					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	3	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	3	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	2	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	2	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**14**					

	PROCESO	BAI04 Gestionar la Disponibilidad y la capacidad					
	DESCRIPCION	Equilibre las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una prestación de servicios rentable. Incluya la evaluación de las capacidades actuales, la previsión de las necesidades futuras en función de los requisitos del negocio, el análisis de los impactos del negocio y la evaluación del riesgo para planificar e implementar acciones para cumplir con los requisitos identificados.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	2	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	2	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	3	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	2	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**13**					

	PROCESO	BAI05 Gestionar la introducción de cambios organizativos					
	DESCRIPCION	Maximice la probabilidad de implementar con éxito cambios organizativos sostenibles en toda la empresa de forma rápida y con riesgos reducidos, cubriendo el ciclo de vida completo del cambio y todas las partes interesadas afectadas en el negocio y la TI.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	3	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	2	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	2	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	3	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	2	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**13**					

	PROCESO	BAI06 Gestionar los Cambios					
	DESCRIPCION	Administre todos los cambios de forma controlada, incluidos los cambios estándar y el mantenimiento de emergencia relacionados con procesos comerciales, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, evaluación de impacto, priorización y autorización, cambios de emergencia, seguimiento, informes, cierre y documentación					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	3	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	3	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	3	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	3	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**16**					

	PROCESO	BAI07 Gestionar la Aceptación del cambio y de la transicion					
	DESCRIPCION	Acepte formalmente y haga nuevas soluciones operativas, incluida la planificación de implementación, conversión de datos y sistemas, pruebas de aceptación, comunicación, preparación de versiones, promoción a producción de procesos comerciales y servicios de TI nuevos o modificados, soporte de producción inicial y una revisión posterior a la implementación.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	2	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	2	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	2	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	3	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	2	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**12**					

	PROCESO	BAI08 Gestionar el Conocimiento					
	DESCRIPCION	Mantener la disponibilidad de conocimiento relevante, actual, validado y confiable para apoyar todas las actividades del proceso y facilitar la toma de decisiones. Planifique la identificación, recopilación, organización, mantenimiento, uso y retiro del conocimiento.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	3	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	2	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	2	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	3	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	2	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	3	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**15**					

	PROCESO	BAI09 Gestionar los Activos					
	DESCRIPCION	Administre licencias de software para garantizar que el número óptimo se adquiera, conserve e implemente en relación con el uso comercial requerido, y que el software instalado cumpla con los acuerdos de licencia.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	3	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	2	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	2	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	2	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	2	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**12**					

	PROCESO	BAI10 Gestionar la Configuración					
	DESCRIPCION	Defina y mantenga descripciones y relaciones entre los recursos clave y las capacidades necesarias para entregar servicios habilitados por TI, incluida la recopilación de información de configuración, el establecimiento de líneas de base, la verificación y auditoría de la información de configuración y la actualización del depósito de configuración					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	2	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	2	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	2	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	3	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	3	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**13**					

	PROCESO	DSS01 Gestionar las Operaciones					
	DESCRIPCION	Coordinar y ejecutar las actividades y los procedimientos operativos necesarios para prestar servicios de TI internos y externos, incluida la ejecución de procedimientos operativos estándar predefinidos y las actividades de supervisión requeridas.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	3	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	3	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	2	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	3	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**15**					

	PROCESO	DSS02 Gestionar las Peticiones ny los incidentes del servicio					
	DESCRIPCION	Proporcione una respuesta oportuna y efectiva a las solicitudes de los usuarios y la resolución de todo tipo de incidentes. Restaurar el servicio normal; registrarse y cumplir con las solicitudes de los usuarios; y registrar, investigar, diagnosticar, escalar y resolver incidentes.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	3	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	2	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	5	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	3	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	3	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**17**					

	PROCESO	DSS03 Gestionar los Problemas					
	DESCRIPCION	Identifique y clasifique los problemas y sus causas principales y proporcione una resolución oportuna para evitar incidentes recurrentes. Proporcione recomendaciones para mejoras					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	3	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	3	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	5	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	3	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**18**					

	PROCESO	DSS04 Gestionar la Continuidad					
	DESCRIPCION	Establecer y mantener un plan para permitir que el negocio y la TI respondan a incidentes e interrupciones a fin de continuar la operación de los procesos comerciales críticos y los servicios de TI requeridos y mantener la disponibilidad de la información en un nivel aceptable para la empresa					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	3	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	5	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	3	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	3	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	3	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**18**					

	PROCESO	DSS05 Gestionar los Servicios de Seguridad					
	DESCRIPCION	Proteja la información de la empresa para mantener el nivel de riesgo de seguridad de la información aceptable para la empresa de acuerdo con la política de seguridad. Establezca y mantenga roles de seguridad de información y privilegios de acceso y realice monitoreo de seguridad					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	4	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	5	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	4	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	3	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**20**					

	PROCESO	DSS06 Gestionar los Controles de lo sprocesos del negocio					
	DESCRIPCION	Define and maintain appropriate business process controls to ensure that information related to and processed by in-house or outsourced business processes satisfies all relevant information control requirements. Identify the relevant information control requirements and manage and operate adequate controls to ensure that information and information processing satisfy these requirements.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	4	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	5	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	4	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	3	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**20**					

	PROCESO	MEA01 Supervisar, Evaluar y Valorar Rendimiento y conformidad					
	DESCRIPCION	Reúna, valide y evalúe los objetivos y las métricas empresariales, de TI y de procesos. Supervise que los procesos funcionen según los objetivos y las metas de cumplimiento y cumplimiento acordados y proporcione informes que sean sistemáticos y oportunos					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	4	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	5	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	3	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	3	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**19**					

	PROCESO	MEA02 Supervisar, Evaluar y Valorar el sistema de control interno					
	DESCRIPCION	Supervise y evalúe continuamente el entorno de control, incluidas autoevaluaciones y revisiones independientes de seguridad. Permita que la administración identifique las deficiencias e ineficiencias de control e inicie acciones de mejora. Planifique, organice y mantenga estándares para evaluaciones de control interno y actividades de aseguramiento					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	4	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	4	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	3	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	3	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**18**					

	PROCESO	MEA03 Supervisar, Evaluar y Valorar la conformidad con los requerimientos externos					
	DESCRIPCION	Evalúe que los procesos de TI y los procesos comerciales respaldados por TI cumplen con las leyes, las reglamentaciones y los requisitos contractuales. Obtenga la seguridad de que se han identificado y cumplido los requisitos e integre el cumplimiento de TI con el cumplimiento general de la empresa.					
No.	PREGUNTA	VALOR	1	2	3	4	5
1	En cuanto influye para el éxito de la empresa el proceso	5	No es importante	Se puede Obviar	Facilita las cosas	Muy significativo	Critico
2	El proceso se desempeña bien	3	Todo se hace siempre bien	En parte se hace bien	Algunas cosas a veces se hacen bien	Algunos aspectos algunas veces	Algunos aspectos raramente
3	Esta claro quien debe responder por los resultados finales	4	Si, todo el mundo lo sabe	Alguien que sabe y lo acepta	Alguien que sabe pero no toma accion	Alguien lo asume asi	No esta totalmente claro
4	El proceso es medido	3	Las mediciones existen y estan integradas y ligadas a los objetivos de TI y del negocio	Se mide eficiencia y efectividad no se liga con objetivo	Algunas medidas de efectividad	Algunas medidas financieras	No del Todo
5	El proceso tiene debilidades de contro conocida	3	Continuamente monitoreadas y mitigadas	Continuamente monitoreadas y mitigadas	Reconocidas pero aun no tratadas	Hay conciencia de que hay que hacer algo al respecto	No se sabe acerca de las debilidades de control
6	Quien lo realiza	1	IT	Otro interno	tercero	no del todo definido	No sabe
	Criticidad	**19**					

ANEXO 4 Carta de Autorización BanEcuador B.P

BanEcuador

Guayaquil, 05 de Octubre del 2017

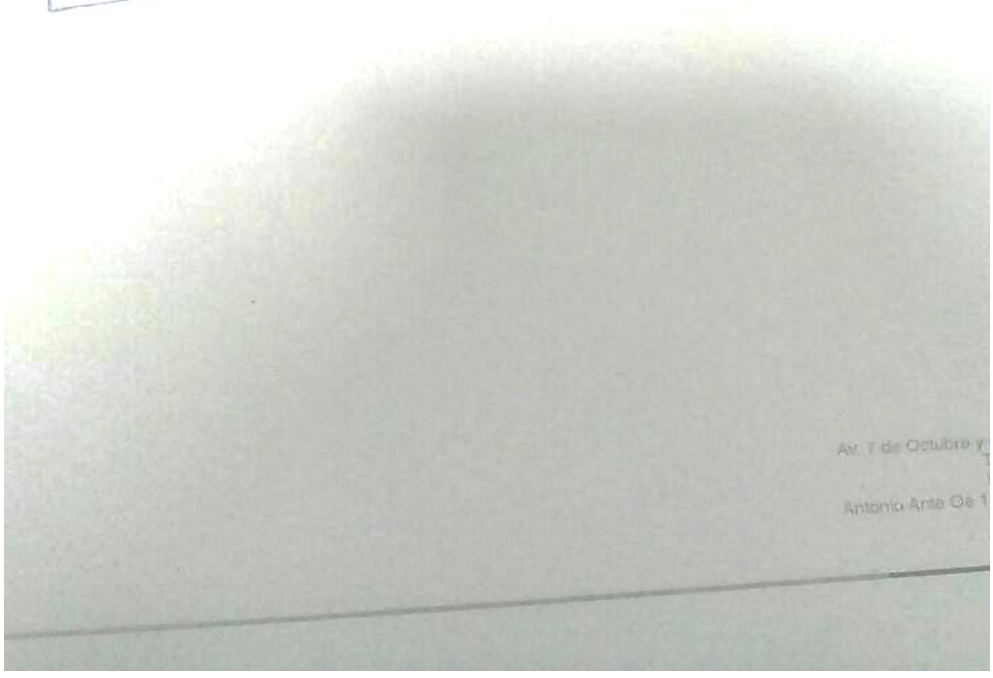
Señores
Universidad Católica Santiago de Guayaquil
Facultad de Ciencias Económicas y Administrativas
Ciudad.-

Por medio de la presente se autoriza a la Sra. Zambrano Gonzalez Stephanie Katherine con C.I: 0923676894, el uso de los manuales del Departamento Financiero y Departamento de Tecnología y Seguridad de la información, de Banecuador B.P., los mismos que serán utilizados en el proceso de la elaboración y sustentación de la Tesis:
"Auditoria informática soportada por COBIT e ISO 27001 en las instituciones financieras públicas de la ciudad de Guayaquil"

Banecuador B.P. queda a disposición de solventar cualquier encuesta a realizarse en base a la tesis mencionada.

Atentamente,

Mgs. David Peralta Cantó
Analista Financiero MR. Zonal
Coordinación Financiera Zonal Guayaquil



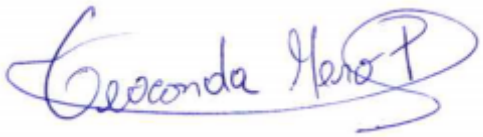
DECLARACIÓN Y AUTORIZACIÓN

Yo, **Mero Paredes , Geoconda Desire** con C.C: # **0927207142** autora del trabajo de titulación: **"Auditoria Informática soportada por COBIT e ISO 27001 en las instituciones financieras públicas de la ciudad de Guayaquil."** previo a la obtención del título de Ingeniero en Contabilidad y Auditoría, CPA en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, Marzo del 2018



f_____

Mero Paredes, Geoconda Desire

C.C: 0927207142

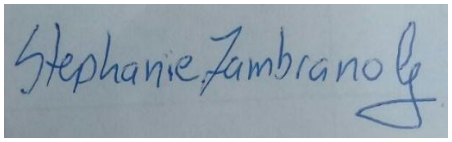
DECLARACIÓN Y AUTORIZACIÓN

Yo, **Zambrano González Stephanie Katherine,** con C.C: # **0923676894** autora del trabajo de titulación: **"Auditoria Informática soportada por COBIT e ISO 27001 en las instituciones financieras públicas de la ciudad de Guayaquil"** previo a la obtención del título de Ingeniero en Contabilidad y Auditoría, CPA en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, marzo del 2018



f. _____

Zambrano González Stephanie Katherine

C.C: 0923676894

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Auditoria Informática soportada por Cobit e ISO 27001 en las instituciones financieras públicas de la ciudad de Guayaquil		
AUTOR(ES)	Mero Paredes Geoconda Desire y Zambrano González Stephanie Katherine		
REVISOR(ES)/TUTOR(ES)	Ing. Fabián Andrés Delgado Loor		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Ciencias Económicas y Administrativas		
CARRERA:	Contabilidad y Auditoría, CPA		
TITULO OBTENIDO:	Ingeniero en Contabilidad y Auditoría, CPA		
FECHA DE PUBLICACIÓN:	Marzo del 2018	**No. DE PÁGINAS:**	(154 páginas)
ÁREAS TEMÁTICAS:	Contabilidad- Auditoria de Sistemas		
PALABRAS CLAVES/ KEYWORDS:	Auditoria de Sistemas, Integración, Riesgos, Vulnerabilidades, Procesos.		

RESUMEN/ABSTRACT : El siguiente trabajo de titulación describe la Auditoría Informática que se le realizará al Sistema Core Bancario Cobis en BanEcuador B.P, a su Gerencia Financiera, utilizando los estándares internacionales, ISO 27001 el cual sirve para especificar los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) basado en el ciclo de mejora continua en conjunto con COBIT que es una herramienta desarrollada para auditar la gestión y control de los sistemas de información.
Primero se definirán los principales conceptos de la auditoria informática, ISO 27001, COBIT y del área financiera, posterior y en conjunto con la identificación de la metodología a plantear y pasos a seguir, mediante el análisis de la información y ejecución de las técnicas de investigación se desprenderán los resultados de cuáles son los principales procesos críticos y la conexión de estos con el área de TI, evaluando su nivel de madurez, logrando identificar las debilidades que se corren en la organización por no tener mejores controles que permitan minimizar los riesgos.
Finalmente se emitirán conclusiones y recomendaciones para ser tomadas en consideración por BanEcuador B.P.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-0996624820/ +593-0989058516	**E-mail:**desiremero@hotmail.com, skatherine.zambrano@gmail.com
CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE):	**Nombre:** Yong Amaya, Linda Evelyn	
	Teléfono: +593-4- 3804600 ext.1635	
	E-mail: linda.yong@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	