UNIVERSIDAD HISPANOAMERICANA

CONTADURÍA PÚBLICA

Tesis para optar por el grado académico de licenciatura en Contaduría Pública

ANÁLISIS DE LAS ACTIVIDADES DE CONTROL ACTUALES EN MATERIA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DE LA COMPAÑÍA ACEITERA EL COCO S.A COMO APOYO PARA EL LOGRO DE LOS OBJETIVOS ESTRATÉGICOS CORPORATIVOS VIGENTES EN EL AÑO 2020

AUTOR: MICHAEL UMAÑA RODRÍGUEZ

FEBRERO, 2020

INDICE DE CONTENIDO

INDICE DE TABLAS

ÍNDICE DE FIGURAS

DEDICATORIA

Dedico este trabajo a la memoria de mi abuela María Luisa Rodríguez, quien me inspira, aún en su ausencia, a valorar todo lo que la vida me brinda y cuyo ejemplo de dedicación y esfuerzo ha calado en mí para hacerme una mejor persona en la vida profesional y familiar.

También quiero dedicarlo a mis hijos, Ximena y Fabian cuya vida recién inicia en el proceso educativo. Que este logro sirva como motivación y muestra de mi apoyo incondicional en los procesos que les espera.

AGRADECIMIENTOS

Agradezco primero que todo a Dios, por darme la oportunidad de lograr una meta más en mi vida, a pesar de las desavenencias y mi testarudez para hacer las cosas.

A mi mamá, por haberme brindado la oportunidad de estudiar porque en medio de las adversidades siempre me apoyó.

A mi esposa Nataly, compañera de vida, amiga incondicional y apoyo permanente que no me permite caer y siempre está para mí.

A todos los profesores que de una u otra forma han contribuido a ser el profesional que soy.

RESUMEN

La Compañía Aceitera El Coco S.A, es una empresa consolidada que próximamente cumplirá 70 años de su creación y que a lo largo del tiempo ha incursionado en toda la cadena productiva y de comercialización de grasas y aceites tanto para consumo humano como para la alimentación animal; esta institución quiere avanzar a la velocidad con que los tiempos actuales se desarrollan.

Sin embargo, la organización no cuenta con un planteamiento estratégico y estandarizado sobre la gestión de las tecnologías de información. Esto ha generado algunos inconvenientes en los procesos que la empresa desarrolla pues no existe un marco de control interno ideal que permita brindar seguridad y confianza de los datos que los sistemas generan.

Este trabajo final de graduación, propone acciones que fomenten el desarrollo de una estructura de control interno alineada a marcos de referencia conocidos que buscan reducir riesgos de tecnologías de información y educar sobre las mejores prácticas que garanticen el buen desempeño de las operaciones para el alcance de los objetivos.

Se recomienda a la compañía, analizar la presente propuesta y que sirva como guía para establecer lineamientos de control interno en el campo de las tecnologías de información y que a la vez sean comunicados a toda la organización con el propósito de la creación de un plan estratégico corporativo.

Palabras clave: Tecnologías de Información, Control Interno, riesgo, COBIT, seguridad.

ABSTRACT

Compañía Aceitera El Coco S.A, is a consolidated company that will soon turn 70 years of its creation and that over time has ventured into the entire production and marketing chain of fats and oils for both human consumption and animal feed; this institution wants to advance at the speed with which current times develop.

However, the organization does not have a strategic and standardized approach to the management of information technology. This has generated some inconveniences in the processes that the company develops since there is no ideal internal control framework that allows providing security and confidence in the data that the systems generate.

This final graduation project proposes actions that promote the development of an internal control structure aligned to known reference frameworks that seek to reduce information technology risks and educate on the best practices that guarantee the good performance of operations for the scope of the objectives.

It is recommended that the company analyze this proposal and that it serves as a guide to establish internal control guidelines in the field of information technologies and that at the same time be communicated to the entire organization with the purpose of creating a strategic plan corporate.

Keywords: Information Technology, Internal Control, risk, COBIT, security.

CAPÍTULO I

INTRODUCCIÓN

1.1 PLANTEAMIENTO DEL PROBLEMA

En los siguientes apartados se presentan los antecedentes, problemática y fundamento del problema que motivan esta investigación.

1.1.1 Antecedentes internacionales y nacionales

Desde hace algunas décadas, el manejo de la información se ha identificado como un factor determinante en los cambios políticos, económicos, culturales y, además, en las relaciones internacionales y de seguridad de la gran mayoría de países; es decir: el motor de la globalización.

La convergencia de los diferentes procesos mencionados se hace más aguda debido a la conectividad de hoy que, impulsa la gran transformación del siglo XXI.

Los avances informáticos y en telecomunicaciones convierten al mundo en una “aldea” global donde, el intercambio de información, junto con el tránsito de personas, bienes y capitales contribuyen en gran escala con una nueva forma de organización mundial.

Las empresas alrededor del mundo viven una integración de sus operaciones con la finalidad de alcanzar objetivos individuales asociados a objetivos comunes por sectores y/o categorías; no obstante, estas relaciones no deben correr el riesgo de sacrificar la seguridad de sus datos.

Con fundamento en lo anterior, han prosperado compañías que brindan seguimiento desde hace años al comportamiento y evolución de las Tecnologías de Información y Comunicación (TIC´s) donde su foco de atención ha sido la seguridad de datos.

Para el año 2009, el Estudio sobre la Privacidad de los Datos Personales y la Seguridad de la Información en las Redes Sociales Online, realizado en España por el Instituto Nacional de Tecnologías de la Comunicación y la Agencia Española de Protección de Datos estableció que entre el 40% y 50% de la población usuaria de internet emplea habitualmente redes sociales y el 44,6% de los internautas españoles cuentan con algún perfil en una red social.

Si consideramos que la tercera edición del estudio *Power to the People Social Media, Wave 3* de Universal McCann en marzo 2008 posicionó en 272 millones de personas a los usuarios de redes sociales, lo que supone un aumento de 21% respecto a junio 2007; tanto los datos sensibles de una empresa como a título personal son vulnerables.

En 2012, Verizon publicó a través de *Background Check* un estudio realizado durante ocho años a más de 2000 brechas de seguridad en más de mil millones de registros que, indicó que el 97% de los incidentes ocurridos podrían haber sido evitados con controles de niveles simples o intermedios; el 69% de las brechas de seguridad ocurrieron debido a infecciones por malware y el 85% de los incidentes ocurridos tardan varias semanas en ser detectados.

La Encuesta Global de Seguridad de la Información 2015 realizada por la firma *Price Waterhouse Cooper* (PwC) a nivel mundial del 07 de mayo al 12 de junio, dictaminó que año tras año los ataques cibernéticos aumentan en un 38% aproximadamente, razón por la cual, el 91% de los encuestados ha optado por un marco de ciberseguridad basado en riesgo y que la tendencia es utilizar servicios de ciberseguridad basados en la nube.

Para el año 2017, Deloitte realizó la primera edición de su estudio de Seguridad de la Información Ecuador 2017 donde aproximadamente el 50% de las empresas participantes sufrió alguna brecha de seguridad en los últimos 12 meses y el 20% de ellas no logró determinar el impacto de dicha brecha; siendo esto sumamente llamativo debido a que ocho de cada diez empresas cuentan con un responsable de seguridad de la información (CISO – *Chief Information Security Officer*).

La Encuesta Global de Seguridad de la Información 2018, ejecutada por PwC Argentina a empresas en el país sudamericano arrojó que el 40% de los encuestados señala la interrupción de las operaciones como la mayor preocupación durante un ataque cibernético, seguido en 39% por el compromiso de datos confidenciales y en menor medida daños a la calidad de productos, propiedad física y perjuicio de la vida humana; a pesar de esto, el 44% de los encuestados no posee una estrategia general de seguridad de la información.

En este mismo año, los expertos de *SearchInform* prepararon el primer estudio sobre el nivel de seguridad de la información de las empresas latinoamericanas durante una serie de conferencias *Road Show SearchInform 2018 "Money Loss Prevention: La protección del futuro"*, que permitió identificar que el 53% de los incidentes se debe a contagios de virus en las computadoras ocasionados en el 60% de los casos por empleados regulares de las compañías.

Este panorama, nos invita a mirar hacia el interior del país y determinar qué tanto pueden hacer nuestras autoridades gubernamentales y los diferentes gobiernos corporativos del sector privado para blindar los datos que utilizan y almacenan con los gustos y preferencias de los usuarios de servicios y consumidores de bienes.

El Estudio Global de Seguridad 2018 elaborado por la Unión Internacional de Telecomunicaciones (UIT), que involucra a expertos de diferentes profesiones y organizaciones, coloca a Costa Rica en el lugar 115 (de 173) del ranking global y en el puesto 18 a nivel regional del continente americano denotando así que se han realizado esfuerzos en materia de seguridad informática, pero con un bajo nivel de compromiso.

El pasado mes de noviembre del año 2019, la Contraloría General de la República publicó un informe sobre la seguridad de los centros de datos que utiliza el Ministerio de Hacienda y uno de los principales hallazgos fue que cerca de 5000 cuentas de usuarios activas no corresponden a funcionarios del Ministerio de Hacienda, lo que "*pone en riesgo la confidencialidad e integridad de la información, procesada y almacenada en sistemas críticos".*

Aunado a esto, la situación se agrava, ya que se determinó en el mismo informe que desde el año 2013 no se ejecutaban actualizaciones de seguridad en los servidores del Ministerio, lo que quedó al descubierto al encontrar 2672 vulnerabilidades, de las cuales 2160 se consideraron como críticas.

En Costa Rica, de acuerdo con datos de la compañía Fortinet, en el primer trimestre del año 2019 se recibió un total de 19 millones de intentos de ataques informáticos; la mayoría de los ataques son *ramsonware, phishing* y *malware*.

1.1.2 Delimitación del Problema

En concordancia con el contexto anterior, se considerará los cinco componentes del sistema de control interno de la instancia bajo estudio, con la intención de conocer y analizar las políticas y procedimientos actuales relacionados con las tecnologías de información y comunicación (TIC), para el aseguramiento de la información general y datos sensibles comparativos. La investigación se realizará durante el primer semestre del 2020 en las Oficinas Centrales de la empresa ubicadas en Costa Rica, provincia de San José, Cantón Central, Distrito Hospital.

1.1.3 Justificación

Las nuevas y amplias leyes de privacidad de datos, que recalcan todavía más los derechos del usuario de un uso adecuado de los datos, suponen un desafío para las empresas y entidades de hoy, que tienen más datos, aplicaciones y ubicaciones que nunca.

Estos datos se han transformado en un activo cada vez más valioso y constituyen la columna vertebral de las perspectivas del mercado y de los clientes, de las ofertas de productos y servicios y de las operaciones cotidianas. Esto es especialmente cierto a medida que las organizaciones amplían su propuesta digital y su modelo de negocio.

Los sistemas de información son determinantes en la productividad; a la vez, mejoran la capacidad de análisis para toma de decisiones y la implementación de soluciones para la prestación de servicios ágiles y de gran alcance. Por eso las Tecnologías de la Información y Comunicación (TIC), deben gestionarse bajo políticas y procedimientos aplicables y vigentes que faciliten el logro de objetivos

alineados con la estrategia de la organización. Si el control interno es efectivo en términos de seguridad de la información, permite a cualquier organización optimizar recursos, mejorando los procesos de negocio y comunicación para lograr las metas con más facilidad.

Garantizar la seguridad de la información a través de la confidencialidad, la disponibilidad y la integridad de los datos se constituye en el objetivo principal que deben asumir las empresas a través del establecimiento de estrategias donde se redacten las políticas de actuación para cada uno de estos tres aspectos.

La presente investigación pretende aportar el conocimiento de las mejores prácticas que se pueden adoptar para proteger la información y garantizar la continuidad del negocio sin comprometer el activo más importante de nuestra era.

Con la investigación se verá beneficiada la Compañía Aceitera El Coco S.A por cuanto se hará aportes para el fortalecimiento general de su Sistema de Control Interno y en específico, del cuarto componente de éste: Sistemas de Información; por medio de la revisión e identificación de oportunidades de mejora en las actividades de control en materia de tecnologías de la información y comunicación.

La integralidad del control interno conlleva que la gestión de las tecnologías de la información responda a un marco más amplio, en el cual, la organización adopta una filosofía de trabajo a nivel macro, que en este caso es el Sistema de Control Interno como tal; situación que, a pesar de su complejidad, reviste de gran relevancia para la organización y constituye un reto académico invaluable para este servidor.

Asimismo, la propuesta de las medidas de mejora para las actividades de control en materia de Tecnologías de Información y Comunicación, aportará una base teórica para que la Compañía Aceitera El Coco S.A pueda sentar mejores bases para su gestión gerencial y de las actividades de fiscalización.

1.2 PREGUNTA DE INVESTIGACIÓN

¿Brindan las actuales actividades de control en materia de tecnologías de información y comunicación de la Compañía Aceitera El Coco S.A. un nivel razonable de seguridad de la información en forma que contribuyan al logro de los objetivos estratégicos corporativos?

1.3 OBJETIVOS

1.3.1 Objetivo General

Evaluar la existencia y oportunidades de mejora en las actividades de control en materia de tecnologías de la información y comunicación de la Compañía Aceitera El Coco S.A. que permitan apoyar el logro de los objetivos estratégicos corporativos durante el ejercicio del periodo 2020.

1.3.2 Objetivos Específicos

1. Determinar el nivel actual de cada uno de los componentes del sistema de control interno.

2. Analizar los procedimientos actuales de control de la sección de Tecnologías de Información.

3. Establecer la vinculación existente entre las actividades de control en materia de tecnologías de información y comunicación con el logro de los objetivos estratégicos corporativos.

4. Valorar el grado de satisfacción y seguridad de los usuarios de los sistemas de información.

5. Proponer medidas de mejora para las actividades de control en materia de Tecnologías de Información y Comunicación

CAPÍTULO II

MARCO TEÓRICO

2.1 CONTEXTO HISTÓRICO

2.1.1 Contexto histórico del objeto de estudio

El desarrollo paulatino de la Compañía Aceitera El Coco S.A. se remonta a la década de los años 30, cuando la *United Fruit Company* se traslada al pacífico húmedo e inicia la sustitución de los cultivos de banano, por cultivos de palma africana, cacao, reforestaciones de teca, implementación de módulos ganaderos y comercialización de granos básicos.

Con el cierre de sus fincas, la Compañía Bananera de Costa Rica impulsa y promueve el cultivo de palma aceitera en el país y se convierte en el principal suplidor de material genético (semillas de planta aceitera) para siembras en América Latina.

Simultáneamente, un inversionista estadounidense radicado en Costa Rica, fundó en 1951 la Compañía Aceitera El Coco S.A., con sede en Barrio Luján. Transcurre el tiempo y ocho años más tarde, se adquieren los terrenos actuales, instalándose en ellos, la planta productora.

El establecimiento y desarrollo de los cultivos de palma, eliminó la importación de materias primas desde Malasia para la producción de mantecas y otros productos. En ese entonces, existía en el país la fábrica de Aceites Garrido y Llovera, líderes en ese campo; al mismo tiempo se competía con productos de la empresa *Unilever* y de *Panamerican Standart Brand*. Poco a poco, El Coco S.A gana la preferencia del consumidor y al consolidarse en el mercado impulsa la diversificación de grasas

y aceites vegetales, destacándose la manteca y el aceite Clavel; así como, la fabricación de insumos para la industria alimentaria y jabonera.

La Compañía expande su ámbito de acción al exportar sus productos a los países de Centroamérica, debido a la apertura del mercado común centroamericano. De esta forma, *Clavel* y *Goldmar* se consolidan como marcas de prestigio dentro de la región.

En 1965, la *United Fruit Co.* compra la Compañía El Coco S.A y se funda en Costa Rica el Grupo Palmeras S.A., integrando varias empresas relacionadas con el cultivo, extracción, procesamiento y manufactura de grasas y aceites vegetales.

En 1995, el Grupo Palmeras es adquirido por un conjunto de inversionistas costarricenses y extranjeros con amplia experiencia en la producción de grasas y aceites. Los nuevos accionistas inician un plan agresivo de siembra de palma africana y de exportación de aceite de palma fuera de Centroamérica. Actualmente, el Grupo Palmeras está constituido por cuatro compañías.

Consciente de su papel en el desarrollo económico y social de Costa Rica, la empresa ofrece un ambiente de trabajo seguro que brinda confianza a sus trabajadores y a la comunidad; respetando la legislación vigente y sus principios empresariales.

Unos de los principios fundamentales que rigen el funcionamiento de la empresa es la utilización de tecnología de punta, con ello, se asegura de ofrecer productos de excelente calidad que satisfagan las necesidades y gustos de sus clientes. La

constante inversión en nuevos equipos, la capacitación de sus colaboradores, el uso de las mejores materias primas y los estrictos controles de calidad distinguen a las plantas de producción de El Coco.

Por otra parte, atendiendo los requerimientos del mercado, El Coco S.A, invierte en su propia planta de plásticos, permitiendo la diversificación de presentaciones e incrementando su competitividad. Además de ser una fuente de empleo y producción para la sociedad costarricense, contribuye a mejorar la calidad de vida de los habitantes del país fomentando el deporte, la educación y la salud, para mantener el equilibrio que permite una vida sana.

En la actualidad nuestro mundo se convierte en un entorno cada vez más dinámico y las empresas no escapan a la transformación y acondicionamiento de sus políticas internas para brindar excelencia en sus procesos y ante esta coyuntura, El Coco ha establecido siete valores que fundamentan su operación:

a. Innovación

b. Servicio

c. Respeto

d. Calidad

e. Pasión

f. Seguridad

g. Adaptabilidad

Este conjunto de virtudes, acompañadas de colaboradores visionarios hacen que cada día la empresa crezca y se consolide como un agente de cambio mediante el alcance de sus metas, el equilibrio financiero y una actitud ganadora ante los desafíos que establece el mercado y la competencia.

Considerando que la economía evoluciona hacia el conocimiento y las habilidades de alto nivel, el capital humano con que se cuente es vital para la organización. El Coco S.A. adopta una visión estratégica de crecimiento constante, que se materializa con la siguiente estructura organizacional:

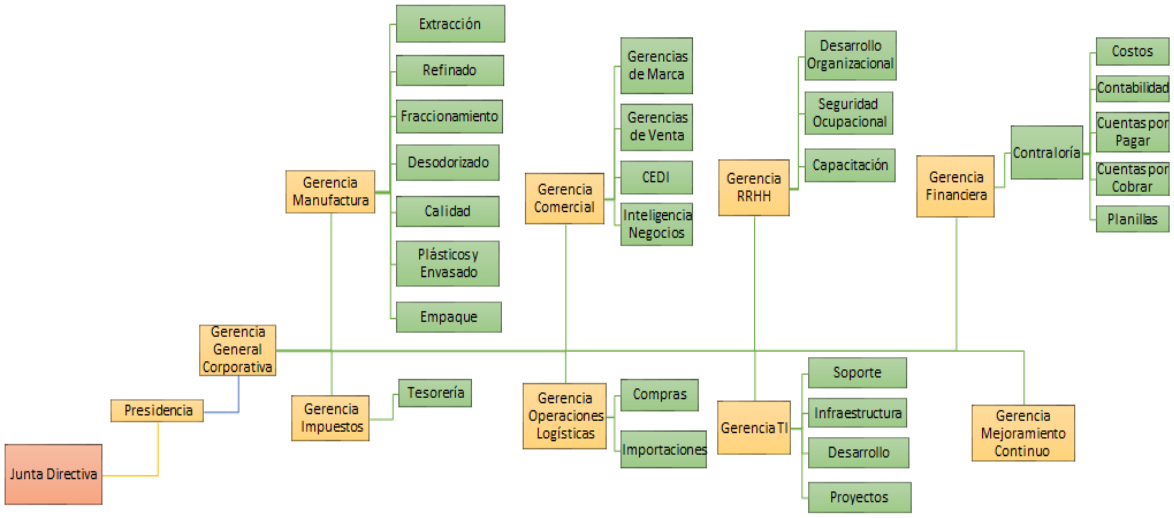

Figura 1: Organigrama Empresarial

Fuente: Elaboración propia

2.2 CONTEXTO TEÓRICO – CONCEPTUAL

2.2.1 Control Interno

Con base en las consecuencias de la Revolución Industrial del siglo XVIII; es decir, a partir de la revolución tecnológica, la transformación de la geopolítica global, la interdependencia económica a escala global, las relaciones entre economía, estado y sociedad, donde el estado regula los mercados, genera competencia a nivel global, y deja de ser estado de bienestar, y finalmente, una reestructuración interna de capitalismo; emergió una sociedad postindustrial que está llamada a vigilar que las operaciones financieras en las compañías de la época sean correctas.

Para esta finalidad, el control interno, se convertiría en la principal herramienta que se ha haya desarrollado en la primera mitad del siglo XX y en adelante le corresponderá a los Contadores independientes aplicarlo para el examen de los estados financieros.

Y la importancia de este concepto quedaría evidenciado en los años setenta con tres sucesos que llamaron la atención a nivel mundial:

- El Escándalo *Watergate* de 1972 en Estados Unidos, donde se intentó robar documentos de la sede del Comité Nacional Demócrata y vio involucrado al presidente de dicho país en aquel entonces: Richard Nixon.

- Creación del Comité de Basilea sobre Supervisión Bancaria en respuesta a la quiebra de un banco alemán que había generado una gran crisis en el sistema financiero internacional.

- El informe de la SEC (*Securities and Exchange Commission*) de Estados Unidos en 1976, que hacía referencia a prácticas cuestionables de grandes corporaciones en el exterior.

A partir de estas y otras circunstancias históricas el Comité de Organizaciones Patrocinadoras de la Comisión *Treadway* (COSO, por sus siglas en inglés) publicó el Marco Integrado de Control Interno, a través del cual es posible evaluar el riesgo y la efectividad de los sistemas de control interno.

El control interno ha sido diseñado, aplicado y considerado como la herramienta más importante para el logro de los objetivos, la utilización eficiente de los recursos y para obtener la productividad, además de prevenir fraudes, errores violación a principios y normas contables, fiscales y tributarias.

Se entiende entonces por Control Interno: "… el sistema integrado por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas u objetivos previstos." (Isaza, A. (2018), Control Interno y Sistema de Gestión de Calidad, Colombia, Ediciones de la U)

Independientemente de la naturaleza de la entidad, sea esta pública o privada, son responsables directos del sistema de control interno todos los integrantes de la misma, pues es la única forma de garantizar la eficiencia total en la aplicación.

2.2.2 Objetivos del Control Interno

Todo sistema de control interno debe estar enfocado hacia el logro de los siguientes objetivos:

a) Obtener la información financiera oportuna, confiable y suficiente como herramienta útil para la gestión y el control.

b) Promover la obtención de la información técnica y otro tipo de información no financiera para utilizarla como elemento útil para la gestión y el control.

c) Procurar adecuadas medidas para la protección, uso y conservación de los recursos financieros, materiales, técnicos y cualquier otro recurso de propiedad de la entidad.

d) Promover la eficiencia organizacional de la entidad para el logro de sus objetivos y misión.

e) Asegurar que todas las acciones institucionales en la entidad se desarrollen en el marco de las normas constitucionales, legales y reglamentarias.

El control interno se fundamenta en la protección a través de todos los instrumentos pertinentes, la cobertura adecuada de las posibles contingencias y la verificación de los sistemas de preservación y registro.

Es común que, al terminar la implementación del sistema de control interno debe realizarse un análisis con una retroalimentación continua para encontrar posibles fallas y controlarlas lo más rápido posible y así evitar situaciones de gran impacto.

2.2.3 Componentes del Control Interno

La estructura del control interno es una amalgama de políticas y procedimientos que implementa la entidad para asegurar que cada una de las metas que se propone sean alcanzadas con la mayor seguridad, respetando la legislación vigente y en el menor tiempo posible; por lo que, se hace necesario segregar sus componentes para que cada colaborador siga las directivas implementadas por la administración.

Todo proceso, incluido el control interno, es dinámico e integral, por lo tanto, aunque sus componentes se describen y analizan de forma independiente, no constituye un proceso lineal en el que una falla en alguno de los mismos afecta únicamente al siguiente. Más bien, la deficiencia en uno solo de dichos componentes afecta a todo el sistema.

Entonces, el control interno consta de cinco componentes a saber:

2.2.3.1 Ambiente de Control

El ambiente de Control constituye un factor intangible de suma importancia en todas las actividades de la entidad. En ocasiones no se le brinda la debida atención, no obstante, es fundamental dentro de la gestión de riesgo.

Este componente se dirige a los métodos y estilo en el que las iniciativas de control interno son implementadas, constituyéndose en el valor que la dirección brinda a la función de la auditoría y la forma en que se administran los riesgos. Provee disciplina y estructura e incide en la manera como:

i. Se estructuran las actividades del negocio.

ii. Se asigna autoridad y responsabilidad

iii. Se organiza y se desarrolla el recurso humano.

iv. Se comunican los valores y creencias del negocio.

v. El personal toma conciencia de la importancia del control.

Es por lo anterior, que es de gran influencia en cómo se desarrollan las operaciones, se establecen los objetivos y se minimizan los riesgos e igualmente en el comportamiento de los sistemas de información y la supervisión general.

Algo tan sencillo como la estructura organizacional, formalizada a través de un organigrama, constituye el marco de autoridad y responsabilidad en el cual las actividades que se desarrollan en cumplimiento de los objetivos del organismo son planeadas, efectuadas y controladas.

El ambiente de control debe ser constantemente evaluado a través del conocimiento y aceptación consciente de las normas escritas, comprobando que las respuestas sean eficientes y contundentes en los casos de actuaciones no conformes con la reglamentación establecida y vigilando que todos los procedimientos contribuyan adecuadamente al mejoramiento continuo del sistema de control implementado.

Un ambiente de control óptimo debe estar dirigido a obtener:

- Operaciones eficientes y eficaces
- Confiabilidad de la Información Financiera
- Cumplimiento de las leyes, regulaciones y las normas aplicables.
- Reducción en las pérdidas

- Salvaguardar los recursos disponibles

2.2.3.2 Evaluación de Riesgos

Se denomina riesgo al impacto y probabilidad de que una amenaza o serie de ellas puedan afectar de manera adversa la consecución de los objetivos.

Desde el punto de vista de un inversionista se podría considerar las siguientes categorías de riesgo:

- Riesgos estratégicos: riesgos tanto para los objetivos estratégicos como de los objetivos estratégicos. La alta gerencia identifica los riesgos más importantes a través del proceso de planificación y obtiene aprobación de la Junta.
- Riesgos Operativos: grandes riesgos que afectan la habilidad de la organización para lograr el plan estratégico.
- Riesgos Financieros: incluyen información financiera, valoración, cobertura, riesgos de mercado y liquidez y riesgos de crédito en instituciones financieras.
- Riesgos de Cumplimiento: riesgos no compensados, generalmente el foco principal para las actividades de gestión de riesgo empresarial.

El Control Interno ha sido pensado esencialmente para limitar los riesgos que afectan las actividades de la entidad. A través de la investigación y análisis de los riesgos relevantes y el punto hasta el cual el control vigente los neutraliza, se evalúa la vulnerabilidad del sistema.

Para ello debe adquirirse un conocimiento práctico de la entidad y sus componentes como manera de identificar los puntos débiles, enfocando los riesgos tanto de la entidad (internos y externos) como de la actividad.

Los pasos a seguir para la evaluación de riesgos se pueden concentrar en cuatro fases:

a) Identificación del riesgo: es un proceso interactivo e integrado a la estrategia y planificación. Su desarrollo comprende la realización de un análisis de riesgo que incluya los puntos clave del organismo, la identificación de los objetivos generales y particulares por la naturaleza del negocio y las amenazas y riesgos que pueden afrontar.

b) Estimación del Riesgo: esta estimación comprende tres variables; probabilidad, impacto y velocidad; con estas consideraciones se puede construir una matriz de riesgos para determinar los riesgos prioritarios. La importancia de cada riesgo en su control interno se basa en la probabilidad de manifestación y en el impacto que puede causar en la organización. La velocidad del riesgo se refiere a la rapidez con la que el impacto se evidenciará en la entidad. El impacto se refiere a la pérdida de activos y de tiempo, la disminución de la eficiencia y eficacia de las actividades, los efectos negativos en los recursos humanos, y la alteración de la exactitud de la información de la organización, entre otras.

c) Determinación de los objetivos de control: se debe establecer los objetivos específicos de control de la entidad, que estarán adecuadamente articulados

con los objetivos globales y sectoriales; en función de estos, se adoptarán las medidas o salvaguardas que se estimen más efectivas al menor costo para minimizar la exposición.

d) Detección del Cambio: los indicadores clave de riesgo representan medidas que indican la presencia potencial, estado o tendencia de una condición de riesgo; si estos indicadores fueron diseñados y utilizados correctamente, las métricas de riesgos tienen un valor de predicción y pueden actuar como alertas tempranas para permitir acciones anticipadas.

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

2.2.3.3 Actividades de Control

Las actividades de control se definen como las acciones establecidas a través de las políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la administración para mitigar los riesgos con impacto potencial en los objetivos.

Son ejecutadas en todos los niveles de la entidad, en todas las etapas de los diferentes procesos del negocio y en el entorno tecnológico; pueden ser preventivas o de detección y pueden abarcar una amplia gama de actividades manuales y automatizadas.

Sin embargo, lo trascendente es que, sin importar su tipo, todas apuntan hacia el riesgo, real o potencial, en beneficio de la organización no sólo porque implican hacer las cosas correctamente, sino que son el medio idóneo de asegurar en mayor grado el logro de objetivos.

Existen normas básicas que se encuentran incluidas dentro de las actividades de control que son:

- Separación de tareas y responsabilidades.
- Coordinación entre áreas.
- Documentación.
- Niveles definidos de autorización.
- Registro oportuno y adecuado de las transacciones y hechos.
- Acceso restringido a los recursos, activos y registros.
- Rotación del personal en las tareas claves.
- Control del sistema de información.
- Control de la tecnología de información.
- Indicadores de desempeño.
- Función de auditoría interna independiente.

En todos los niveles de la entidad existen responsabilidades de control y es preciso que todos los agentes conozcan individualmente cuáles son las que les competen.

2.2.3.4 Información y Comunicación

Son los métodos utilizados para entrenar a la población de colaboradores en referencia a las actividades de control. Los sistemas de información y comunicación se entrelazan ayudando al personal de la entidad a capturar e intercambiar información relevante para conducir, administrar y controlar sus operaciones.

Esta información debe ser captada y transmitida oportunamente a todos los actores de forma que permita asumir las responsabilidades individuales, deben ser especificadas con claridad y fomentar además un ambiente adecuado para una comunicación abierta y efectiva.

Es importante que la dirección disponga de datos fiables, a la hora de efectuar la planificación, preparar presupuestos, y demás actividades. Es por esto que la información debe ser de calidad y tener en cuenta los siguientes aspectos:

- ✓ Contenido: ¿Presenta toda la información necesaria?
- ✓ Oportunidad: ¿Se facilita en el tiempo adecuado?
- ✓ Actualidad: ¿Está disponible la información más reciente?
- ✓ Exactitud: ¿Los datos son correctos y fiables?
- ✓ Accesibilidad: ¿La información puede ser obtenida fácilmente por las personas adecuadas?

La comunicación interna es el medio utilizado para la difusión a través de toda la organización y debe fluir en todo sentido tanto ascendente, descendente y a todos

los niveles de la misma, esto hace que los colaboradores reciban un mensaje claro desde la alta dirección sobre las responsabilidades de control.

Pero, la información no viaja sólo internamente; desde el exterior la comunicación tiene dos funciones: extraer datos de interés hacia el interior y proporcionar información interna en respuesta a las necesidades y expectativas de grupos de interés externos.

La comunicación puede y debe materializarse en manuales de políticas, avisos, mensajes de vídeo y la actuación de la dirección debe ser ejemplo para el personal de la entidad.

Fuentes de datos internos	Datos internos
• Comunicaciones por correo – email • Inspecciones del procesamiento de la planta de producción. • Minutas o notas de los encuentros del comité operativo. • Sistema de reporte en tiempo del personal. • Reportes de los sistemas de fabricación. • Respuestas a las encuestas de clientes. • Líneas directas para informantes	• Cambios organizacionales • Experiencias de producción de calidad y a tiempo. • Acciones en respuesta a las métricas de consumo de energía. • Horas incurridas en proyectos basados en tiempo. • Número de unidades enviadas en un mes. • Factores que impactan en las tasas de deserción de clientes. • Quejas del comportamiento del administrador.
Fuentes de datos externos	**Datos externos**
• Datos recibidos de los proveedores de servicios externos. • Reportes de investigación de la industria • Publicación de ganancias de compañías del mismo sector • Entes regulatorios • Medios sociales y blogs • Ferias • Líneas directas para informantes	• Productos enviados por manufactura contratada. • Información de productos competitivos • Métricas del mercado y la industria • Requerimientos nuevos o ampliados • Opiniones acerca de la entidad • Evolución de las preferencias de clientes • Declaraciones de uso incorrecto de fondos o sobornos.

Figura 2: Elementos de Comunicación

Fuente: https://www.auditool.org/blog/control-interno/3194-sistema-de-informacion-y-comunicacion-coso-iii-principio-13

Las organizaciones desarrollan además sistemas de información para obtener, capturar y procesar grandes cantidades de datos desde fuentes internas como externas para convertirlos en información significativa y procesable con el fin de cumplir con los requerimientos definidos de información. Estos sistemas de información implican una combinación de personal, datos y tecnología que apoyan los procesos del negocio.

Para estos sistemas existen controles generales y controles de aplicación, los cuales se detallan de la siguiente manera:

a) Controles Generales: su propósito es asegurar una operación y continuidad adecuada e incluyen al control sobre el centro de procesamiento de datos y seguridad física, contratación y mantenimiento de hardware y software, así como la operación propiamente dicha, además se relacionan con funciones de desarrollo y mantenimiento de sistemas, soporte técnico y administración de bases de datos.

b) 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 y cubren las aplicaciones destinadas a las interfaces con otros sistemas de los que se reciben o entregan información.

Definitivamente, los sistemas de información y tecnología son y serán un medio para incrementar la productividad y competitividad.

2.2.3.5 Supervisión o Monitoreo

Todo proceso debe ser sometido a un escrutinio que permita desarrollar el concepto de mejoramiento continuo. Es decir, mantener las acciones diarias que permitan a la entidad y sus procesos ser más competitivos en la satisfacción del cliente, ya sea este interno o externo.

Las actividades de supervisión y monitoreo deben evaluar si los componentes y principios están presentes dentro de la compañía y si estos funcionan correctamente.

El resultado de estas actividades, debe conducir a identificar controles débiles, que no son suficientes u obsoletos, con la intención de promover siempre de la mano del gobierno corporativo, la actualización y establecimiento de mejoras.

El proceso de evaluación puede llevarse a cabo de tres formas a saber:

a) Durante la realización de actividades diarias en todos los niveles de la organización.

b) A través de personal que no es responsable directo de la ejecución de las actividades.

c) Combinación de las dos anteriores.

Dentro del marco de supervisión o monitoreo existen diferentes normas que se deben considerar:

a) Evaluación del Sistema de Control Interno: mediante la aplicación de las evaluaciones periódicas se garantiza la tranquilidad de un funcionamiento

adecuado, la oportunidad de corrección y fortalecimiento mediante el análisis de resultados.

b) Eficacia del Sistema de Control Interno: se considera eficiente el sistema en la medida en que la autoridad a la que apoya tenga una seguridad razonable en la información sobre el avance en el logro de objetivos y metas, la confiabilidad y validez de la información y por último el cumplimiento de la legislación y normativa vigente.

c) Auditorías del Sistema de Control Interno: permiten obtener una opinión técnica válida del estado y funcionamiento del sistema, proporcionando además recomendaciones para su fortalecimiento en caso que corresponda.

d) Tratamiento de las Deficiencias Detectadas: consiste en comunicar a través de un informe las debilidades y oportunidades del sistema, debe estar dirigido hacia quienes son los propietarios y responsables de su operación, con la finalidad de que implementen las acciones necesarias.

   En la medida en la que se establezca el nivel de importancia para las debilidades identificadas, la magnitud del riesgo existente y la probabilidad de que ocurra, se determinará el nivel al cual se deben escalar las deficiencias.

2.1.2 Tecnología de la Información y Comunicación (TIC)

Son el resultado de enlazar la interacción de la informática y las telecomunicaciones con la finalidad de mejorar el procesamiento, almacenamiento y transmisión de la información.

Hacen uso de una serie de recursos para dar tratamiento a los datos a través de una serie de dispositivos electrónicos, aplicaciones informáticas y redes que permiten convertirlos en información relevante para la toma de decisiones oportunas en la operación de una entidad.

Un sistema de información es eficaz cuando facilita la información necesaria para la información y será eficiente cuando alcance ese resultado con los menores recursos tecnológicos, humanos y económicos posibles en el momento oportuno.

2.1.2.1 Composición de las Tecnologías de la Información y Comunicación

Muchas son las herramientas de las cuales se hacen las TIC para brindar el amplio abanico de soluciones que las empresas buscan hoy, y para tener claridad de las mismas se procederá con la determinación de algunos conceptos que pueden resultar familiares en la cotidianidad pero que muchos desconocen.

- Software: es el conjunto de componentes lógicos necesarios que hacen posible la realización de tareas específicas.
- Hardware: conjunto de componentes tangibles que integran una computadora.

- Internet: es un conjunto de redes de comunicación interconectadas que utilizan diferentes reglas de comunicación llamadas protocolos de forma tal que permiten realizar un alcance global de información.
- Servidor: es una aplicación en ejecución capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.
- Sistema operativo: es el software principal que gestiona los recursos de hardware y provee servicios a los programas de aplicación.
- *E-commerce:* consiste en la compra y venta de productos o servicios a través de los medios electrónicos que utilizan las TIC.
- Redes Sociales: es un conjunto de personas con intereses compartidos que interactúan a través de un medio virtual.
- Nube: red mundial de servidores remotos que están conectados para funcionar como un único ecosistema a través de internet.

Desde la perspectiva de estos conceptos, las tecnologías de información y comunicación aportan un valor a la empresa; ya que, a nivel de información pueden reducir costos y mejorar el flujo de la misma. A nivel de infraestructura de la empresa mejora la comunicación y relaciones personales de los trabajadores lo que tiene un impacto a nivel comercial también donde permite extender el mercado a través del comercio electrónico, reduciendo costos logísticos y facilitando la retroalimentación por parte del cliente, lo que a su vez permite mejorar la imagen de una marca.

En medio de este mar de oportunidades que generan las TIC en beneficio de las personas y las empresas, también han fomentado la dispersión de la información provocando desordenes de contenido fomentando la ignorancia y la irresponsabilidad de muchos.

A raíz de esto, han surgido también amenazas que se pueden determinar a través de otros conceptos como:

- *Malware:* son programas maliciosos que realiza acciones dañinas en un sistema informático de forma intencional.
- Virus: Código malicioso tipo huésped que se aloja en ficheros ejecutables y tiene la propiedad de reproducirse.
- Troyano: programa de apariencia inofensivo que permite tomar el control de manera remota para realizar instalación de otros programas.
- *Spyware*: programa que permite enviar información a terceros sin que el usuario principal se percate.
- *Phishing*: técnica de suplantación de identidad que persigue engañar a una víctima para que brinde información sensible.
- Ingeniería Social: práctica de obtener información confidencial a través de la manipulación de los usuarios legítimos.

La combinación de estas variables son un arma para la ciberdelincuencia que cada día desarrolla ataques a nivel personal y empresarial para ocasionar daños que pueden llegar a ser irreparables.

2.1.2.2 Marco para la gestión de riesgos asociados a TIC

2.1.2.2.1 COBIT 5 (*Control Objectives for Information System and related Technology*)

La normativa COBIT 5 (Objetivos de Control para Tecnología de la Información y Tecnologías relacionadas) materializa un conjunto de las “mejores prácticas” para la gestión de los Sistemas de Información dentro de las organizaciones. Su objetivo es brindar un marco de trabajo de dominios y procesos presentando las actividades de una manera manejable y lógica.

Esta norma establece un vínculo entre las metas del negocio con las metas de Tecnologías de Información (TI), brindando métricas y modelos de madurez para medir sus logros e identificando las responsabilidades asociadas a los dueños de los procesos y el departamento de TI.

Figura 3: Principios de COBIT 5

Fuente**:** ISACA, 2012

Tomando en cuenta los elementos anteriores, todos los principios se revisten de vital importancia, no obstante, hay dos que merecen atención adicional para efectos de la presente investigación:

- ✓ Cubrir la empresa de extremo a extremo: todos los niveles de organización comparten una única línea de conocimiento sobre las políticas.
- ✓ Aplicar un marco de referencia único integrado: estandarización de prácticas y procedimientos utilizados para la gestión de riesgos de TI.

COBIT no es una normativa nueva, sino que ha evolucionado con el tiempo según el entorno empresarial y ha venido abarcando los diferentes procesos de la organización.

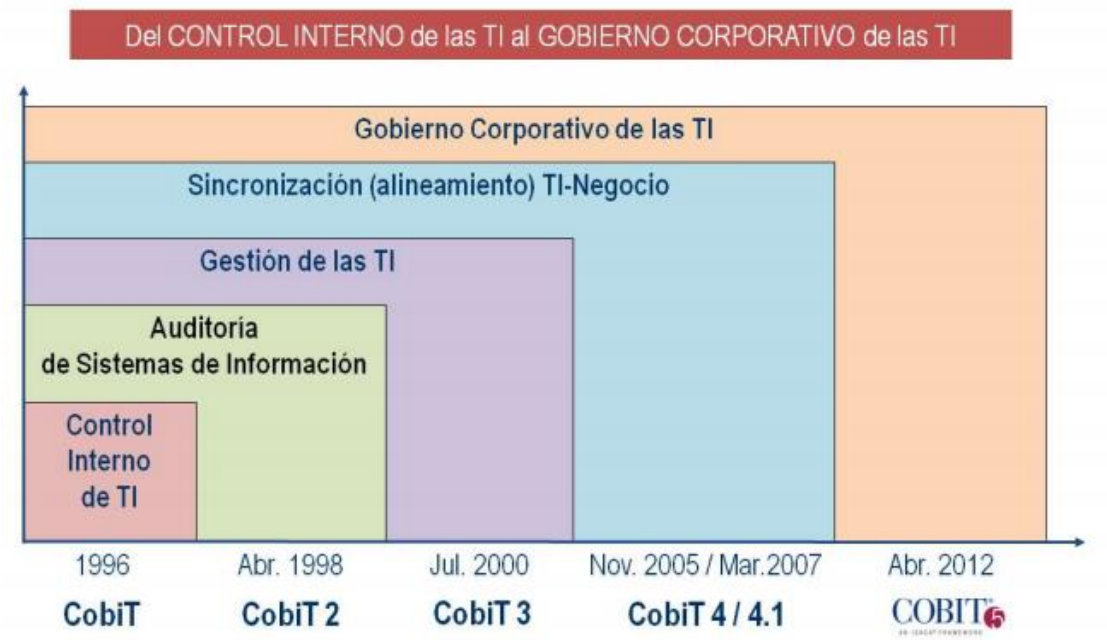

Figura 4: Evolución de COBIT

Fuente: ISACA, 2012

Aunque cada organización es diferente y por lo tanto puede organizar sus procesos como crea conveniente pero no puede dejar de cubrir sus metas de gobierno y gestión. A mayor escala empresarial mayor cantidad de metas, pero sin desorientarse del objetivo que persigue esta norma.

En el siguiente gráfico se observa la cobertura de las áreas según la norma COBIT y aunque es un modelo completo e integral, no constituye el único existente.

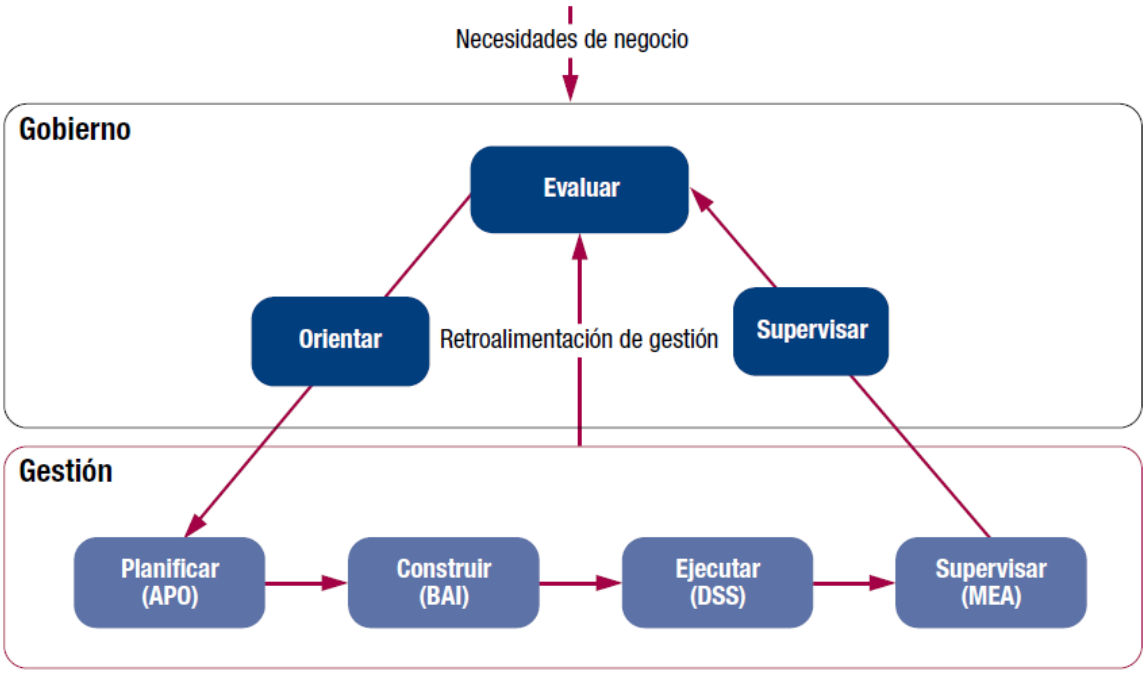

Figura 5: Áreas Claves de Gobierno y Gestión

Fuente: ISACA, 2012

Aunque este último gráfico prácticamente secciona los diferentes procesos en dos grandes categorías, internamente cada una de ellas se subdivide con la intención de brindar una amplitud que permita entender los beneficios que COBIT aporta a la organización independientemente del tamaño de la misma.

Dichos aportes se pueden considerar como:

1) Mantener la calidad de la información para apoyar las decisiones de negocios.
2) Alcanzar los objetivos estratégicos y obtener beneficios de negocio a través del uso innovador de las tecnologías de información.
3) Lograr la excelencia operativa a través de una confiable y eficiente aplicación de tecnología.
4) Limitar los riesgos asociados con TI a un nivel aceptable.
5) Optimizar los servicios y costos de TI
6) Apoyar con el cumplimiento de las leyes, reglamentos, acuerdos y políticas.

Es importante determinar la distinción entre las partes que persiguen las necesidades del negocio de forma tal que no se confundan los objetivos que cada una busca; así se determina que:

A. Gobierno: garantiza que se evalúan las necesidades, condiciones y opciones de los interesados para que se alcancen las metas corporativas a través de la priorización y la toma de decisiones midiendo el rendimiento y el cumplimiento de las metas acordadas. (ISACA, 2012)
B. Gestión: “planifica, construye, ejecuta y controla actividades alineadas con las direcciones establecidas por el gobierno para alcanzar las metas empresariales.” (ISACA, 2012)

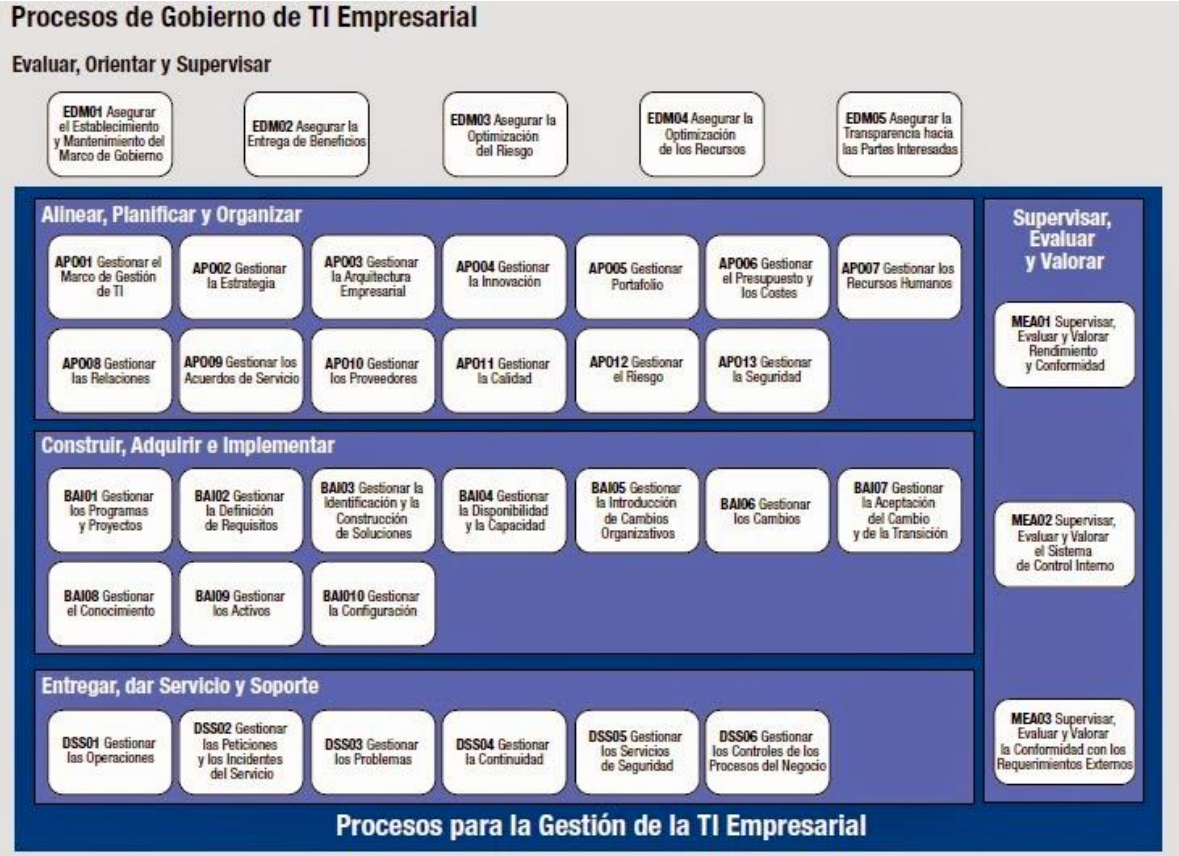

Figura 6: Modelo Referencia de Procesos COBIT 5

Fuente**:** ISACA, 2012

I. EDM01 Asegurar el establecimiento y mantenimiento del marco de Gobierno: analiza y articula los requerimientos para el gobierno de TI, garantizando la supervisión de los procesos de manera efectiva y transparente, cumpliendo con la legalidad y marco regulatorio.

II. EDM02 Asegurar la entrega de beneficios: que las iniciativas de TI, servicios y activos disponibles generen valor al negocio, de forma confiable y precisa para asegurar la efectividad y eficiencia a costos aceptables.

III. EDM03 Asegurar la optimización del riesgo: que el impacto de los riesgos de TI pueda identificarse, gestionarse y reducir el fallo potencial al mínimo.

IV. EDM04 Asegurar la optimización de recursos: tanto, personas, procesos y tecnologías estén disponibles para soportar de manera eficaz los objetivos de la empresa a un costo mínimo y puedan adaptarse a cambios futuros.

V. EDM05 Asegurar la transparencia hacia las partes interesadas: la comunicación con las partes interesadas debe ser efectiva y oportuna con la intención de elaborar informes que aumenten el desempeño, identifique susceptibilidades y confirme las estrategias.

VI. AP001 Gestionar el marco de gestión de TI: el enfoque de gestión debe ser consistente de forma tal que permita cumplir con los requisitos de gobierno corporativo y detallando las estructuras organizativas con responsabilidades y competencias.

VII. APO02 Gestionar la estrategia: alinear los planes estratégicos de TI con los objetivos del negocio y comunicar los mismos para que sean comprendidos e integrados a la filosofía del negocio.

VIII. APO03 Gestionar la arquitectura empresarial: establecer el flujo de operación de la empresa y la forma como se interrelacionan los procesos, de forma que se permita entregar resultados estándar, sensibles y eficientes de acuerdo con los objetivos operativos y estratégicos.

IX. APO04 Gestionar la Innovación: conocimientos y tendencias al día de parte de todos los participantes de los procesos en relación con las necesidades del negocio que mediante la explotación de desarrollos tecnológicos permitan generar valor de la información que se almacena.

X. APO05 Gestionar el Portafolio: ejecutar el conjunto de programas y servicios en respuesta al rendimiento que se desea, de forma alineada con la visión de la arquitectura empresarial, las características de inversión deseadas y las limitantes existentes estableciendo prioridades corporativas.

XI. APO06 Gestionar el presupuesto y los costos: fomentar la colaboración entre TI y las partes interesadas de la empresa para catalizar el uso eficaz y eficiente de los recursos, enfocándolos en el mayor beneficio que brinden las soluciones sometidas a valoración.

XII. APO07 Gestionar los recursos humanos: optimizar las capacidades de los recursos humanos con que se cuenta a través de la definición de funciones, la formación y planes de desarrollo organizacional que genere expectativas de desempeño en la gente competente y motivada.

XIII. APO08 Gestionar las relaciones: enfocar las relaciones entre TI y el negocio hacia un objetivo común que cree mejores resultados, confianza en las herramientas tecnológicas y efectividad de los recursos.

XIV. APO09 Gestionar los acuerdos de servicio: alinear los servicios basados en TI y los niveles de servicio necesarios para cubrir las necesidades presentes y futuras de la empresa.

XV. APO10 Gestionar los proveedores: trasladar y minimizar los riesgos en los servicios de TI prestados por todo tipo de proveedores que no rindan y garantizar el acceso a los menores costos posibles.

XVI. APO11 Gestionar la calidad: tener claros los requisitos de calidad que se buscan en todos los procesos, incluyendo controles de vigilancia y el uso de buenas prácticas probadas y estándares de mejora continua que satisfagan las necesidades de las partes interesadas.

XVII. APO12 Gestionar el riesgo: identificar, evaluar y reducir los riesgos relacionados con TI integrándolos con la gestión de riesgos empresarial, equilibrando costos y beneficios a la vez.

XVIII. APO13 Gestionar la seguridad: mantener la ocurrencia y el impacto de los incidentes de seguridad bajo niveles mínimos de riesgo aceptado.

XIX. BAI01 Gestión de programas y proyectos: alcanzar los beneficios de negocio y reducir riesgos de retrasos y costos inesperados, mediante la mejora de las comunicaciones y el involucramiento de los usuarios, asegurando de esta forma la calidad y la retribución del valor invertido al hacer una revisión post-implementación.

XX. BAI02 Gestionar la definición de requisitos: creación de soluciones viables y óptimas que estén en línea con los requerimientos estratégicos de la organización y con cobertura de todos los procesos de negocio mediante la integración de todas las partes involucradas.

XXI. BAI03 Gestionar la identificación y construcción de soluciones: establecer los requerimientos de la empresa en función del diseño, desarrollo y asociación con proveedores-fabricantes mediante soluciones puntuales y rentables.

XXII. BAI04 Gestionar la disponibilidad y la capacidad: evaluar las capacidades actuales y futuras de disponibilidad y rendimiento mediante el análisis del impacto en el negocio y la evaluación resultante del riesgo previsto en el servicio.

XXIII. BAI05 Gestionar la facilitación del cambio organizativo: preparar y comprometer a las partes para la implementación exitosa para el cambio en el negocio y reducir así el riesgo de fracaso.

XXIV. BAI06 Gestionar los cambios: que todos los cambios en proceso de implementación se generen de forma rápida y fiable para el negocio, mitigando el riesgo que impacte de forma negativa en la estabilidad de la empresa.

XXV. BAI07 Gestionar la aceptación del cambio y la transición: aceptar formalmente y hacer operativas las nuevas soluciones a través de una implementación segura y en línea con las expectativas y resultados acordados.

XXVI. BAI08 Gestionar el conocimiento: proporcionar el conocimiento necesario para dar soporte a todo el personal en los procesos operacionales y facilitar la toma de decisiones.

XXVII. BAI09 Gestionar los activos: contabilizar cada uno de los activos y gestionarlos a lo largo del ciclo de vida, garantizando la funcionalidad de los mismos.

XXVIII. BAI10 Gestionar la configuración: definir y mantener las relaciones entre los recursos y las capacidades necesarias para la prestación de los servicios proporcionados por TI, evaluando el impacto de los cambios y los posibles incidentes.

XXIX. DSS01 Gestionar operaciones: coordinar y ejecutar los procedimientos operativos requeridos para entregar servicios de TI según lo planificado.

XXX. DSS02 Gestionar peticiones e incidentes de servicio: brindar respuesta oportuna y efectiva a las interrupciones de servicios, registrarlos, investigarlos y escalarlos según correspondan.

XXXI. DSS03 Gestionar problemas: reducir el número de problemas operativos mediante la identificación de sus causas raíz y la pronta solución.

XXXII. DSS04 Gestionar la continuidad: establecer y mantener un plan que permita continuar las operaciones críticas para el negocio garantizando la disponibilidad de la información ante un evento significativo.

XXXIII. DSS05 Gestionar servicios de seguridad: establecer y mantener los roles de seguridad y privilegios de acceso a la información de forma tal que, no se comprometa la integridad de los datos.

XXXIV. DSS06 Gestionar controles de proceso de negocio: mantener la integridad de la información a través de controles adecuados previamente definidos y apropiados para cada proceso.

XXXV. MEA01 Supervisar, evaluar y valorar el rendimiento y la conformidad: recolectar información a través de mediciones y supervisar que los procesos

se estén realizando acorde a lo acordado y conforme a los objetivos, generando reportes que proporcionen transparencia.

XXXVI. MEA02 Supervisar, evaluar y valorar el sistema de control interno: mantener vigilado el entorno de control, incluyendo autoevaluaciones externas independientes que permitan a la dirección identificar deficiencias e ineficiencias en el control para establecer rápidamente acciones de mejora.

XXXVII. MEA03 Supervisar, evaluar y valorar la conformidad con los requerimientos externos: asegurarse que la empresa cumple con todos los requisitos externos aplicables a sus operaciones, tanto en los procesos de TI como en los procesos dependientes de las tecnologías de información.

2.1.2.2.2 ITIL (*Information Technology Infrastructure Library*)

La Biblioteca de Infraestructura de Tecnologías de Información (ITIL) consiste en un conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de información, el desarrollo de dichas tecnologías y las operaciones relacionadas en general.

Proporciona asesoramiento sobre cómo proveer servicios tecnológicos de calidad a través de procesos, funciones y capacidades que brindan apoyo; se basa en el ciclo de vida del servicio y pueden segmentarse según sectores económicos, tipos de organizaciones, modelos de operación y arquitectura de tecnología.

Figura 7: Proceso ITIL

Fuente:https://es.wikipedia.org/wiki/Information_Technology_Infrastructure_Library#Estrategia_del_Servicio

1. Estrategia del Servicio: se enfoca en el estudio del mercado y la búsqueda de servicios innovadores que satisfagan al cliente considerando la factibilidad real de su puesta en marcha, además se consideran las posibles mejoras a servicios ya existentes.

   Se constituye de los siguientes procesos:

   - ✓ Gestión Financiera: responsable de garantizar la prestación de servicios con costos controlados y correcta relación calidad – precio.
   - ✓ Gestión de Portafolio: responsable de buscar alternativas de inversión en servicios nuevos y actualizados que minimice los riesgos y costos asociados.
   - ✓ Gestión de la Demanda: responsable de armonizar la oferta de servicios ofrecidos con la demanda.
   - ✓ Gestión de Relaciones del Negocio: identifica las necesidades del cliente y asegura que el proveedor de servicios sea capaz de satisfacer las necesidades con un catálogo adecuado.

2. Diseño del Servicio: su misión es diseñar nuevos servicios o modificar los existentes para su incorporación al catálogo y su paso al entorno de producción.

   Los procesos asociados con esta fase son:

- ✓ Gestión del Catálogo de Servicios: responsable de crear y mantener un catálogo que incluya toda la información relevante como: gestores, estatus, proveedores, entre otros.
- ✓ Gestión de Niveles de Servicio: responsable de acordar y garantizar los niveles de calidad recibidos.
- ✓ Gestión de la Capacidad: responsable de garantizar que la organización TI dispone de la capacidad para prestar los servicios.
- ✓ Gestión de la Disponibilidad: responsable de garantizar que se cumplen los niveles de disponibilidad acordados.
- ✓ Gestión de la Continuidad de los Servicios de TI: responsable de establecer planes de contingencia que aseguren la continuidad de servicios en un tiempo determinado con el menor impacto posible.
- ✓ Gestión de Seguridad de la Información: establece las políticas de integridad, confidencialidad y disponibilidad de información.
- ✓ Gestión de Proveedores: responsable de la relación con los proveedores.
- ✓ Coordinación del Diseño: asegura que las metas y objetivos del diseño se cumplan coordinando y controlando todas las actividades y procesos manteniendo un único punto de coordinación y control.

3. Transición del Servicio: hace que los productos y servicios definidos en la fase de diseño se integren en el entorno de producción y sea accesibles a clientes y usuarios autorizados.

    - ✓ Gestión de la Configuración y Activos: responsable del registro y gestión de los elementos de configuración que soporta todos los aspectos de Gestión del Servicio.
    - ✓ Gestión del Cambio: supervisa y aprueba la introducción o modificación de servicios garantizando que el proceso haya sido planificado, evaluado, probado, implementado y documentado.
    - ✓ Gestión del Conocimiento: garantiza que la información relevante esté disponible para todos los actores y agentes implicados en los procesos.
    - ✓ Planificación y Apoyo a la Transición: planifica y coordina todo el proceso asociado a la creación y modificación de los servicios TI.
    - ✓ Gestión de Entregas y Despliegue: desarrolla, prueba e implementa las nuevas versiones de los servicios según la fase de Diseño.
    - ✓ Gestión Validación y Pruebas: garantiza que los servicios cumplen los requisitos preestablecidos antes de su paso a producción.
    - ✓ Evaluación: evalúa la calidad general del servicio, rentabilidad, utilización y percepción de los usuarios.

4. Operación del Servicio: se lleva a cabo el monitoreo del servicio, se registran los eventos, incidentes, problemas, peticiones adicionales y accesos al servicio. Es primordial la entrega a satisfacción del cliente con la calidad acordada.

    - ✓ Gestión de Incidentes: responsable de registrar los incidentes que afectan la calidad del servicio y restaura los niveles acordados en el menor plazo posible.
    - ✓ Gestión de Problemas: responsable de analizar y ofrecer soluciones a las incidencias constantes o frecuentes.
    - ✓ Cumplimiento de Solicitudes: gestiona las peticiones de los usuarios y clientes que requieren pequeños cambios en la prestación del servicio.
    - ✓ Gestión de Eventos: monitorea los eventos en la infraestructura de TI con el objetivo de asegurar su correcto funcionamiento y prevenir incidencias.
    - ✓ Gestión de Accesos: garantiza que sólo las personas con los permisos adecuados puedan acceder a la información restringida.

5. Mejora Continua del Servicio: se utilizan herramientas de medición y retroalimentación para documentar todo lo referente al funcionamiento del servicio, resultados, problemas ocasionados, soluciones implementadas y dispone de esta información para el resto de los usuarios a fin de que todos alcancen un nivel de conocimiento idóneo respecto con el nuevo servicio.

2.1.2.2.3 ISO/IEC 27005

Esta norma pertenece a la familia de las normas ISO 27000 la cual contiene un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de sistemas de Gestión de la Seguridad de la Información.

La norma 27005 es el estándar internacional que se encarga de la gestión de riesgos de seguridad de información y es aplicable a todas las organizaciones que tengan la intención de gestionar los riesgos asociados con la seguridad de la información.

Aunque no proporciona una metodología concreta para el análisis de riesgos sí describe mediante cláusulas el proceso que se recomienda seguir para analizar el riesgo.

El procedimiento presentado por esta norma es similar al analizado previamente en la sección INTE/ISO 31000:2011. Este procedimiento consiste en establecer el contexto, evaluar el riesgo, tratar el riesgo, si el tratamiento fue efectivo entonces aceptar el riesgo residual y finalmente, comunicar el riesgo y efectuar la revisión y monitoreo; estos dos últimos aspectos, llevados a cabo de manera transversal durante todo el proceso.

Este proceso involucra seis grandes grupos de actividades:

1. Definición del contexto: en esta etapa se define el ambiente, alcance, criterios de evaluación y otros ajustes.
2. Análisis / Evaluación del riesgo: permite identificar el riesgo y determinar las acciones necesarias para reducir el riesgo a un nivel aceptable.

3. Tratamiento del riesgo: se define a partir de los resultados obtenidos del análisis y la evaluación.
4. Aceptación del riesgo: asegura los riesgos asumidos por la organización, es decir, el riesgo que por alguna razón no será tratado o se le trata parcialmente. A estos se les denomina riesgos residuales.
5. Comunicación del riesgo: en esta etapa se informa el riesgo y la forma como será tratado, para todas las áreas operacionales y sus gestores.
6. Seguimiento y análisis crítico: se conforman por las actividades de acompañamiento de los resultados, implementación de controles y un análisis exhaustivo para el mejoramiento continuo del proceso de gestión del riesgo.

La gestión del riesgo de seguridad de la información es llevada a cabo por las organizaciones en la búsqueda de ventajas competitiva para los negocios. Es crucial para demostrar a las partes interesadas, una actitud de seguridad en la gestión de los riesgos relacionados con la protección de los activos de la información.

Aumentar la capacidad de gestionar el riesgo y optimizar el retorno son acciones integrantes de un enfoque sistémico, que proporciona un proceso formal para la mejora de la capacidad de identificación y evaluación del riesgo.

En resumen se detalla a continuación un gráfico con las etapas explicadas anteriormente y el flujo correspondiente; cabe destacar, que esta norma puede ser aplicada en conjunto con la norma ISO 27001 (Sistemas de Gestión de Riesgos y Seguridad) e ISO 31000 (Gestión de Riesgos).

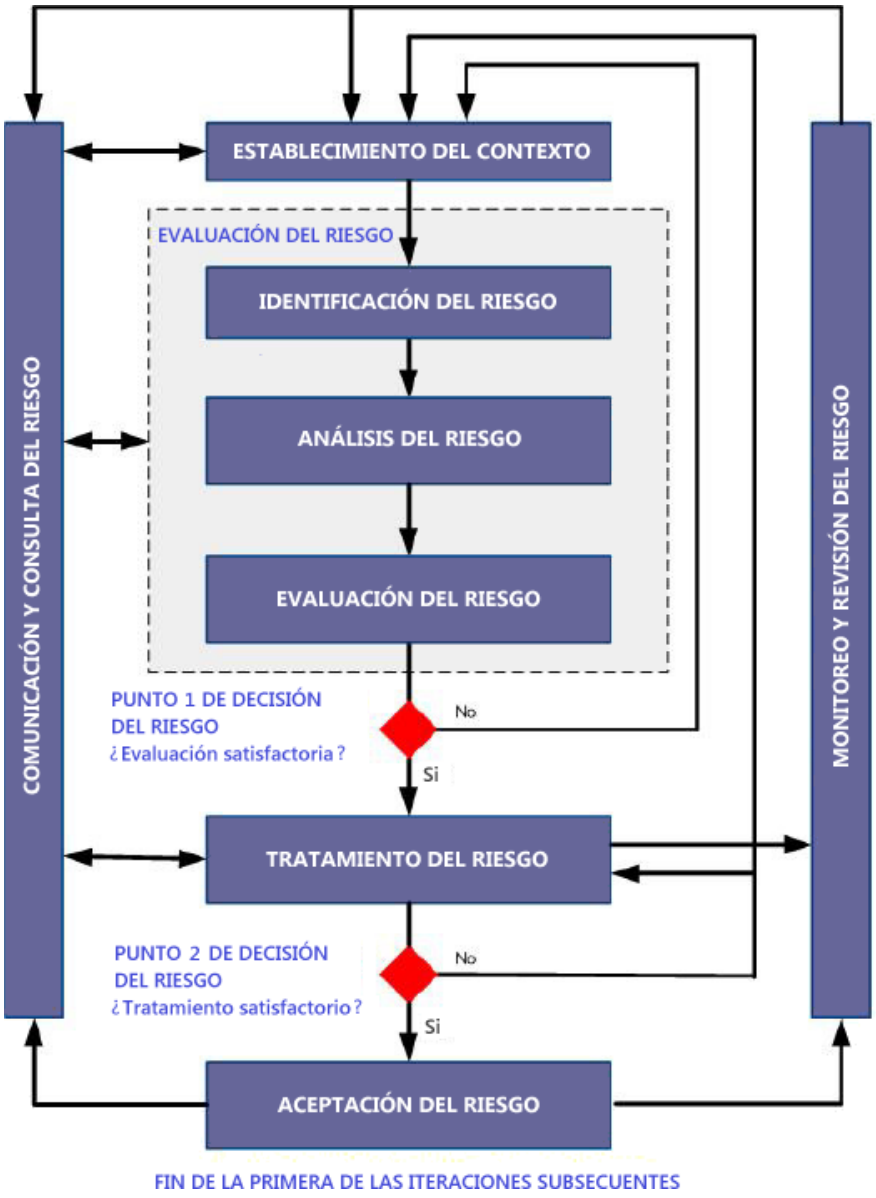

Figura 8: Proceso de gestión de riesgos ISO 27005

Fuente: http://ecorfan.org/handbooks/Ciencias%20Sistemas%20Informacion%20T-I/Handbook%20Universidad%20Iberoamericana_2.pdf

2.3 HIPÓTESIS

Si tomamos en cuenta que una empresa debe funcionar como una unidad que está conformada por secciones, áreas y departamentos que se relacionan entre si y que el funcionamiento sincronizado entre dichos elementos es la ruta hacia la obtención del éxito, hay un factor que se convierte en eje fundamental de este engranaje: el ambiente de control.

El manejo de toda entidad está cimentado sobre la ejecución de actividades; estas, conservan determinados procedimientos que son realizados por todo el recurso humano y que deben tener controles inmersos que, permitan una evaluación constante, identificación de oportunidades de mejora y replanteo, de lo contrario, no es posible determinar si las actividades se hacen de manera correcta.

Es necesario que a cada proceso se le realice un análisis que permita asegurar de forma razonable que el siguiente no se ve afectado por alguna falta en el anterior, la periodicidad de esta evaluación debe ser constante y aplicable a todos los procesos en la empresa, sean estos administrativos u operativos.

Este ambiente es la base de la administración de riesgos corporativos, pues proporciona disciplina y estructura, además, impacta en todos los componentes de la gestión de riesgo. El control es, por lo tanto, el único mecanismo efectivo que asegura el cumplimiento a cabalidad de los objetivos, propósitos, procesos y actividades en la empresa.

Entonces, para mantener el pulso de la empresa es prioridad establecer instrumentos de aplicación cíclica que sirvan como “medidores” o sensores muy

afinados que permitan recaudar información para tomar decisiones y actuar en consecuencia de estas, generando así un ambiente de control que evoluciona hasta re expresarse como todo un sistema de control interno.

El ambiente de control lo que busca es la implementación de las condiciones ideales en la compañía que permitan la correcta y completa implementación de los mecanismos de control interno y es a la vez, un entorno ideal que fomenta la aplicación de dichos mecanismos a través del compromiso de cada uno de los miembros de la organización de asegurar el cumplimiento de los objetivos y propósitos de esta.

Si el personal está convencido de la importancia de aplicar un control sobre los procesos que realiza y además encuentra las condiciones favorables para aplicarlos, es posible que cada individuo asuma como suyo el propósito de lograr que la empresa avance perfectamente en todos sus aspectos.

Y es que corresponde a los colaboradores de todos los niveles de la compañía la implementación, seguimiento y evaluación del control, por lo que, se debe fomentar la cultura y el hábito de ejercerlo siempre, logrando que cada uno haga conciencia de la necesidad y responsabilidad de ejercerlo en cada actividad que realizan dentro del negocio.

La estructura que se establezca en la entidad incide de gran forma en el ambiente de control; si es abierta, es decir, donde se facilita la participación de todos los departamentos y empleados, existe la retroalimentación, lo que beneficiará y estimulará la detección de errores, sus causas, efectos y posibles soluciones. Por

lo que es ideal que la estructura contemple la posibilidad de que los colabores expresen libremente sus opiniones.

Debido al auge de la tecnología y la participación de esta en la vida empresarial, el ambiente de control que las organizaciones han conocido hasta hoy, debe ser trasladado a los sistemas informáticos y toda red de comunicación que maneje los datos sensibles de los negocios.

Las empresas deben garantizar razonablemente, la confidencialidad, integridad y disponibilidad de la información, protegerla contra el mal uso, divulgación o alteración no autorizada, daño, pérdida o algún factor adicional que comprometa la continuidad del negocio.

2.4 OPERACIONALIZACIÓN DE LA HIPÓTESIS

HIPÓTESIS	CONCEPTOS	VARIABLES	INDICADORES
Existen debilidades en los diferentes procesos que llevan a cabo las Tecnologías de Información y Comunicación en la Compañía Aceitera El Coco S.A. que pueden comprometer la seguridad de la información a la cual se tiene acceso por parte de los quienes ejecutan las actividades de control.	**Control Interno:** proceso integrado a las actividades operativas de una entidad diseñado para garantizar la seguridad razonable de la información y fiabilidad en el logro de los objetivos del gobierno corporativo. **Seguridad de datos:** aplicación y gestión de buenas prácticas que permiten proteger los datos en todas las aplicaciones y plataformas de una organización. **Riesgo:** probabilidad de que una amenaza se convierta en desastre.	**Externas:** * Naturales * Humanos * Materiales **Internas:** * Robos * Sabotaje * Fraude * Destrucción	Ambiente de Control. Cumplimiento de Normativas. Análisis de Vulnerabilidades. Administración de Riesgos. Recursos Utilizados. Satisfacción del Cliente.

CAPÍTULO III

MARCO METODOLÓGICO

3.1 ENFOQUE DE LA INVESTIGACIÓN

La presente investigación responde al enfoque cualitativo; pues desarrollará interrogantes e hipótesis durante todo el proceso de recolección y análisis de datos.

Así pues, en primera instancia se explorará y se describirá la realidad actual de la instancia bajo análisis; para posteriormente generar perspectivas teóricas que permitirán proponer medidas de mejora.

El presente estudio, se fundamenta en el análisis de información relacionada con la adopción e interpretación de las buenas prácticas empresariales y la normativa afín que permite un ambiente de control interno, eficaz y alineado con los objetivos de la entidad; por lo que su naturaleza es de enfoque cualitativo.

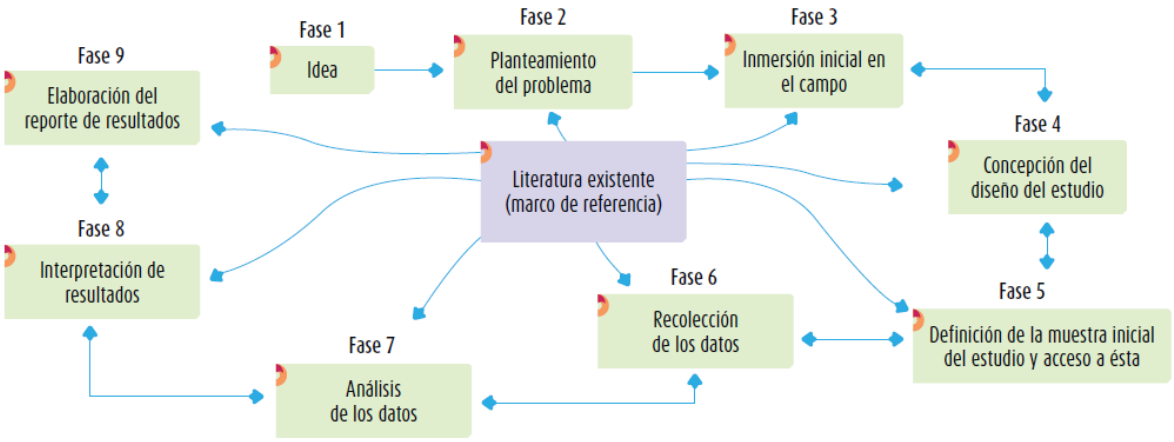

Figura 9: Proceso de Enfoque Cualitativo

Fuente: Hernández, Fernández, Baptista (2014)

3.2 ALCANCE DE LA INVESTIGACIÓN

Este estudio de investigación se cataloga como descriptiva; por cuanto se centrará en la temática del control interno, misma que ha sido ampliamente abordada en diversos foros y marcos normativos nacionales e internacionales; materia de la cual pueden determinarse claramente sus alcances para las organizaciones que le han adoptado como filosofía de trabajo.

3.3 DISEÑO DE LA INVESTIGACIÓN

La presente investigación aplica el diseño no experimental – transversal; por cuanto se observará el estado actual de las actividades de control en materia de tecnologías de la información y comunicación de la Compañía Aceitera El Coco S.A; recolectando los datos de la información en un momento determinado para poder proponer las medidas de mejora del caso.

3.4 UNIDADES DE ANÁLISIS U OBJETOS DE ESTUDIO

La unidad de análisis la constituye cada una de las actividades de control en materia de tecnologías de la información y comunicación de la empresa bajo análisis.

3.4.1. Población

La población está conformada por la cantidad total de las actividades de control en materia de tecnologías de la información y comunicación de la empresa bajo análisis, existentes en el segundo semestre de 2020.

3.5 CUIDADOS ÉTICOS PARA EL MANEJO DE LA INFORMACIÓN Y EL CONTACTO CON PARTICIPANTES

La información proveída por la Compañía Aceitera El Coco S.A; fue obtenida con el visto bueno del jerarca institucional y será tratada con los más estrictos estándares de confidencialidad y discrecionalidad que exige una investigación universitaria de este tipo; de forma que, el desarrollo de la misma no acarreará perjuicios para la entidad analizada.

3.6 INSTRUMENTOS PARA LA RECOLECCIÓN DE LA INFORMACIÓN

Para la determinación del nivel actual de cada uno de los cinco componentes del sistema de control interno, se aplicará un cuestionario que está estructurado con base a veinte preguntas cerradas (una por cada principio de control interno), contenidas en una batería de cuestiones; de la siguiente manera:

Componente	Atributos a evaluar (Preguntas)	Posibles respuestas
Ambiente de Control	1. Compromiso superior	A. Nivel incipiente B. Nivel novato. C. Nivel competente D. Nivel diestro. E. Nivel experto.
	2. Ética	A. Nivel incipiente B. Nivel novato.

Componente	Atributos a evaluar (Preguntas)	Posibles respuestas
		C. Nivel competente D. Nivel diestro. E. Nivel experto.
	3. Idoneidad del Personal	A. Nivel incipiente B. Nivel novato. C. Nivel competente D. Nivel diestro. E. Nivel experto.
	4. Estructura organizativa	A. Nivel incipiente B. Nivel novato. C. Nivel competente D. Nivel diestro. E. Nivel experto.
Gestión de Riesgos	5. Marco orientador	A. Nivel incipiente B. Nivel novato. C. Nivel competente D. Nivel diestro. E. Nivel experto.
	6. Herramienta de valoración.	A. Nivel incipiente B. Nivel novato. C. Nivel competente

Componente	Atributos a evaluar (Preguntas)	Posibles respuestas
		D. Nivel diestro. E. Nivel experto.
	7.Funcionamiento de la herramienta	A. Nivel incipiente B. Nivel novato. C. Nivel competente D. Nivel diestro. E. Nivel experto.
	8.Documentación y comunicación.	A. Nivel incipiente B. Nivel novato. C. Nivel competente D. Nivel diestro. E. Nivel experto.
Actividades de Control	9.Características	A. Nivel incipiente B. Nivel novato. C. Nivel competente D. Nivel diestro. E. Nivel experto.
	10.Alcance	A. Nivel incipiente B. Nivel novato. C. Nivel competente D. Nivel diestro.

Componente	Atributos a evaluar (Preguntas)	Posibles respuestas
		E. Nivel experto.
	11.Formalidad	A. Nivel incipiente B. Nivel novato. C. Nivel competente D. Nivel diestro. E. Nivel experto.
	12.Aplicación	A. Nivel incipiente B. Nivel novato. C. Nivel competente D. Nivel diestro. E. Nivel experto.
Sistemas de Información	13.Alcance	A. Nivel incipiente B. Nivel novato. C. Nivel competente D. Nivel diestro. E. Nivel experto.
	14.Calidad de la información	A. Nivel incipiente B. Nivel novato. C. Nivel competente D. Nivel diestro. E. Nivel experto.

Componente	Atributos a evaluar (Preguntas)	Posibles respuestas
	15.Calidad de la comunicación	A. Nivel incipiente B. Nivel novato. C. Nivel competente D. Nivel diestro. E. Nivel experto.
	16.Control de los sistemas	A. Nivel incipiente B. Nivel novato. C. Nivel competente D. Nivel diestro. E. Nivel experto.
Seguimiento del Control Interno	17.Participantes	A. Nivel incipiente B. Nivel novato. C. Nivel competente D. Nivel diestro. E. Nivel experto.
	18.Formalidad	A. Nivel incipiente B. Nivel novato. C. Nivel competente D. Nivel diestro. E. Nivel experto.
	19.Alcance	A. Nivel incipiente

Componente	Atributos a evaluar (Preguntas)	Posibles respuestas
		B. Nivel novato. C. Nivel competente D. Nivel diestro. E. Nivel experto.
	20.Contribución	A. Nivel incipiente B. Nivel novato. C. Nivel competente D. Nivel diestro. E. Nivel experto.

Tabla 1: Cuestionario de Control Interno

Dicho instrumento está previamente validado, por cuanto está basado en el usado por la Unidad de Control Interno de la Oficina de Mejoramiento y Control de la Gestión Institucional del Ministerio de Seguridad Pública; mismo que está disponible para su consulta en la sección “Transparencia” del portal web de dicha institución pública (www.seguridadpublica.go.cr)

3.7 VARIABLES O CATEGORÍAS

Objetivo Específico 01	Determinar el nivel actual de cada uno de los componentes del sistema de control interno.				
Variable	**Definición Conceptual**	**Definición Operacional**	**Dimensión**	**Indicadores**	**Instrumento**
Componentes del sistema de control interno	Madurez de cada componente.	Valoración del nivel de cada componente.	Escalonada (cinco niveles)	Nivel incipiente Nivel novato. Nivel competente Nivel diestro. Nivel experto	Valoración de control interno.
Objetivo Específico 02	Analizar los procedimientos actuales de control de la sección de Tecnologías de Información.				
Variable	**Definición Conceptual**	**Definición Operacional**	**Dimensión**	**Indicadores**	**Instrumento**
Procedimientos de control de Tecnologías de Información.	Existencia, formalidad y valor agregado de los procedimientos.	Utilidad de los procedimientos.	Dicotómica	Útiles / Inútiles	Matriz de Juicio cualitativo.
Objetivo Específico 03	Establecer la vinculación existente entre las actividades de control en materia de tecnologías de la información y comunicación con el logro de los objetivos estratégicos corporativos.				
Variable	**Definición Conceptual**	**Definición Operacional**	**Dimensión**	**Indicadores**	**Instrumento**
Vinculación entre las actividades de control en TI con el logro de los objetivos estratégicos corporativos.	Posibles discrepancias significativas entre ambos.	Vinculación y alineación.	Dicotómica	Vinculación / No vinculación.	Matriz comparativa
Objetivo Específico 04	Establecer el grado de satisfacción y seguridad de los usuarios de los sistemas de información.				
Variable	**Definición Conceptual**	**Definición Operacional**	**Dimensión**	**Indicadores**	**Instrumento**
Grado de satisfacción y seguridad de los usuarios de los sistemas de información.	Expectativas de los *stakeholders* involucrados.	Satisfacción de las expectativas.	Dicotómica	Satisfacción / No satisfacción.	Entrevistas a *stakeholders* involucrados.

Objetivo Específico 05	Proponer medidas de mejora para las actividades de control en materia de tecnologías de la información y comunicación				
Variable	**Definición Conceptual**	**Definición Operacional**	**Dimensión**	**Indicadores**	**Instrumento**
Medidas de mejora para las actividades de control en TI.	Mejoras en gestión de las tecnologías de la información.	Sanas prácticas	Dicotómica	Existencia de las prácticas / Inexistencia de las prácticas.	Marco de sanas prácticas en gestión de las tecnologías de la información

3.8 ANÁLISIS DE DATOS

Se realizaron anotaciones de entrevistas y sesiones de observación, a efectos de llevar a cabo un análisis de contenido.

CAPÍTULO IV

RESULTADOS

4.1 NIVEL ACTUAL DE CADA UNO DE LOS COMPONENTES DEL SISTEMA DE CONTROL INTERNO

Como la presente investigación se basa en la evaluación de las actividades de control en materia de tecnologías de la información –en lo sucesivo, TI-; así como de identificar oportunidades de mejora en este tema; como por ejemplo la propuesta de un marco de sanas prácticas para la gestión de las tecnologías de la información.

Así pues, correspondió previamente, verificar la noción del control interno corporativo que tienen de sí mismos los diferentes gerentes o jefes de la empresa.

Lo anterior si se tiene en consideración, que un marco de sanas prácticas para la gestión de las tecnologías de información, no es más que una actividad de control interno; mismo que, colabora en el esfuerzo de que se alcancen los objetivos corporativos.

Debe tenerse claro, que las actividades de control corresponden nacen o se generan como producto de las medidas de mitigación de riesgos; las cuales a su vez, se derivan de la gestión de riesgos; y ésta, tiene lugar en una empresa o institución, siempre y cuando haya un robusto ambiente de control.

En ese sentido, es importante tener claro que no se puede instaurar un marco de sanas prácticas, si la entidad bajo análisis, tiene debilidades en cualquiera de los cinco componentes de control interno, especialmente en la valoración en la valoración de riesgos y ambiente de control.

Así pues, al seleccionar una muestra por conveniencia, se consultó diferentes jefaturas y gerencias, acerca de su percepción en cuanto a cada uno de los componentes de control interno.

Concretamente los entrevistados fueron el Gerente Comercial, el Gerente de TI, el Subgerente de Compras, el señor Contralor de la Compañía, el Jefe de Infraestructura de TI, el Jefe de Arquitectura de TI y el Jefe de Cuentas por Cobrar.

La mecánica fue aplicar un cuestionario que estuvo estructurado con base a veinte preguntas cerradas, contenidas en una batería de cuestiones, como se detalló en las secciones previas de este informe.

En consecuencia, cada entrevistado evaluó el nivel de madurez corporativo que ostenta actualmente cada uno de los principios que conforman los cinco componentes del control interno, asignado uno de los siguientes niveles a cada principio: incipiente, novato, competente, diestro o experto. Posteriormente, se le permitió al entrevistado emitir un juicio cualitativo en caso de que así lo decidiera, para profundizar más opinión y ampliar el panorama. En el caso del primer componente del sistema de control interno; es decir, ambiente de control, la calificación obtenida fue:

Componente	Principio de Control	Nivel asignado
Ambiente de Control	Compromiso superior	Incipiente
	Ética	Incipiente
	Idoneidad del Personal	Diestro
	Estructura organizativa	Competente

Tabla 2: Autoevaluación del Ambiente de Control

En cuanto al compromiso superior, los entrevistados anotaron que existe un limitado compromiso por parte de los gerentes y jefes con respecto al control interno; dado que el mismo es entendido de diferentes maneras.

Asimismo, indicaron que no existen regulaciones corporativas en materia de control interno.

Por otra parte, en lo que ética se refiere, se indicó que la misma es percibida por los funcionarios de la empresa como un comportamiento correcto, de acuerdo con sus creencias y valores; de modo que, es verdad que los empleados reconocen la importancia de algunos valores corporativos; sin embargo, la ética es considerada como una responsabilidad de las autoridades institucionales.

Por su lado, el tema de la autoevaluación de personal arrojó comentarios importantes, dado que los entrevistados consideraron que en términos generales, la empresa cuenta con un equipo humano que dispone de la actualización y formación continuas, para el desempeño de su cargo, de acuerdo con las necesidades organizacionales.

Adicionalmente se argumentó que los procesos de administración de recursos humanos se evalúan y mejoran de manera continua, destacándose la jefatura como el líder.

Finalmente, en lo referente a la estructura organizacional, se anotó que en la empresa se ha instaurado procesos para procurar una estructura corporativa que sea adaptativa con base en las circunstancias, las necesidades y los objetivos, así como los riesgos que le plantea su entorno.

Paralelamente, se mencionó que se han introducido ajustes en la estructura organizacional para armonizarla con los objetivos organizacionales.

En otro orden de cosas, al conocer la autoevaluación de la gestión de riesgos corporativa, los entrevistados en esta ocasión otorgaron un nivel de incipiente a los cuatro principios de este componente de control.

Componente	Principio de Control	Nivel asignado
Gestión de Riesgos	Marco orientador	Incipiente
	Herramienta de valoración.	Incipiente
	Funcionamiento de la herramienta	Incipiente
	Documentación y comunicación.	Incipiente

Tabla 3: Autoevaluación de la Gestión de Riesgos

Sobre el marco orientador, entendido como un marco técnico de sanas prácticas y procedimientos, la empresa carece de ellos.

Los entrevistados manifestaron grosso modo que la conciencia sobre la importancia de llevar a cabo una valoración del riesgo como medio para conducir las operaciones organizacionales con eficiencia, es apenas incipiente, y se pone de manifiesto sólo en algunas áreas; por lo que el tema de la gestión de riesgos se conoce vagamente, y se carece de disposiciones jurídicas y técnicas en la materia.

En consecuencia, no existe en la empresa una herramienta para la gestión de riesgos; de modo que, se administra de manera precaria la información sobre los riesgos que se llegan a identificar y analizar.

En adición, de los comentarios obtenidos se resume que en general, las jefaturas y gerencias realizan una valoración intuitiva de algunos riesgos que afectan las actividades de las unidades que dirigen; puesto que, tienen una noción mínima de cuáles son los riesgos más relevantes, y definen, en consecuencia, con esa noción, los controles que deben aplicarse.

Así las cosas, no hay mayor documentación al respecto de los riesgos, sus medidas de mitigación propuestas ni de los seguimientos reales efectuados a las actividades que en teoría se llevaron a cabo para administrar los riesgos.

Esto implica que la empresa no está previendo sus amenazas con suficiente antelación, lo que le resta cada vez más margen de maniobra en caso de que una de esas situaciones se llegase a materializar; lo cual atenta contra la existencia de la empresa misma.

Seguidamente, al conocer el criterio de los entrevistados sobre las actividades de control como tercer componente del sistema de control interno, nuevamente se

obtuvo un consenso al calificar de incipiente cada uno de los principios de este componente; tal y como se evidencia en esta tabla.

Componente	Principio de Control	Nivel asignado
Actividades de control	Características	Incipiente
	Alcance	Incipiente
	Formalidad	Incipiente
	Aplicación	Incipiente

Tabla 4: Autoevaluación de las Actividades de Control

Los entrevistados dieron fe de que las actividades de control se han establecido con base en prácticas tradicionales, y sólo en algunos casos se ha considerado la relación del costo – beneficio de éstas.

En coherencia con lo descrito, se apuntó que las actividades de control vigentes se orientan a la protección de algunos activos y a la prevención de fraude; detalle que es fundamental para la presente investigación y que será retomado páginas más adelante.

Sobre la documentación pertinente, se indicó que solamente algunas actividades de control están documentadas; pero en breves descripciones de funciones y puestos; otras se han dispuesto mediante instrucciones a funcionarios específicos; además, las mismas no son divulgadas entre el personal.

Así pues, no hay certeza de que las actividades de control que existen, sean acatadas y cumplidas el 100% de las veces.

Por otro lado, al abordar el cuarto componente de control interno, nuevamente las autoevaluaciones coincidieron en otorgar un nivel de incipiente a cada uno de los principios de los sistemas de información.

Componente	Principio de Control	Nivel asignado
Sistemas de información	Alcance	Incipiente
	Calidad de la información	Incipiente
	Calidad de la comunicación	Incipiente
	Control de los sistemas	Incipiente

Tabla 5: Autoevaluación de los Sistemas de Información

En primera instancia, en cuanto al alcance de los sistemas, se manifestó que en la empresa se recopila, procesa y comunica información para cumplir con algunos requerimientos específicos; y que, en honor a la verdad, las diferentes jefaturas han realizado esfuerzos aislados para el procesamiento, generación y comunicación de información relativa a las actividades a su cargo.

En cuanto a la calidad de la información, algunos sistemas de información generan la información necesaria para la atención de ciertos requerimientos específicos.

Por otro lado, no se ha definido canales de comunicación para enviar la información requerida por las instancias internas únicamente; aunque sí existen algunos controles para asegurar la calidad de la información y su comunicación, como la definición de accesos a los sistemas de información que utilizan recursos tecnológicos, y la asignación de responsabilidades sobre la custodia de los acopios físicos de información.

Finalmente, en lo que se refiere a la autoevaluación del último componente de control interno, el nivel asignado por los entrevistados fue de incipiente para los cuatro principios.

Componente	Principio de Control	Nivel asignado
Seguimiento del control interno	Participantes	Incipiente
	Formalidad	Incipiente
	Alcance	Incipiente
	Contribución	Incipiente

Tabla 6: Autoevaluación del Seguimiento del Control Interno

En términos generales, se indicó que la labor del seguimiento del sistema de control interno no está asignada ni es responsabilidad de una o varias unidades; aunque ciertamente, hay algunos controles específicos, que en realidad son mecanismos de vigilancia que, de manera rutinaria, ejercen las jefaturas sobre el cumplimiento de algunas actividades.

Asimismo, como se mostró en la figura 01 de este documento, en la empresa no existe una gerencia administrativa o al menos una oficina o unidad de planificación, que se encargue de gestionar todo lo relativo a la planificación estratégica y del control interno; así como tampoco existe una auditoría interna.

Lo anotado en el párrafo anterior, sin duda confirma que en general el nivel de madurez de la empresa analizada es incipiente en lo que respecta al control interno; pudiendo deberse esto a diferentes factores; mismos que ameritaría todo un análisis aparte a lo que busca esta investigación; sin embargo, se puede mencionar de

forma general que es una empresa con muchos años de antigüedad y de naturaleza familiar, que ha implementado modelo de gestión gerencial por décadas; sin haber reparado en actualizaciones filosóficas administrativas, obviando, en consecuencia, todo lo que implica el sistema de control interno y sus beneficios.

4.2 PROCEDIMIENTOS ACTUALES DE CONTROL DE LA SECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

En cuanto al tema específicamente de tecnología de información, la empresa tampoco cuenta con manuales de procedimientos, políticas, instructivos, reglamentos o alguna otra forma de actividad de control que regule adecuadamente el uso de las tecnologías de información y el resguardo de la información importante en la empresa.

Lo descrito en el párrafo anterior, es esperable por cuanto no sería lógico que una empresa que no ha aplicado el sistema ni la filosofía de control interno, contase con una robusta estructura normativa en cuanto a tecnología de información.

Así las cosas, no existe un Reglamento de Normas y Políticas de TI, que defina pautas a seguir en diversos temas como, por ejemplo, el respaldo a nivel de usuario, aunque verbalmente se han girado instrucciones para que cada usuario es responsable de respaldar su información, mas no se ha establecido formalmente de qué forma ni con qué frecuencia debe hacerse tal actividad.

Considérese que el computador de escritorio promedio en la empresa solo cuenta con unidad lectora de disquetes, puertos USB y un lector de CD. El equipo no cuenta con un quemador DVD, no hay Discos Duros Externos o Unidades de

almacenamiento USB (Llaves Maya) asignadas al funcionario para la exclusiva tarea de respaldar información (Además hay que tener en cuenta la capacidad de almacenamiento que debe tener la hipotética llave maya de respaldo dado que la información a respaldar podría no caber en la misma). Tampoco hay procedimientos para el respaldo de información en servidores.

Por todo lo anterior, se hace difícil que cada usuario pueda respaldar adecuadamente la información, salvo que por iniciativa personal traiga de su hogar llaves mayas personales, discos duros externos e incluso computadores particulares para respaldar la información, situación que de por sí ya es extremadamente peligrosa dado que se estaría tolerando la extracción de información corporativa sensible.

Por otro lado, para el caso de los funcionarios que tienen asignadas laptops corporativas, o que puedan hacer uso de ellas en ciertos momentos por la naturaleza misma del puesto no existen políticas y/o procedimientos para el uso de las conexiones Bluetooth en lugares públicos como restaurantes, cafeterías, entre otros. Independientemente de las defensas lógicas de los equipos, no hay políticas claras que traten el tema de las conexiones de Bluetooth con otros equipos, telefónicos celulares, inteligentes, entre otros.

Esto incrementa el riesgo de que por desconocimiento de la tecnología Bluetooth, accidental o intencionalmente, un funcionario permita el enlace del equipo corporativo con equipos externos, tolerando la extracción de información.

Sobre el mismo orden de cosas, también para los funcionarios que tienen asignadas laptops corporativas, o que puedan hacer uso de ellas en ciertos momentos por la naturaleza misma del puesto, tampoco existen políticas y/o procedimientos para el uso de redes inalámbricas ajenas a la empresa. Así las cosas, los funcionarios ignoran los peligros de conectarse a internet en cualquier lugar en que haya libre acceso a las redes, abriendo la posibilidad de que los equipos corporativos sean víctimas de intrusiones no autorizadas.

Por otra parte, la Administración no ha informado al personal del acerca de la importancia administrar correctamente las sesiones en Windows para minimizar la probabilidad de un uso de las mismas por terceras personas. Dado lo anterior es común ver computadores en plena sesión mientras sus usuarios están en hora de almuerzo, en ejecución de labores fuera de la oficina o bien siendo usados por otros funcionarios.

Tampoco se ha informado al personal del acerca de métodos para crear passwords seguros. En consecuencia, lo usual es que cada funcionario escoja una clave predecible como el nombre de sus hijos o conyugue, fechas de cumpleaños, entre otros. Esto aumenta considerablemente el riesgo de que un equipo pueda ser accedido por una tercera persona con intenciones cuestionables.

Adicionalmente, no se ha informado al personal de la importancia de no notificar automáticamente vía correo electrónico cuando se está fuera de la oficina o de vacaciones, por lo tanto, no se ha contrarrestado la amenaza de que terceras personas sepan que esos equipos están sin el funcionario esos días, aumentando la probabilidad de ocurrencia de un ataque.

Las medidas preventivas y correctivas que ha tomado la Gerencia de TI con respecto al Hoax y Phishing se basan en la eficacia del Firewall, el cual restringe el acceso a websites, sin embargo, no existen políticas al respecto ni capacitación a los usuarios para que éstos puedan identificar dichas amenazas.

Por su lado, los correos electrónicos corporativos se crean con la primera letra del nombre del funcionario seguido del primer apellido; no obstante, no se ha advertido de la vulnerabilidad de usar esta práctica para efectos del envío de Spam, Hoax y Phishing; si terceras personas obtuviesen una la lista de personal de la empresa de manera parcial o total, independientemente de las barreras disponibles como antivirus, antispyware, firewalls, entre otros, dado que para la mayoría de los casos es sumamente fácil inferir la cuenta de correo electrónico de cada funcionario al conocer su nombre y primer apellido.

No menos importante es indicar que no hay políticas y/o procedimientos claros y puntuales para el uso de dispositivos de almacenamiento USB (Llaves Maya) personales o propiedad de la empresa en equipos particulares y corporativos. La extracción de información a través de USB Llave Maya no está siendo controlada.

Tampoco hay un acuerdo de confidencialidad institucional de la información contenida en las Bases de Datos corporativas cuando tiene lugar la contratación de un funcionario.

Por su parte, en el caso de renuncia, despido o vencimiento del nombramiento de un funcionario, no existen políticas y/o procedimientos para salvaguardar la información que dicho servidor tiene en su máquina y/o llave maya.

Finalmente, se puede señalar que los respaldos de las bases de datos corporativas están en la sede central de la empresa, así como los servidores y bases de datos originales.

4.3 VINCULACIÓN EXISTENTE ENTRE LAS ACTIVIDADES DE CONTROL EN MATERIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN CON EL LOGRO DE LOS OBJETIVOS ESTRATÉGICOS CORPORATIVOS.

La Gerencia de TI carece de un plan estratégico; por cuanto, considera que eso es un tema ajeno a sus competencias y que es una responsabilidad más de la Gerencia General Corporativa.

Lo señalado tiene lugar por un desconocimiento de las sanas prácticas globales y la carencia de un marco normativo aplicable a la gestión de las TI en la empresa, lo cual a su vez se da por deficiencias en el ambiente de control de la empresa.

A tenor de lo expuesto, la Gerencia de TI no tiene idea de cuál es el rumbo de la empresa y, por ende; no puede otorgar valor a la misma, mejorar sus servicios internos ni generar oportunidades nuevas para negocio basadas en las tecnologías de la información; de modo que, sus funciones actuales se limitan a brindar un soporte técnico y al resguardo de los sistemas ante ataques externos.

Así las cosas, no existe una planificación estratégica en la Gerencia de TI, restándole valor y eficacia a la planificación estratégica corporativa; dado que dicha Gerencia no está contemplando los objetivos estratégicos corporativos al planificar sus acciones.

4.4 GRADO DE SATISFACCIÓN EN CUANTO A LA SEGURIDAD DE LOS USUARIOS DE LOS SISTEMAS DE INFORMACIÓN.

Los principales sistemas que se utilizan en la empresa son ERP- AS400, NAF (en el área comercial), Power BI (usado por las jefaturas) y BI Manager (usado por las áreas comercial, operaciones y contabilidad) y los mismos son utilizados por 125 empleados, para el desarrollo de sus funciones.

Gracias a la colaboración de la Gerencia General Corporativa, por medio del *chat* interno de la empresa se pudo consultar a los usuarios citados sobre su opinión en cuanto a la seguridad de los sistemas de información que operan diariamente.

Por medio de una pregunta cerrada, se determinó que el 80% estaban muy conformes, el 10% medianamente conformes y el 10% restante se decantó por la opción de inconformes.

Cabe destacar que ese 10% que manifestó inconformidad, provino de los funcionarios de la Gerencia de TI, mismos que tienen un panorama más amplio y conocimientos técnicos superiores a los que ostenta el promedio de los usuarios corporativos.

Como se mencionó anteriormente, el resguardo de los sistemas ante ataques externos ha sido un punto acertado de la Gerencia de TI; sin embargo, no se ha desarrollado un plan de respaldo de los datos; aspecto que, muchas veces pasa desapercibido para los usuarios finales pero que, sin duda, constituye un riesgo relevante para la seguridad de la información corporativa.

CAPÍTULO V

DISCUSIÓN E INTERPRETACIÓN DE LOS RESULTADOS

5.1 PROPUESTA DE MEDIDAS DE MEJORA PARA LAS ACTIVIDADES DE CONTROL EN MATERIA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN.

Tras la evaluación de las actividades de control en materia de TI existentes en la Compañía Aceitera El Coco S.A., procede ahora la propuesta de medidas de mejora.

Lo que se ha encontrado en el desarrollo de esta investigación, formula un reto importante para el investigador, pues no se puede proponer simplemente la implementación de un marco de gestión de las tecnologías de información; si primeramente, en la entidad auditada no existen las bases necesarias en cuanto a control interno.

Es por ello, que se va a hacer una propuesta inicial de control interno, con el fin de fundar las bases de un sistema de control interno corporativo, sobre el cual posteriormente, se podría estructurar un marco de gestión de tecnologías de información.

Lo anterior por cuanto si se considera que proponer un marco de sanas prácticas en tecnologías de información sin detenerse analizar y hacer propuestas sobre el control interno *per sé*, lo único que causará es el fracaso del marco propuesto.

5.1.1. Políticas de Control Interno

Observando lo estipulado en el Informe COSO, Ley General de Control Interno y en las Normas de Control Interno para el Sector Público N-2-2009-CO-DFOE; se ha diseñado este breve, pero importante marco de políticas de control interno para la Compañía Aceitera El Coco S.A.

AC	***Ambiente de Control***	
AC.01	***Ambiente de Control***	La Presidencia Ejecutiva y las Gerencias Corporativas, según sus competencias, deben establecer un ambiente de control que se constituya en el fundamento para la operación y el fortalecimiento del sistema de control interno, y, en consecuencia, para el logro de los objetivos corporativos.
AC.02	***Responsabilidad por el Control Interno***	La responsabilidad por el establecimiento, mantenimiento, funcionamiento, perfeccionamiento y evaluación del SCI es inherente al jerarca y a los titulares subordinados, en el ámbito de sus competencias.
AC.03	***Responsabilidad de los funcionarios***	Los funcionarios deben, de manera oportuna, realizar las acciones pertinentes y atender los requerimientos para el debido diseño, implantación, operación, y fortalecimiento de los distintos componentes funcionales del sistema de control interno.
AC.04	***Auditoría Interna***	La empresa debe contar con una auditoría interna, como ente asesor de la junta directiva. Dicha unidad operará con todos los alcances definidos en las Normas Internaciones de la Auditoría y pronunciamientos del Colegio de Contadores Públicos de Costa Rica y del Instituto de Auditores Internos de Costa Rica. La auditoría interna, en cumplimiento de sus funciones, debe brindar servicios de auditoría interna orientados a fortalecer el sistema de control interno.
AC.05	***Ética***	La Presidencia Ejecutiva y las Gerencias Corporativas, según sus competencias, deben propiciar el fortalecimiento de la ética en la gestión, mediante la implantación de medidas e instrumentos formales y la consideración de elementos informales que conceptualicen y materialicen la filosofía, los enfoques, el comportamiento y la gestión éticos de la institución, y que conlleven la integración de la ética a los sistemas de gestión.
AC.06	***Idoneidad del personal***	El personal debe reunir las competencias y valores requeridos, de conformidad con los manuales de puestos, para el desempeño de los puestos y la operación de las actividades de control respectivas. Con

		ese propósito, las políticas y actividades de planificación, reclutamiento, selección, motivación, promoción, evaluación del desempeño, capacitación y otras relacionadas con la gestión de recursos humanos, deben dirigirse técnica y profesionalmente con miras a la contratación, la retención y la actualización de personal idóneo en la cantidad que se estime suficiente para el logro de los objetivos corporativos.
AC.07	***Estructura corporativa***	La Presidencia Ejecutiva y las Gerencias Corporativas, según sus competencias, deben procurar una estructura que defina la organización formal, sus relaciones jerárquicas, líneas de dependencia y coordinación, así como la relación con otros elementos que conforman la institución, y que apoye el logro de los objetivos.
GR	***Gestión de Riesgos***	
GR.01	***Gestión de Riesgos***	La Presidencia Ejecutiva y las Gerencias Corporativas, según sus competencias, deben definir, implantar, verificar y perfeccionar un proceso permanente y participativo de gestión de riesgos corporativos.
GR.02	***Vinculación con la planificación estratégica y operativa***	La gestión del riesgo debe sustentarse en un proceso de planificación que considere la misión y la visión corporativa, así como objetivos, metas, políticas e indicadores de desempeño claros, medibles, realistas y aplicables, establecidos con base en un conocimiento adecuado del ambiente interno y externo en que la institución desarrolla sus operaciones, y, en consecuencia, de los riesgos correspondientes. Asimismo, los resultados de la valoración del riesgo deben ser insumos para realimentar ese proceso de planificación.
GR.03	***Planes estratégicos***	Cada gerencia debe contar con un plan estratégico que esté alineado con el plan estratégico corporativo.
GR.04	***Planes operativos***	Cada gerencia debe contar con un plan anual operativo que contribuya proporcionalmente al logro del plan estratégico gerencial.
AT	***Actividades de Control***	
AT.01	***Actividades de Control***	La Presidencia Ejecutiva y las Gerencias Corporativas, según sus competencias, deben diseñar, adoptar, evaluar y perfeccionar, como parte del sistema de control interno, las actividades de control pertinentes, las que comprenden las políticas, los procedimientos y los mecanismos que contribuyen a asegurar razonablemente la operación y el fortalecimiento del sistema de control interno y el logro de los objetivos corporativos. Dichas actividades deben ser dinámicas, a fin de introducirles las mejoras que procedan en virtud de los requisitos que deben cumplir para garantizar razonablemente su efectividad. El ámbito de aplicación de tales actividades de control debe estar referido a todos los niveles y funciones de la empresa. En ese sentido, la gestión institucional y la operación del sistema de control interno deben contemplar, de acuerdo con los niveles de complejidad y riesgo involucrados, actividades de control de

naturaleza previa, concomitante, posterior o una conjunción de ellas. Lo anterior, debe hacer posible la prevención, la detección y la corrección ante debilidades del sistema de control interno y respecto de los objetivos, así como ante indicios de la eventual materialización de un riesgo relevante.

AT.02 Atributos de las Actividades de Control

a. **Integración a la gestión**. Las actividades de control diseñadas deben ser parte inherente de la gestión corporativa, e incorporarse en ella los principios de eficacia, eficiencia, simplicidad y celeridad.

b. **Respuesta a riesgos.** Las actividades de control deben ser congruentes con los riesgos que se pretende administrar, lo que conlleva su dinamismo de acuerdo con el comportamiento de esos riesgos.

c. **Contribución al logro de los objetivos con un costo razonable.** Las actividades de control deben presentar una relación satisfactoria de costo-beneficio, de manera que su contribución esperada al logro de los objetivos, sea mayor que los costos requeridos para su operación.

d. **Viabilidad.** Las actividades de control deben adaptarse a la capacidad de la empresa de implantarlas, teniendo presente, fundamentalmente, la disponibilidad de recursos, la capacidad del personal para ejecutarlas correcta y oportunamente.

e. **Documentación.** Las actividades de control deben documentarse mediante su incorporación en los manuales de procedimientos, en las descripciones de puestos y procesos, o en documentos de naturaleza similar. Esa documentación debe estar disponible, en forma ordenada conforme a criterios previamente establecidos, para su uso, consulta y evaluación.

f. **Divulgación.** Las actividades de control deben ser de conocimiento general, y comunicarse a los funcionarios que deben aplicarlas en el desempeño de sus cargos. Dicha comunicación debe darse preferiblemente por escrito, en términos claros y específicos.

SI Sistemas de Información

SI.01 Sistemas de Información

La Presidencia Ejecutiva y las Gerencias Corporativas, según sus competencias, deben disponer los elementos y condiciones necesarias para que de manera organizada, uniforme, consistente y oportuna se ejecuten las actividades de obtener, procesar, generar y comunicar, en forma eficaz, eficiente y económica, la información de la gestión corporativa y otra de interés

		para la consecución de los objetivos empresariales. El conjunto de esos elementos y condiciones con las características y fines indicados, se denomina sistema de información, los cuales pueden instaurarse en forma manual, automatizada, o ambas.
SI.02	***Confiabilidad y oportunidad de la información***	La Presidencia Ejecutiva y las Gerencias Corporativas, según sus competencias, deben diseñar, adoptar, evaluar y perfeccionar las actividades de control pertinentes a fin de asegurar razonablemente que se recopile, procese, mantenga y custodie información de calidad sobre el funcionamiento del sistema de control interno y sobre el desempeño empresarial, así como que esa información se comunique con la prontitud requerida a las instancias internas y externas respectivas.
SI.03	***Flexibilidad de los sistemas de información***	Los sistemas de información deben ser lo suficientemente flexibles, de modo que sean susceptibles de modificaciones que permitan dar respuesta oportuna a necesidades cambiantes de la institución.
SI.04	***Armonización de los sistemas de información con los objetivos***	La organización y el funcionamiento de los sistemas de información deben estar integrados a nivel organizacional y ser coherentes con los objetivos institucionales y, en consecuencia, con los objetivos del sistema de control interno. La adecuación de tales sistemas a los objetivos corporativos involucra, entre otros, su desarrollo de conformidad con el plan estratégico corporativo, y con el marco estratégico de las tecnologías de información, cuando se haga uso de estas para su funcionamiento.
SI.05	***Gestión documental***	La empresa debe asegurar razonablemente que los sistemas de información propicien una debida gestión documental corporativa, mediante la que se ejerza control, se almacene y se recupere la información en la organización, de manera oportuna y eficiente, y de conformidad con las necesidades institucionales.
SI.06	***Archivo institucional***	La Presidencia Ejecutiva y las Gerencias Corporativas, según sus competencias, deben implantar, comunicar, vigilar la aplicación y perfeccionar políticas y procedimientos de archivo apropiados para la preservación de los documentos e información que la institución deba conservar en virtud de su utilidad o por requerimiento técnico o jurídico. Lo anterior incluye lo relativo a las políticas y procedimientos para la creación, organización, utilización, disponibilidad, acceso, confidencialidad, autenticidad, migración, respaldo periódico y conservación de los documentos en soporte electrónico, así como otras condiciones pertinentes.
SI.07	***Calidad de la información***	La Presidencia Ejecutiva y las Gerencias Corporativas, según sus competencias, deben asegurar razonablemente que los sistemas de información contemplen los procesos requeridos para recopilar, procesar y generar información que responda a las

		necesidades de los distintos usuarios. Dichos procesos deben estar basados en un enfoque de efectividad y de mejoramiento continuo.
SI.09	***Confiabilidad de la información***	La información debe poseer las cualidades necesarias que la acrediten como confiable, de modo que se encuentre libre de errores, defectos, omisiones y modificaciones no autorizadas, y sea emitida por la instancia competente.
SI.10	***Oportunidad de la información***	Las actividades de recopilar, procesar y generar información, deben realizarse y darse en tiempo a propósito y en el momento adecuado, de acuerdo con los fines corporativos.
SI.11	***Utilidad de la información***	La información debe poseer características que la hagan útil para los distintos usuarios, en términos de pertinencia, relevancia, suficiencia y presentación adecuada, de conformidad con las necesidades específicas de cada destinatario.
SI.12	***Calidad de la Comunicación***	La Presidencia Ejecutiva y las Gerencias Corporativas, según sus competencias, deben establecer los procesos necesarios para asegurar razonablemente que la comunicación de la información se da a las instancias pertinentes y en el tiempo propicio, de acuerdo con las necesidades de los usuarios, según los asuntos que se encuentran y son necesarios en su esfera de acción. Dichos procesos deben estar basados en un enfoque de efectividad y mejoramiento continuo.
SI.13	***Canales y medios de comunicación***	Deben establecerse y funcionar adecuados canales y medios de comunicación, que permitan trasladar la información de manera transparente, ágil, segura, correcta y oportuna, a los destinatarios idóneos dentro y fuera de la empresa.
SI.14	***Destinatarios de la información***	La información debe comunicarse a las instancias competentes, dentro y fuera de la empresa, para actuar con base en ella en el logro de los objetivos institucionales.
SI.15	***Seguridad de la información***	Deben instaurarse los controles que aseguren que la información que se comunica resguarde sus características propias de calidad, y sea trasladada bajo las condiciones de protección apropiadas, según su grado de sensibilidad y confidencialidad. Así también, que garanticen razonablemente su disponibilidad y acceso por parte de los distintos usuarios en la oportunidad y con la prontitud que la requieran.
SI.16	***Control de sistemas de información***	La Presidencia Ejecutiva y las Gerencias Corporativas, según sus competencias, deben disponer los controles pertinentes para que los sistemas de información garanticen razonablemente la calidad de la información y de la comunicación, la seguridad y una clara asignación de responsabilidades y administración de los niveles de acceso a la información y datos sensibles, así como la garantía de confidencialidad de la información que ostente ese carácter.
SG	***Seguimiento del Control Interno***	
SG.01	***Seguimiento del Sistema de Control Interno***	La Presidencia Ejecutiva y las Gerencias Corporativas, según sus competencias, deben diseñar, adoptar,

		evaluar y perfeccionar, como parte del sistema de control interno, actividades permanentes y periódicas de seguimiento para valorar la calidad del funcionamiento de los elementos del sistema a lo largo del tiempo, así como para asegurar que las medidas producto de los hallazgos de auditoría y los resultados de otras revisiones se atiendan de manera efectiva y con prontitud.
SG.02	***Actividades de seguimiento***	a) La comprobación durante el curso normal de las operaciones, de que se estén cumpliendo las actividades de control incorporadas en los procesos y ordenadas por la jerarquía correspondiente. b) Autoevaluaciones periódicas en las que se verifiquen el cumplimiento, validez y suficiencia del sistema de control interno.

5.1.2. Políticas de Sanas Prácticas en la Gestión de las TI

Considerando lo normado en el marco Cobit (Objetivos de Control para Tecnologías de Información y Relacionadas) y en las Normas Técnicas para la Gestión y Control de las Tecnologías de la Información TI N-2-2007-CO-DFOE; se ha adaptado y propuesto el siguiente marco de sanas prácticas en TI para la Compañía Aceitera El Coco S.A.

PO	***Planear y Organizar***	
PO.01	***Plan Estratégico de TI.***	La planeación estratégica de TI es necesaria para gestionar y dirigir todos los recursos de TI en línea con la estrategia y prioridades del negocio. La función de TI y los interesados del negocio son responsables de asegurar que el valor óptimo se consigue desde los proyectos y el portafolio de servicios. El plan estratégico mejora la comprensión de los interesados clave de las oportunidades y limitaciones de TI, evalúa el desempeño actual, identifica la capacidad y los requerimientos de recursos humanos, y clarifica el nivel de investigación requerido. La estrategia de negocio y prioridades se reflejarán en portafolios y se ejecutarán por los planes estratégicos de TI, que especifican objetivos concisos, planes de acción y tareas que están comprendidas y aceptadas tanto por el negocio como por TI.
PO.02	***Arquitectura de la Información***	La función de sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que

contiene las reglas de sintaxis de los datos de la organización, el esquema de clasificación de datos y los niveles de seguridad. Este proceso mejora la calidad de la toma de decisiones gerenciales asegurándose que se proporciona información confiable y segura, y permite racionalizar los recursos de los sistemas de información para igualarse con las estrategias del negocio.

PO.03 ***Comunicar aspiraciones a la Gerencia.***

La dirección debe elaborar un marco de trabajo de control empresarial para TI, y definir y comunicar las políticas. Un programa de comunicación continua se debe implementar para articular la misión, los objetivos de servicio, las políticas y procedimientos, etc., aprobados y apoyados por la dirección. La comunicación apoya el logro de los objetivos de TI y asegura la concienciación y el entendimiento de los riesgos de negocio y de TI. El proceso debe garantizar el cumplimiento de leyes y reglamentos relevantes.

PO.04 ***Riesgos de TI***

Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los interesados (stakeholders) y se debe expresar en términos financieros, para permitirles alinear los riesgos a un nivel aceptable de tolerancia.

AI ***Adquirir e Implementar***

AI.01 ***Identificar Soluciones Automatizadas***

La necesidad de una nueva aplicación o función requiere de un análisis antes de la compra o desarrollo; por ende, es necesaria una definición de necesidades, fuentes alternativas, viabilidad técnica y financiera, análisis de riesgo y de costo - beneficio.

Para este efecto debe existir:

a) Reporte de análisis de riesgos asociados, con los requerimientos del negocio y diseño de soluciones
b) Estudio de factibilidad y formulación de cursos de acción alternativos, con la viabilidad de la solución y planes B y C.
c) Requerimientos, decisión de factibilidad y aprobación: El patrocinador del negocio tiene la decisión final con respecto a la elección de la solución.

AI.02 ***Adquirir y Mantener Software Aplicativo.***

Las aplicaciones deben estar disponibles de acuerdo con los requerimientos del negocio (controles, seguridad y configuración de acuerdo a estándares) en tiempo y costo razonable; considerándose lo siguiente:

a) Diseño de alto nivel: Traducir las necesidades del negocio a especificaciones de diseño de alto nivel para la adquisición de *software*.

b) **Diseño detallado:** Obtener el criterio de aceptación de los requerimientos técnicos del *software* y aprobarlos si cumplen con el diseño de alto nivel.

c) **Control y posibilidad de auditar las aplicaciones:** Implementar controles de negocio, cuando aplique, en controles de aplicación automatizados tal que el procesamiento sea exacto, completo, oportuno, autorizado y auditable.

d) **Seguridad y disponibilidad de las aplicaciones:** Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados y en línea con la clasificación de datos, la arquitectura de la información, la arquitectura de seguridad de la información y la tolerancia a riesgos de la organización.

e) **Desarrollo de *software* aplicativo:** Garantizar que la funcionalidad de automatización se desarrolla de acuerdo con las especificaciones de diseño, los estándares de desarrollo y documentación, los requerimientos de calidad y estándares de aprobación. Asegurar que todos los aspectos legales y contractuales se identifican y direccionan para el *software* aplicativo desarrollado por terceros.

f) **Aseguramiento de la calidad del *software*:** Desarrollar, implementar los recursos y ejecutar un plan de aseguramiento de calidad del *software*, para obtener la calidad que se especifica en la definición de los requerimientos y en las políticas y procedimientos de calidad de la organización.

g) **Administración de los requerimientos de aplicaciones:** Seguir el estado de los requerimientos individuales durante el diseño, desarrollo e implementación.

h) **Mantenimiento de *software* aplicativo:** Desarrollar una estrategia y un plan.

i) **Aseguramiento de la calidad del *software*:** Desarrollar, implementar los recursos y ejecutar un plan de aseguramiento de calidad del *software*, para obtener la calidad que se especifica en la definición de los requerimientos y en las políticas y procedimientos de calidad de la organización.

j) **Administración de los requerimientos de aplicaciones:** Seguir el estado de los requerimientos individuales durante el diseño, desarrollo e implementación.

k) **Mantenimiento de *software* aplicativo:** Desarrollar una estrategia y un plan.

AI.03 ***Adquirir y Mantener Infraestructura Tecnológica***

Se debe contar con procesos para adquirir, implementar y actualizar la infraestructura tecnológica. Además de garantizar que exista un soporte tecnológico continuo

para las aplicaciones del negocio y disponer de un plan de adquisición de tecnología; así como, implantar medidas de control interno, seguridad y auditabilidad.
Se debe contar con un plan para adquirir, implementar y mantener la infraestructura tecnológica de acuerdo con los requerimientos funcionales y técnicos del negocio.
Debe implementarse medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del *hardware* y *software* de la infraestructura para proteger los recursos y garantizar su disponibilidad.

Se debe definir y comprender claramente las responsabilidades al utilizar componentes de infraestructura sensitivos por todos aquellos que desarrollan e integran los componentes de infraestructura. Se debe monitorear y evaluar su uso.
Procédase a establecer el ambiente de desarrollo y pruebas para soportar la efectividad y eficiencia de las pruebas de factibilidad e integración de aplicaciones en infraestructura, en las primeras fases del proceso de adquisición y desarrollo.

AI.04 ***Facilitar la Operación y el Uso***

- El conocimiento sobre los nuevos sistemas debe estar disponible.
- Generar documentación y manuales para usuarios y para TI.
- Garantizar la satisfacción de los usuarios finales mediante ofrecimientos y niveles de servicio.
- Integrar las soluciones de aplicación al proceso del negocio.

Debe **d**esarrollarse un plan para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos.
Transferencia de Conocimiento a la Gerencia del Negocio: Incluye la aprobación de acceso, administración de privilegios, segregación de tareas, controles automatizados del negocio, respaldo/recuperación, seguridad física y archivo de la documentación fuente.
Transferencia de Conocimiento a Usuarios Finales: Los usuarios puedan utilizar con efectividad y eficiencia el sistema de aplicación.
Transferencia de Conocimiento al Personal de Operaciones y Soporte: El personal de soporte técnico y de operaciones deben poder entregar, apoyar y mantener la aplicación y la infraestructura asociada de manera efectiva y eficiente de acuerdo a los niveles de servicio requeridos.
Entrenamiento inicial y continuo, materiales de entrenamiento, manuales de operación, manuales de procedimiento y escenarios de atención al usuario

AI.05 ***Adquirir Recursos de TI***

Software, *Hardware*, personas y servicios, debe definirse y ejecutarse los procedimientos de adquisición, la selección de proveedores, el ajuste de arreglos contractuales y la adquisición en sí.

		Debe existir un procedimiento para establecer, modificar y concluir contratos con todos los proveedores. Adquisición de Recursos de TI: Proteger y hacer cumplir los intereses de la organización en todos los contratos de adquisiciones, incluyendo derechos y obligaciones.
AI.06	***Administrar Cambios.***	Todos los cambios deben administrarse formalmente y controladamente, incluyendo el mantenimiento de emergencias y parches. Los cambios se deben registrar, evaluar y autorizar de previo a la implantación y revisar contra los resultados planeados. Estándares y Procedimientos para cambios formales. Evaluación de Impacto, Priorización y Autorización: Garantizar que todas las solicitudes de cambio se evalúan de una manera estructurada en cuanto a impactos en el sistema operacional y su funcionalidad. Establecer un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia. Mantener actualizados a los solicitantes de cambios y a los interesados relevantes. Siempre que se implanten cambios al sistema, se debe actualizar el sistema asociado y la documentación de usuario y procedimientos correspondientes.
AI.07	***Instalar y Acreditar Soluciones y Cambios***	Los nuevos sistemas necesitan estar funcionales una vez que su desarrollo se completa. Esto requiere de pruebas adecuadas en un ambiente dedicado con datos de prueba relevantes, definir la transición e instrucciones de migración, planear la liberación y la transición en sí al ambiente de producción, y revisar la post-implantación. **Entrenamiento:** Plan definido de entrenamiento e implantación y materiales. **Plan de Prueba:** Tener en cuenta roles, responsabilidades y criterios de entrada y de salida. **Plan de Implantación:** Establecer un plan de implantación y respaldo y vuelta atrás. **Ambiente de Prueba:** Definir y establecer un entorno seguro de pruebas con seguridad, controles internos, prácticas operativas, calidad de datos, requerimientos de privacidad y cargas de trabajo. **Conversión de Sistemas y Datos:** Conversión y migración de infraestructuras. Incluyen pistas de auditoría, respaldo y vuelta atrás. **Pruebas de Cambios:** Pruebas de cambios independientemente en acuerdo con los planes de pruebas definidos antes de la migración al entorno de operaciones. Asegurar que el plan considera la seguridad y el desempeño. **Pruebas de Aceptación Final:** El dueño del proceso de negocio y los interesados de TI evalúan los resultados de los procesos de pruebas. **Promoción a Producción:** Seguimiento de pruebas, controlar la entrega de los sistemas de operaciones. Obtener el VB de los interesados clave. Cuando sea apropiado, ejecutar el sistema en paralelo con el viejo sistema por un tiempo y comparar resultados.

		Revisión posterior a la Implantación: Establecer procedimientos en línea con los estándares de gestión de cambios organizacionales para requerir una revisión posterior a la implantación como conjunto de salida en el plan de implementación.
AI.07	***Autorización para implementar soluciones de TI***	La Gerencia de TI enviará en el segundo trimestre de cada año, invitación a los directores o jefaturas, para que presenten las solicitudes de automatización de sus procesos en caso de que lo requieran. Cada Dirección o jefatura informará por escrito, en el tercer trimestre a la Gerencia de TI, de las necesidades de automatización de sus procesos, constituyendo el 30 de setiembre la última fecha posible de presentación y recepción de tales solicitudes Las solicitudes de automatización que se presenten deberán indicar, con la mayor precisión posible, la necesidad que se requiere satisfacer, y constituirán insumo a la Gerencia de TI para ser remitido a la Gerencia General. Solo en caso de extrema urgencia o necesidad institucional y debidamente justificado por la jefatura de la dependencia interesada, la Gerencia General podrá autorizar, por vía de excepción, el desarrollo de una Solución Tecnológica para una determinada dependencia sin que se encuentre dentro del plan de trabajo de la Gerencia de TI. En tal supuesto, deberá evidenciarse la realización del proyecto priorizado como logro alcanzado en sustitución de alguno de los otros que no se pudieran realizar en razón de la alteración al plan anual operativo. Para desarrollar cualquier tipo de Solución Tecnológica, será la Gerencia de TI la única autorizada para tal efecto. La Gerencia de TI enviará en el segundo trimestre de cada año, invitación a los directores o jefaturas, para que presenten las solicitudes de automatización de sus procesos en caso de que lo requieran.
ES	***Entregar y dar soporte***	
ES.01	***Definir y Administrar los Niveles de Servicio:***	• Contar con una definición documentada y un acuerdo de servicios de TI y de niveles de servicio. • Monitoreo de la satisfacción de los *stakeholders* sobre el cumplimiento de los niveles de servicio. • Alinear los servicios claves de TI con la estrategia corporativa. Debe contarse con un proceso formal entre el cliente y el prestador del servicio (incluyendo roles, tareas, responsabilidades de proveedores y de los clientes).
ES.02	***Administrar los Servicios de Terceros:***	Se deben definir roles, responsabilidades y expectativas en los acuerdos de terceros, así como la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos. También debe minimizarse riesgos por servicios proveídos por terceros.

Identificación de todas las Relaciones con Proveedores: Categorizarlos por tipo de proveedor, significado y criticidad.
Gestión de Relaciones con Proveedores: Formalizar el proceso para cada proveedor.
Administración de Riesgos del Proveedor: Identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener un efectivo servicio de entrega de forma segura y eficiente.
Monitoreo del Desempeño del Proveedor: Proceso para asegurar que el proveedor cumple con los requerimientos actuales y que se adhiere a los acuerdos del contrato. Que sea competitivo.

ES.03 ***Administrar el Desempeño y la Calidad:***

- Proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI.
- Tomar en cuenta las necesidades futuras.

Optimizar el desempeño de la infraestructura, los recursos y las capacidades de TI en respuesta a las necesidades del negocio.
Capacidad y Desempeño Actual: Revisar en intervalos regulares.
Capacidad y Desempeño Futuros: Minimizar el riesgo de interrupciones del servicio por falta de capacidad y degradación del desempeño. Si existiera exceso de capacidad, se redistribuye.
Monitoreo y Reporte: Determinar el desempeño y capacidad de los recursos de TI.

ES.04 ***Garantizar la Continuidad del Servicio:***

- Desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad.
- Minimizar el riesgo de interrupciones mayores en los servicios de TI.

DS4.2 Planes de Continuidad de TI: Reducir el impacto de una interrupción mayor de las funciones y procesos claves. Considerar requerimientos de resistencia, procesamiento alternativo y capacidad de recuperación de los servicios críticos.
DS4.5 Pruebas del Plan de Continuidad de TI: Probarlo regularmente.
DS4.6 Entrenamiento del Plan de Continuidad de TI: Todas las partes involucradas deben ser habilitadas de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre.
DS4.9 Almacenamiento de Respaldos fuera de las Instalaciones: Medios de respaldo, documentación y otros recursos críticos.

ES.05 ***Garantizar la Seguridad de los Sistemas:***

- Proceso de administración de la seguridad.
- Incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI.

Administración de la Seguridad de TI: Al más alto nivel de la organización.
Plan de Seguridad de TI: Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de

seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad. Asegurar que el plan está implementado en las políticas y procedimientos de seguridad junto con las inversiones apropiadas en los servicios, personal, *software* y *hardware*. Comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios.

Administración de Identidad: Todos los usuarios y sus actividades deben ser identificados de manera única. Mecanismos de autenticación.

Administración de Cuentas de Usuario: Procedimientos para solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuarios y privilegios.

Protección de la Tecnología de Seguridad: Garantizar que la tecnología relacionada con la seguridad sea resistente al sabotaje y no revele documentación de seguridad innecesaria.

Administración de Llaves Criptográficas: Políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas.

Prevención, Detección y Corrección de *Software* Malicioso: Medidas preventivas, detectivas y correctivas contra el *malware*.

Seguridad de la Red: *Firewalls*, dispositivos de seguridad, segmentación de redes y detección de intrusos.

Intercambio de Datos Sensitivos: Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles para proporcionar la autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen.

ES.06 ***Educar y Entrenar a los Usuarios:***

- Identificar las necesidades de entrenamiento de cada grupo de usuarios.
- Brindar un entrenamiento efectivo y medir los resultados.
- Proporción de satisfacción de los interesados con el entrenamiento recibido.

Identificación de Necesidades de Entrenamiento y Educación: Un programa de entrenamiento que incluya:

- Estrategias y requerimientos (actuales y futuros del negocio).
- Valores corporativos (ética, cultura de control y seguridad).
- Implementación de nuevo *software* e infraestructura de TI.
- Habilidades, perfiles de competencias y certificaciones
- actuales.
- Métodos de enseñanza.

Impartición del Entrenamiento: Identificar a los grupos objetivos y a sus miembros, mecanismos de impartición eficientes a maestros, instructores y

		consejeros. Control de registro y evaluaciones del desempeño. **Evaluación del Entrenamiento Recibido:** Evaluar el contenido del entrenamiento con respecto a la relevancia, calidad, efectividad, percepción y retención del conocimiento, costo y valor.
ES.07	***Administración de Datos:***	• Procedimientos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios. • Garantizar la calidad, oportunidad y disponibilidad de la información del negocio. **Sistema de Administración de Librerías de Medios:** Inventario de medios almacenados y archivados para asegurar su uso e integridad. **Eliminación:** Procedimientos para asegurar la protección de datos sensitivos y el *software* cuando se eliminan o transfieren. **Respaldo y Restauración:** De sistemas, aplicaciones, datos y documentación en línea. **Requerimientos de Seguridad para la Administración de Datos:** Definir e implementar políticas y procedimientos.
ME	***Monitorear y evaluar***	
ME.01	***Monitorear y evaluar el desempeño de TI***	Se debe definir indicadores de desempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomarse medidas expeditas cuando existan desviaciones entre lo planeado y lo ejecutado.
ME.02	***Monitorear y evaluar el control interno***	Debe establecerse un programa de control interno que se constantemente monitoreado, no solo por la propia entidad sino por parte de terceros.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

6.1.1. El nivel actual de cada uno de los componentes del sistema de control interno en la Compañía Aceitera El Coco S.A. es incipiente.

6.1.2. La Compañía Aceitera El Coco S.A carece manuales de procedimientos, políticas, instructivos, reglamentos o alguna otra forma de actividad de control que regule adecuadamente el uso de las tecnologías de información y el resguardo de la información relevante en la empresa.

6.1.3. En la Compañía Aceitera El Coco S.A no existe una vinculación entre las actividades de control interno en materia de tecnologías de la información con el logro de los objetivos estratégicos empresariales.

6.1.4. Los usuarios de los principales sistemas de información de la empresa, manifiestan estar satisfechos en cuanto al resguardo de dichos sistemas ante ataques externos.

6.1.5. La Compañía Aceitera El Coco S.A no solamente carece de un marco de gestión de tecnologías de la información; sino que, tampoco tiene un marco de sanas prácticas en control interno que sea la base del primer marco referido.

6.2 RECOMENDACIONES

Por todos los aspectos antes señalados, se presenta las siguientes recomendaciones:

6.2.1. Adoptar e implementar el marco de sanas prácticas en control interno sugerido en la presente investigación.

6.2.2. Adoptar e implementar el marco de gestión de tecnologías de la información presentado en la presente investigación.

6.2.3 Crear un Reglamento de Normas y Políticas de TI, procedimientos y políticas sobre el uso de llaves maya, accesos a redes inalámbricas externas, uso de Bluetooth, entre otros.

6.2.4 Formular políticas puntuales de respaldo de datos por parte de los usuarios a través de medios disponibles.

6.2.5. Capacitar a los usuarios sobre la existencia de amenazas informáticas actuales (concepto, medidas preventivas y acciones correctivas) para que estos puedan hacer un uso adecuado de los equipos, programas y correo electrónico.

6.2.6. Capacitar a los usuarios sobre la creación de passwords seguros, protección de archivos y uso correcto de las sesiones de Windows.

6.2.7. Desarrollar medios de respaldos institucionales en locaciones distintas a la sede central de la empresa.

6.2.8. Valorar la política institucional de creación de crear cuentas de correo electrónico con la primera letra del nombre y primer apellido del funcionario para

estimar el nivel de riesgo existente ante un ataque externo e interno vía e mail, para efectos de que definan nuevos sistemas que proporcionen una mayor seguridad a los usuarios contra correos no deseados y masivos de redes.

BIBLIOGRAFÍA

7.1 LIBROS

Sisto, V. (2009). Cambios en el trabajo, identidad e inclusión social en chile: Desafíos para la investigación. Revista Universum, 24(2): 192-216.

Gómez Giovanny. (2001, mayo 11). *Control interno en la organización empresarial*. Recuperado de https://www.gestiopolis.com/control-interno-organizacion-empresarial/

Isaza, A. (2018), Control Interno y Sistema de Gestión de Calidad. Recuperado de http://ebooks7-24.com.uh.remotexs.xyz/stage.aspx?il=&pg=&ed=

Tamayo, M. (2004). El proceso de la Investigación Científica (4.a ed.). Recuperado de http://www.enfermeriaaps.com/portal/?wpfb_dl=4387

Hernández, R., Fernández, C., & Baptista, P. (2014). Metodología de la investigación (6.a ed.). Recuperado de https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

7.2 SITIOS WEB

https://www.welivesecurity.com/la-es/2012/05/31/estudio-estado-seguridad-informacion-corporativa/

https://www2.deloitte.com/content/dam/Deloitte/ec/Documents/deloitte-analytics/Estudios/SeguridadInformacion2017.pdf

https://www.pwc.com.ar/es/publicaciones/assets/encuesta-global-seguridad-informacion-primer-reporte-2018.pdf

https://www.evaluandosoftware.com/estudio-del-nivel-seguridad-la-informacion-empresas-america-latina-2018/

https://delfino.cr/2019/11/contraloria-encuentra-fallas-de-seguridad-en-centros-de-datos-de-de-hacienda

https://www.crhoy.com/tecnologia/costa-rica-recibio-19-millones-de-ciberataques-este-semestre-sector-publico-no-esta-preparado/

https://cnnespanol.cnn.com/2017/05/17/watergate-el-escandalo-que-cambio-la-politica-estadounidense/#0

https://en.wikipedia.org/wiki/Committee_of_Sponsoring_Organizations_of_the_Treadway_Commission

https://pyme.lavoztx.com/componentes-de-la-estructura-de-control-interno-8182.html

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

http://www.eumed.net/libros-gratis/2010d/796/Componentes%20de%20Control%20Interno.htm

https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/COSO-Sesion1.pdf

https://economiatic.com/concepto-de-tic/

https://economipedia.com/definiciones/tecnologias-de-la-informacion-y-comunicacion-tic.html

https://es.wikipedia.org/

https://www.aec.es/web/guest/centro-conocimiento/cobit

https://isaca.org.ar/wp-content/uploads/2017/06/2017-06-13_itti-isaca-cobit-xx-aniversario_radiografc3ada-de-cobit_v01-00.pdf

http://estgesti.blogspot.com/2015/04/itil-v3-2011-cobit-50.html

https://es.wikipedia.org/wiki/Information_Technology_Infrastructure_Library#Estrategia_del_Servicio

https://www.cedia.edu.ec/dmdocuments/publicaciones/Libros/GTI9.pdf

7.3 OTROS DOCUMENTOS

Ley General de Control Interno

Normas de Control Interno para el Sector Público N-2-2009-CO-DFOE

ANEXOS

8.1 DECLARACIÓN JURADA

DECLARACIÓN JURADA

Yo Michael Umaña Rodríguez, mayor de edad, portador de la cédula de identidad número 1-1269-0501 egresado de la carrera de Contaduría Pública de la Universidad Hispanoamericana, hago constar por medio de éste acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de Licenciatura en Contaduría Pública, juro solemnemente que mi trabajo de investigación titulado: Análisis de las Actividades de Control Actuales en materia de Tecnologías de Información y Comunicación de la Compañía El Coco S.A como apoyo para el logro de los objetivos estratégicos corporativos vigentes en el año 2020, es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 del 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte; articulo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad se reserva el derecho de protocolizar este documento ante Notario Público.

En fe de lo anterior, firmo en la ciudad de San José, a los 24 días del mes de Agosto del año dos mil Veinte (20).

Firma del estudiante

Cédula: 1-1269-0501

8.2 CARTA DEL TUTOR

CARTA DEL TUTOR

Cartago, 24 de agosto de 2020

Universidad Hispanoamericana
Contaduría Pública
Sede Llorente

Estimado señor:

El estudiante Michael Umaña Rodríguez, cédula de identidad número 1-1269-0501, me ha presentado, para efectos de revisión y aprobación, el trabajo de investigación denominado "*Análisis de las actividades de control actuales en materia de tecnologías de la información y comunicación de la Compañía Aceitera El Coco S.A. como apoyo para el logro de los objetivos estratégicos corporativos vigentes en el año 2020*", el cual ha elaborado para optar por el grado académico de Licenciatura en Contaduría pública.

En mi calidad de tutor, he verificado que se han hecho las correcciones indicadas durante el proceso de tutoría y he evaluado los aspectos relativos a la elaboración del problema, objetivos, justificación; antecedentes, marco teórico, marco metodológico, tabulación, análisis de datos; conclusiones y recomendaciones.

De los resultados obtenidos por el postulante, se obtiene la siguiente calificación:

a)	ORIGINAL DEL TEMA	10%	10%
b)	CUMPLIMIENTO DE ENTREGA DE AVANCES	20%	18%
C)	COHERENCIA ENTRE LOS OBJETIVOS, LOS INSTRUMENTOS APLICADOS Y LOS RESULTADOS DE LA INVESTIGACION	30%	30%
d)	RELEVANCIA DE LAS CONCLUSIONES Y RECOMENDACIONES	20%	18%
e)	CALIDAD, DETALLE DEL MARCO TEORICO	20%	18%
	TOTAL		94%

En virtud de la calificación obtenida, se avala el traslado al proceso de lectura.

Atentamente,

CARLOS EDUARDO LOPEZ FUENTES (FIRMA)

Digitally signed by CARLOS EDUARDO LOPEZ FUENTES (FIRMA)
Date: 2020.08.25 16:30:39 -06'00'
Reason: Hecho por
Location: Costa Rica, San Jose, San Jose, Carmen

Lic. Carlos Eduardo López Fuentes, MATI
Cédula identidad N 303720378
Miembro 1 606 353 del Institute of Internal Auditors (Global).
Miembro 686 del Instituto de Auditores Internos de Costa Rica.
Miembro 7 508 del Colegio de Contadores Públicos de Costa Rica.
Miembro 23 292 del Colegio de Profesionales en Ciencias Económicas de Costa Rica.

8.3 CARTA DEL LECTOR

Llc. Gustavo Adolfo Chaves Vargas
CPA # 5268 / IAI # 635
Asesorías Contables, Financieras, Tributarias, Administrativas, Servicios de Auditoría y Certificación para Partidos Políticos.

CARTA DEL LECTOR

San José, 1 de Octubre del 2020

MBA. Gerardo Calderón Zuñiga
Director Carrera Contaduría Pública
Universidad Hispanoamericana

Estimado señor:

El estudiante Michael Umaña Rodríguez, cédula de identidad número 1-1269-0501, me ha presentado, para efectos de revisión y aprobación, el trabajo de investigación denominado "ANÁLISIS DE LAS ACTIVIDADES DE CONTROL ACTUALES EN MATERIA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DE LA COMPAÑÍA ACEITERA EL COCO S.A COMO APOYO PARA EL LOGRO DE LOS OBJETIVOS ESTRATÉGICOS CORPORATIVOS VIGENTES EN EL AÑO 2020", el cual ha elaborado para optar por el grado de Licenciatura en Contaduría Pública.

He revisado y he hecho las observaciones relativas al contenido analizado, particularmente, lo relativo a la coherencia entre el marco teórico y el análisis de datos; la consistencia de los datos recopilados y la coherencia entre estos y las conclusiones; asimismo, la aplicabilidad y originalidad de las recomendaciones, en términos de aporte de la investigación. He verificado que se han hecho las modificaciones correspondientes a las observaciones indicadas.

Por consiguiente, este trabajo cuenta con mi aval para ser presentado en la defensa pública.

Cordialmente,

Prof. Gustavo A. Chaves Vargas

Firmado digitalmente por Prof. Gustavo A. Chaves Vargas
Fecha: 2020.10.01 20:44:05 -06'00'

Lic. Gustavo Adolfo Chaves Vargas
Cédula identidad No. 1-0904-0350
Carné Colegio Profesional No. 5268

Cel.: 8320-9635 • e-mail: chavesvg@ice.co.cr / chavesvg@gmail.com

8.4 AUTORIZACIÓN DEL AUTOR PARA CONSULTA

UNIVERSIDAD HISPANOAMERICANA
CENTRO DE INFORMACION TECNOLOGICO (CENIT)
CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DE LOS TRABAJOS FINALES DE GRADUACION

San José, 13 de octubre del 2020

Señores:
Universidad Hispanoamericana
Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito (a) Michael Umaña Rodríguez con número de identificación 1-1269-0501 autor (a) del trabajo de graduación titulado Análisis de las actividades de control actuales en materia de Tecnologías de Información y Comunicación de la Compañía Aceitera El Coco S.A como apoyo para el logro de los objetivos estratégicos corporativos vigentes en el año 2020. presentado y aprobado en el año 2020 como requisito para optar por el título de Licenciatura en Contaduría Pública; (SI / NO) autorizo al Centro de Información Tecnológico (CENIT) para que con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

Cordialmente,

1-1269-0501
Firma y Documento de Identidad

ANEXO 1 (Versión en línea dentro del Repositorio)
LICENCIA Y AUTORIZACIÓN DE LOS AUTORES PARA PUBLICAR Y PERMITIR LA CONSULTA Y USO

Parte 1. Términos de la licencia general para publicación de obras en el repositorio institucional

Como titular del derecho de autor, confiero al Centro de Información Tecnológico (CENIT) una licencia no exclusiva, limitada y gratuita sobre la obra que se integrará en el Repositorio Institucional, que se ajusta a las siguientes características:

a) Estará vigente a partir de la fecha de inclusión en el repositorio, el autor podrá dar por terminada la licencia solicitándolo a la Universidad por escrito.

b) Autoriza al Centro de Información Tecnológico (CENIT) a publicar la obra en digital, los usuarios puedan consultar el contenido de su Trabajo Final de Graduación en la página Web de la Biblioteca Digital de la Universidad Hispanoamericana

c) Los autores aceptan que la autorización se hace a título gratuito, por lo tanto, renuncian a recibir beneficio alguno por la publicación, distribución, comunicación pública y cualquier otro uso que se haga en los términos de la presente licencia y de la licencia de uso con que se publica.

d) Los autores manifiestan que se trata de una obra original sobre la que tienen los derechos que autorizan y que son ellos quienes asumen total responsabilidad por el contenido de su obra ante el Centro de Información Tecnológico (CENIT) y ante terceros. En todo caso el Centro de Información Tecnológico (CENIT) se compromete a indicar siempre la autoría incluyendo el nombre del autor y la fecha de publicación.

e) Autorizo al Centro de Información Tecnológica (CENIT) para incluir la obra en los índices y buscadores que estimen necesarios para promover su difusión.

f) Acepto que el Centro de Información Tecnológico (CENIT) pueda convertir el documento a cualquier medio o formato para propósitos de preservación digital.

g) Autorizo que la obra sea puesta a disposición de la comunidad universitaria en los términos autorizados en los literales anteriores bajo los límites definidos por la universidad en las "Condiciones de uso de estricto cumplimiento" de los recursos publicados en Repositorio Institucional.

SI EL DOCUMENTO SE BASA EN UN TRABAJO QUE HA SIDO PATROCINADO O APOYADO POR UNA AGENCIA O UNA ORGANIZACIÓN, CON EXCEPCIÓN DEL CENTRO DE INFORMACIÓN TECNOLÓGICO (CENIT), EL AUTOR GARANTIZA QUE SE HA CUMPLIDO CON LOS DERECHOS Y OBLIGACIONES REQUERIDOS POR EL RESPECTIVO CONTRATO O ACUERDO.

8.5 ENCUESTA AMBIENTE CONTROL

AUTOEVALUACIÓN CONTROL INTERNO

Instancia:

COMPONENTE SEGUIMIENTO

El seguimiento comprende las actividades que se realizan para valorar la calidad del funcionamiento del sistema de control interno, a lo largo del tiempo; asimismo, para asegurar que los hallazgos de la auditoría y los resultados de otras revisiones se atiendan con prontitud. El modelo de madurez incluye los siguientes cuatro atributos en relación con el seguimiento: 1 - Participantes / 2 - Formalidad / 3 - Alcance / 4 - Contribución a la mejora del sistema de control interno

1.	Participantes en el seguimiento del sistema de control interno	PENDIENTE
¿En qué consiste?	*El liderazgo por el seguimiento del sistema de control interno debe ser asumido por el jefe y compartido con todos los titulares subordinados. Por su parte, los funcionarios tienen una participación activa en las labores de seguimiento continuo y periódico.*	Seleccionar una opción abajo
Opciones	**Señale la opción que describa mejor la situación actual de su entidad, colocando una "X" en la celda correspondiente en la columna de la derecha:**	Colocar una X
A	El seguimiento del sistema de control interno es responsabilidad de una o varias unidades particulares.	
B	El seguimiento periódico del sistema de control interno es ordenado por el jefe a los demás titulares subordinados bajo su cargo, quienes a su vez solicitan a algunos funcionarios que participen en el seguimiento del control interno atinente a las actividades relacionadas con sus puestos. Esto ha generado un reforzamiento del criterio de que el seguimiento requiere la participación de todos los funcionarios.	
C	El seguimiento del sistema de control interno es asumido por el jefe, demás titulares subordinados y todos los demás funcionarios, cada quien en el ámbito de sus competencias.	
D	El seguimiento del sistema de control interno forma parte de las actividades diarias del jefe, demás titulares subordinados y los funcionarios en general, y se promueven revisiones independientes por parte de otras instancias.	
E	Los titulares subordinados han asumido un liderazgo compartido respecto del seguimiento del sistema de control interno; y han instaurado lo mecanismos necesarios para la innovación y MEJORAS continua del sistema.	
SELECCIONAR UNA OPCION		PENDIENTE

Usted como responsable del SCI indique que acción o acciones está dispuesto a emprender en cuanto a la Participación, según lo que establece el Componente Seguimiento, para mejorar la condición de su Sistema de Control Interno.

FORMULACIÓN PLAN DE MEJORAS

PENDIENTE

SEGUIMIENTO PLAN DE MEJORAS

EVALUACIÓN PLAN DE MEJORAS

2.	**Formalidad del seguimiento del sistema de control interno**	**PENDIENTE**
¿En qué consiste?	*El seguimiento del sistema de control interno debe observar un proceso estructurado debidamente oficializado mediante las disposiciones administrativas pertinentes, en relación con el alcance, la periodicidad, las responsabilidades, los mecanismos y las herramientas correspondientes.*	**Seleccionar una opción abajo**
Opciones	**Señale la opción que describa mejor la situación actual de su entidad, colocando una "X" en la celda correspondiente en la columna de la derecha:**	**Colocar una X**
A	Para algunas unidades específicas de la instancia, existen disposiciones sobre el seguimiento que deben ejercer sobre el control interno aplicable a algunas de las actividades que realizan.	
B	El jefe ha emitido disposiciones de tipo general sobre la obligación de los titulares subordinados de dar seguimiento al sistema de control interno, con la colaboración de los funcionarios que corresponda.	
C	Los titulares subordinados han instaurado regulaciones formales sobre el seguimiento del sistema de control interno, requiriendo que éste se realice vigilando la eficacia de las actividades de control en las operaciones diarias y que se lleve a cabo una autoevaluación anual del sistema de control interno y se elabore un plan de mejoras.	
D	Las regulaciones cubren todos los aspectos relacionados con el seguimiento continuo y periódico interno y externo, así como con la implementación y la verificación de las mejoras que se determinen, sean éstas de carácter operativo o estratégico.	
E	El seguimiento del sistema de control interno es un proceso estructurado que incorpora revisiones de diversos tipos y herramientas flexibles. Los esfuerzos realizados en torno a este componente del control interno han contribuido a que se convierta en parte de la cultura institucional.	
SELECCIONAR UNA OPCION		**PENDIENTE**

Usted como responsable del SCI indique que acción o acciones está dispuesto a emprender en cuanto a la Formalidad, según lo que establece el Componente Seguimiento, para mejorar la condición de su Sistema de Control Interno.

FORMULACIÓN PLAN DE MEJORAS

PENDIENTE

SEGUIMIENTO PLAN DE MEJORAS

EVALUACIÓN PLAN DE MEJORAS

3.	Alcance del seguimiento del sistema de control interno	PENDIENTE
¿En qué consiste?	*El seguimiento del sistema de control interno debe abarcar el funcionamiento, la suficiencia y la validez del sistema, su contribución al desempeño institucional y al logro de los objetivos, y el grado en que los componentes funcionares se han establecido e integrado en el accionar institucional. Asimismo, debe comprender actividades permanentes y periódicas, y la implantación de las mejoras que se determinen.*	Seleccionar una opción abajo
Opciones	**Señale la opción que describa mejor la situación actual de su entidad, colocando una "X" en la celda correspondiente en la columna de la derecha:**	Colocar una X
A	Existen labores aisladas de seguimiento del sistema de control interno con un alcance limitado a algunos controles específicos, las cuales se ponen de manifiesto mediante la vigilancia que, de manera rutinaria, ejercen los titulares sobre el cumplimiento de algunas actividades.	
B	Los titulares subordinados vigilan las actividades bajo su control con una visión de corto plazo y en procura del cumplimiento de las obligaciones legales que establece el ordenamiento.	
C	El seguimiento del sistema de control interno y sus mecanismos se han integrado a las actividades organizacionales, y en lo procedente se han incorporado en la documentación de los puestos y procesos. En ese sentido, los funcionarios aplican las actividades de seguimiento que les corresponden, y en esos esfuerzos son supervisados por los titulares subordinados, quienes a su vez realizan un seguimiento general sobre las unidades a su cargo, con la orientación del jefe.	
D	El seguimiento del sistema de control interno se ha convertido en un proceso formal para una valoración y mejora permanente del sistema de control interno en el que todos los participantes asumen sus responsabilidades.	
E	El seguimiento del sistema de control interno se realiza con un enfoque estratégico, y cubre el control de las actividades cotidianas, revisiones puntuales y el monitoreo de las mejoras acordadas	
SELECCIONAR UNA OPCION		PENDIENTE

Usted como responsable del SCI indique que acción o acciones está dispuesto a emprender en cuanto al Alcance, según lo que establece el Componente Seguimiento, para mejorar la condición de su Sistema de Control Interno.

FORMULACIÓN PLAN DE MEJORAS

PENDIENTE

SEGUIMIENTO PLAN DE MEJORAS

EVALUACIÓN PLAN DE MEJORAS

4.	Contribución del seguimiento a la mejora del sistema de control interno	PENDIENTE
¿En qué consiste?	*Como resultado del seguimiento del sistema de control interno, deben determinarse las mejoras que procedan, las cuales se calendarizan en un plan de implementación que, a su vez, será objeto de verificación en términos de su aplicación conforme a lo planeado y de la efectividad de las medidas adoptadas para fortalecer dicho sistema.*	**Seleccionar una opción abajo**
Opciones	**Señale la opción que describa mejor la situación actual de su entidad, colocando una "X" en la celda correspondiente en la columna de la derecha:**	**Colocar una X**
A	La contribución del seguimiento a la mejora del sistema de control interno es mínima.	
B	El seguimiento y permite detectar algunas oportunidades de mejora del sistema de control interno.	
C	El seguimiento del sistema de control interno constituye una herramienta que permite la valoración y mejora de dicho sistema y de su contribución a la gestión.	
D	Mediante la ejecución cotidiana de labores de seguimiento en el desarrollo de las actividades organizacionales, constantemente se introducen mejoras sustanciales en el desempeño organizacional y en el sistema de control interno. Adicionalmente, se realizan valoraciones específicas del sistema de control interno, y se implementan las mejoras necesarias.	
E	El proceso de seguimiento se mejora constantemente, con lo que se incrementan sus aportes al valor, a la gestión y al sistema de control interno institucionales, así como la identificación de nuevos modos de gestión y de control.	
SELECCIONAR UNA OPCION		**PENDIENTE**

Usted como responsable del SCI indique que acción o acciones está dispuesto a emprender para el Fortalecimiento, según lo que establece el Componente Seguimiento, para mejorar la condición de su Sistema de Control Interno.

FORMULACIÓN PLAN DE MEJORAS

PENDIENTE

SEGUIMIENTO PLAN DE MEJORAS

EVALUACIÓN PLAN DE MEJORAS

8.6 ENCUESTA VALORACIÓN DE RIESGOS

AUTOEVALUACIÓN CONTROL INTERNO

Instancia:

COMPONENTE VALORACIÓN DEL RIESGO

La valoración del riesgo conlleva la identificación y el análisis de los riesgos que enfrenta la organización, tanto de fuentes internas como externas relevantes para la consecución de los objetivos; deben ser realizados por el jerarca y titulares subordinados, con el fin de determinar cómo se deben administrar dichos riesgos. Es fundamental para el logro de los objetivos de la planificación estratégica, táctica y operativa de la entidad. El modelo de madurez contempla los siguientes cuatro atributos en relación con la valoración del riesgo: 2.1 - Marco orientador / 2.2 - Herramienta para la administración de la información / 2.3 - Funcionamiento del SEVRI / 2.4 - Documentación y comunicación

1.	Marco orientador	PENDIENTE
¿En qué consiste?	*Debe establecerse un marco orientador para la valoración del riesgo institucional que comprenda la política de valoración del riesgo, la estrategia del Sistema Específico de Valoración del Riesgo Institucional y la normativa interna que regule este último. Las tres anteriores, deben ser aprobadas por el Jerarca, divulgadas a toda la organización y aplicadas por todos los funcionarios.*	**Seleccionar una opción abajo**
Opciones	**Señale la opción que describa mejor la situación actual de su entidad, colocando una "X" en la celda correspondiente en la columna de la derecha:**	**Colocar una X**
A	- El riesgo es entendido de diferentes maneras por los titulares subordinados y los funcionarios en general de la instancia. - La conciencia sobre la importancia de llevar a cabo una valoración del riesgo como medio para conducir las operaciones organizacionales con eficiencia, es apenas incipiente, y se pone de manifiesto sólo en algunas áreas. - En la instancia se conoce vagamente las disposiciones del marco jurídico y técnico en materia de valoración del riesgo.	
B	- Se realiza la actividad de Valoración del Riesgo solo con la participación del titular subordinado, jefe de la instancia y el enlace. - Los titulares subordinados tienen la percepción de que la valoración del riesgo agrega poco valor a la organización. - Los titulares subordinados han emitido orientaciones básicas sobre las acciones que deberán efectuarse a corto plazo para llevar a cabo una valoración del riesgo y no tienen una noción clara de los parámetros institucionales de aceptabilidad de riesgos, aprobados por el jerarca.	

C	- La valoración de los riesgos es realizada con la participación de todos los responsables de los procesos que se llevan en la instancia. El significado del concepto de riesgo es uniforme para todos y ampliamente compartido. - La instancia ha establecido metas específicas sobre los riesgos relevantes. Se determinan los resultados esperados de la valoración del riesgo en tiempo y espacio, los recursos necesarios y sus responsables. - La política, la estrategia y la normativa de valoración del riego, así como los parámetros de aceptabilidad de riesgos, aprobados por el jerarca, han sido divulgados por el jefe a toda la organización.	
D	- La Valoración de los riesgos es revisada constantemente y se actualiza en función de los cambios en el entorno y de la normativa aplicable. - Se cuenta con mecanismos instaurados para la divulgación oportuna de los cambios en los riesgos y demás asuntos relacionados con el Sistema Específico de Valoración del Riesgo Institucional. - La política, la estrategia y la normativa institucionales de valoración de riesgos son dadas a conocer a todos los funcionarios oportunamente por los titulares subordinados.	
E	- Se han instaurado procesos para la investigación constante sobre valoración del riesgo y su afectación por cambios en el entorno, y se promueve la generación de iniciativas innovadoras y su implementación. - La convicción sobre la importancia la valoración de los riesgos ha calado profundamente en el accionar organizacional, lo que ha generado una actitud proactiva e investigativa para la mejora constante de los esfuerzos sobre el particular. - Las acciones emprendidas con base en los conocimientos sobre la política, la estrategia y la normativa institucionales de valoración de riesgos y su afectación por parte del entorno se actualizan periódicamente conforme avanza el conocimiento sobre el tema y en procura del aprovechamiento de oportunidades de mejora de la gestión.	
SELECCIONAR UNA OPCION		**PENDIENTE**

Usted como responsable del SCI indique que acción o acciones está dispuesto a emprender en cuanto a dar a conocer el Marco Orientador, según lo que establece el Componente Valoración del Riesgo, para mejorar la condición de su Sistema de Control Interno.

FORMULACIÓN PLAN DE MEJORAS

SEGUIMIENTO PLAN DE MEJORAS

EVALUACIÓN PLAN DE MEJORAS

2.	**Herramienta para la administración de la información**	**PENDIENTE**
¿En qué consiste?	*Debe establecerse una herramienta para la gestión y documentación de la información que utilizará y generará el Sistema Específico de Valoración del Riesgo Institucional, la cual podrá ser de tipo manual, computadorizada o una combinación de ambos.*	**Seleccionar una opción abajo**
Opciones	**Señale la opción que describa mejor la situación actual de su entidad, colocando una "X" en la celda correspondiente en la columna de la derecha:**	**Colocar una X**

A	Los titulares subordinados administran de manera precaria la información sobre los riesgos que analizan, utilizando los recursos informáticos disponibles en sus instancias.	
B	Los titulares subordinados han interiorizado la definición de los alcances de la herramienta para la administración de la información sobre los riesgos organizacionales.	
C	Se sabe utilizar la herramienta para la administración de la información sobre los riesgos, cuyo alcance es congruente con el marco orientador de valoración del riesgo.	
D	La información incluida en la herramienta para la administración de la información sobre los riesgos se monitorea y ajusta constantemente a las necesidades del entorno.	
E	La herramienta para la administración de la información provee oportunamente a los titulares subordinados, alertas de nuevos riesgos o de cambios en los riesgos existentes.	
SELECCIONAR UNA OPCION		**PENDIENTE**

Usted como responsable del SCI indique que acción o acciones está dispuesto a emprender en cuanto al manejo de la Herramienta para la aplicación del SEVRI, según lo que establece el Componente Valoración del Riesgo, para mejorar la condición de su Sistema de Control Interno.

FORMULACIÓN PLAN DE MEJORAS

PENDIENTE

SEGUIMIENTO PLAN DE MEJORAS

EVALUACIÓN PLAN DE MEJORAS

3.	**Funcionamiento del SEVRI**	**PENDIENTE**
¿En qué consiste?	*Deben ejecutarse actividades para la identificación, análisis, evaluación, administración y revisión por áreas, sectores, actividades o tareas, de conformidad con las particularidades de la institución.*	**Seleccionar una opción abajo**
Opciones	**Señale la opción que describa mejor la situación actual de su entidad, colocando una "X" en la celda correspondiente en la columna de la derecha:**	**Colocar una X**
A	- Los titulares subordinados realizan una valoración intuitiva de algunos riesgos que afectan las actividades de las unidades orgánicas que dirigen. - Las autoridades tienen una noción mínima de cuáles son los riesgos más relevante, y definen, en consecuencia con esa noción, los controles que deben aplicarse. - Las autoridades están atentas a la eficacia de los controles que han aplicado en relación con los riesgos que han determinado de manera intuitiva.	
B	- Los titulares subordinados han identificado al menos los eventos que podrían afectar de forma significativa el cumplimiento de los objetivos establecidos, así como sus causas internas y externas y las posibles consecuencias. - Con base en su experiencia y en las discusiones que llevan a cabo, las autoridades priorizan los riesgos con fundamento en criterios básicos no oficializados, a fin de determinar y aplicar medidas que permitan atacar sus causas y en caso necesario, enfrentar sus consecuencias. - Las autoridades procuran dar seguimiento a los eventos riesgosos, a fin de lograr acuerdos sobre la atención que deben brindárseles y las acciones que deben emprenderse en relación con ellos.	

C	- Los titulares subordinados conocen los riesgos relevantes y analizan las medidas que se han tomado para administrarlos. - Los parámetros de aceptabilidad de riesgos institucionales son aplicados para analizar y priorizar los riesgos con base en su nivel, dado por la combinación de probabilidad de ocurrencia y la magnitud de su eventual impacto. - Los riesgos se revisan periódicamente con base en los parámetros de aceptabilidad de riesgos, a fin de determinar variaciones en su nivel, medido por la combinación de su posibilidad de ocurrencia y la magnitud de su eventual impacto.	
D	- Se da una participación activa de diversos actores de la instancia, en procesos regulares de identificación y análisis de riesgos relevantes, como medio para ajustar o actualizar las medidas de administración respectivas. - Las autoridades participan de manera directa en el análisis y la administración de los riesgos que merecen atención prioritaria, en tanto que tales actividades se ejecutan, en relación con otros riesgos, por partes de diferentes niveles, con base en el conocimiento que se ha logrado generalizar en la entidad. - Se da seguimiento al nivel de riesgo, a los factores de riesgo, y al grado de ejecución, la eficacia y la eficiencia de la medidas para la administración de riesgo.	
E	- La valoración de riesgos está inmersa en las actividades diarias, y permite anticipar condiciones que podrían incidir en la consecución de los objetivos organizacionales, así como emprender las acciones correspondientes. - Se cuenta con mecanismos y procedimientos que propician un análisis constante de los riesgos, basados en la Política Institucional, a fin de ajustar oportunamente las medidas de administración vigentes. - Constantemente y de manera sistemática se evalúa la información que suministra el Sistema Específico de Valoración del Riesgo Institucional y se ajustan las medidas para la administración de riesgos.	
SELECCIONAR UNA OPCION		**PENDIENTE**

Usted como responsable del SCI indique que acción o acciones está dispuesto a emprender en cuanto al Funcionamiento del SEVRI, según lo que establece el Componente Valoración del Riesgo, para mejorar la condición de su Sistema de Control Interno.

FORMULACIÓN PLAN DE MEJORAS

PENDIENTE

SEGUIMIENTO PLAN DE MEJORAS

EVALUACIÓN PLAN DE MEJORAS

4.	**Documentación y comunicación**	**PENDIENTE**
¿En qué consiste?	*Deben establecer actividades permanentes del proceso de valoración del riesgo referidas a la documentación y comunicación, que consisten en el registro y la sistematización de información asociada con los riesgos, así como la preparación, distribución y actualización de información sobre los riesgos.*	**Seleccionar una opción abajo**
Opciones	**Señale la opción que describa mejor la situación actual de su entidad, colocando una "X" en la celda correspondiente en la columna de la derecha:**	**Colocar una X**

A	- La información sobre riesgos consta únicamente en la documentación elaborada por el titular subordinado acerca del análisis que ha efectuado en relación con las situaciones que afectan las labores de la unidad orgánica que dirige. - La documentación de los riesgos se efectúa sin haber definido los elementos mínimos que debe contemplar. - La documentación de los riesgos es mantenida por la jefatura, y sólo eventualmente se comparte con las áreas que conforman la instancia.	
B	- Se cuenta con información sobre eventos que podrían afectar de forma significativa el cumplimiento de los objetivos establecidos, así como sus causa internas y externas y las posibles consecuencias, misma que está a disposición de los funcionarios de la instancia. - Se cuenta con una definición de los elementos mínimos que deben documentarse acerca de los riesgos. - La instancia ha establecido algunos mecanismos de coordinación y comunicación en relación con el Sistema Específico de Valoración del Riesgo Institucional.	
C	- Se documentan los elementos mínimos sobre los riesgos (probabilidad y consecuencia de materialización de los riesgos, nivel de riesgos y medidas de administración), y dicha documentación está disponible para los funcionarios de la instancia. - La instancia ha establecido y aplica de manera sistemática, mecanismos de documentación y comunicación sobre riesgos. - Se han definido los usos de la información que genera la revisión de riesgos.	
D	- Se revisa, ajusta y difunde periódicamente la información disponible sobre los riesgos y sus elementos fundamentales, con la participación de diferentes áreas de la instancia, a quienes se reconoce como “dueños de las actividades” y, en consecuencia, como fuentes de información sobre el comportamiento de los riesgos y la eficacia de su documentación. - Los mecanismos de documentación y comunicación se evalúan para determinar su efectividad. - La información sobre los riesgos institucionales está disponible, es completa y se ajusta a las necesidades de los usuarios.	
E	- Se cuenta con mecanismos y procedimientos que garantizan razonablemente la revisión y actualización permanente de la información sobre los riesgos, la cual se evalúa y se ajusta de acuerdo con los requerimientos del entorno. - Se han instaurado procesos para la documentación de riesgos, que promuevan la generación de iniciativas innovadoras. - Se han instaurado procesos para la comunicación de riesgos, que promuevan la generación de iniciativas innovadoras.	
SELECCIONAR UNA OPCION		**PENDIENTE**

Usted como responsable del SCI indique que acción o acciones está dispuesto a emprender en cuanto a la Documentación y Comunicación del SEVRI, según lo que establece el Componente Valoración del Riesgo, para mejorar la condición de su Sistema de Control Interno.

FORMULACIÓN PLAN DE MEJORAS

PENDIENTE

SEGUIMIENTO PLAN DE MEJORAS

EVALUACIÓN PLAN DE MEJORAS

8.7 ENCUESTA ACTIVIDADES DE CONTROL

AUTOEVALUACIÓN CONTROL INTERNO

Instancia :

COMPONENTE ACTIVIDADES DE CONTROL

La Ley General de Control Interno define las actividades de control como políticas y procedimientos que permiten obtener la seguridad de que se llevan a cabo las disposiciones emitidas por la Contraloría General de la República, por el jerarca y los titulares subordinados para la consecución de los objetivos del sistema de control interno. Los analizaremos según los siguientes atributos respecto de las actividades de control:
1 - Características / 2 - Alcance / 3 - Formalidad / 4 - Aplicación

1.	Características de las actividades de control	PENDIENTE
¿En qué consiste?	*Las actividades de control deben reunir las siguientes características:* *a) Integración a la gestión* *b) Respuesta a riesgos* *c) Contribución al logro de los objetivos a un costo razonable (costo-beneficio)* *d) Viabilidad* *e) Documentación en manuales de procedimientos, descripciones de puestos u otros documentos similares* *f) Divulgación entre los funcionarios que deben aplicarlas en el desempeño de sus cargos*	Seleccionar una opción abajo
Opciones	**Señale la opción que describa mejor la situación actual de su entidad, colocando una "X" en la celda correspondiente en la columna de la derecha:**	Colocar una X
A	Las actividades de control se han establecido con base en prácticas tradicionales, y sólo en algunos casos se considera su costo.	
B	Las actividades de control se dirigen a algunos eventos que podrían afectar negativamente el logro de los objetivos institucionales.	
C	Las actividades de control reúnen las características requeridas, a saber: integración a la gestión, respuesta a riesgos, costo-beneficio, viabilidad, documentación y divulgación.	
D	Continuamente se evalúa el funcionamiento de las actividades de control en la gestión, procurando que sus características se mantengan.	
E	Se han instaurado mecanismos para la investigación e innovación de temas atinentes a las actividades de control propias de la institución, lo que permite que éstas se ajusten de manera dinámica oportuna, conforme cambian los riesgos institucionales.	
SELECCIONAR UNA OPCION		PENDIENTE
Usted como responsable del SCI indique que acción o acciones está dispuesto a emprender en cuanto a las Características, según lo que establece el Componente Actividades de Control, para mejorar la condición de su Sistema de Control Interno.		

FORMULACIÓN PLAN DE MEJORAS

PENDIENTE

SEGUIMIENTO PLAN DE MEJORAS

EVALUACIÓN PLAN DE MEJORAS

2.	**Alcance de las actividades de control**	**PENDIENTE**
¿En qué consiste?	*Las actividades de control deben cubrir todos los ámbitos de la gestión institucional y contribuir al logro de los objetivos del sistema de control interno.*	**Seleccionar una opción abajo**
Opciones	**Señale la opción que describa mejor la situación actual de su entidad, colocando una "X" en la celda correspondiente en la columna de la derecha:**	**Colocar una X**
A	Las actividades de control vigentes en la instancia se orientan a la protección de algunos activos y a la prevención de fraude.	
B	Las actividades de control establecidas se refieren, fundamentalmente, a la administración y custodia de los activos y al mantenimiento de algunos registros.	
C	Se cuenta con actividades de control referidas al mantenimiento y la verificación de documentación y registros sobre la gestión organizacional.	
D	Existen actividades de control para todos los alcances de la gestión organizacional, en sus ámbitos operativo y estratégico, las cuales se evalúan constantemente.	
E	Se aplican mecanismos para la búsqueda de medios innovadores para garantizar el cumplimiento de los objetivos, los cuales se traducen en actividades de control analizadas y documentadas.	
SELECCIONAR UNA OPCION		**PENDIENTE**

Usted como responsable del SCI indique que acción o acciones está dispuesto a emprender en cuanto al Alcance, según lo que establece el Componente Actividades de Control, para mejorar la condición de su Sistema de Control Interno.

FORMULACIÓN PLAN DE MEJORAS

PENDIENTE

SEGUIMIENTO PLAN DE MEJORAS

EVALUACIÓN PLAN DE MEJORAS

3.	Formalidad de las actividades de control	PENDIENTE
¿En qué consiste?	*Los requisitos de las actividades de control de control incluyen su documentación y comunicación, para lo cual se tiene como condición previa que sean oficializadas mediante su aprobación por las autoridades institucionales competentes.*	Seleccionar una opción abajo
Opciones	**Señale la opción que describa mejor la situación actual de su entidad, colocando una "X" en la celda correspondiente en la columna de la derecha:**	Colocar una X
A	- Sólo algunas actividades de control están documentadas en breves descripciones de funciones y puestos; otras se han dispuesto mediante instrucciones a funcionarios específicos. - La documentación de las actividades de control es mantenida por el jefe de la unidad, y sólo se dan a conocer a los funcionarios que deben aplicarlas.	
B	- Las actividades de control están documentadas mediante políticas, procedimientos, normas, lineamientos u otros similares. - La mayor parte de las actividades de control vigentes se han comunicado a los funcionarios de la instancia.	
C	- La preparación, actualización y difusión de la documentación relativa a las actividades de control es una práctica normal y debidamente regulada en la instancia. - Las actividades de control son de conocimiento de los funcionarios de la instancia, y su documentación se mantiene disponible para su consulta por los funcionarios de la instancia que deseen consultarla.	
D	- Los titulares subordinados han establecido y aplican mecanismos adecuados para mantener actualizada y comunicar oportunamente, la información relativa a las actividades de control. - Existe apertura de las autoridades superiores para recibir comentarios y sugerencias para el fortalecimiento de dichas actividades. - Las nuevas actividades de control y las actualizaciones de las existentes se comunican oportunamente a los funcionarios encargados de su aplicación. - La documentación relativa a las actividades de control vigentes se tiene disponible en medios de acceso general para su consulta y retroalimentación por los funcionarios.	
E	- La documentación de las actividades de control se depura y actualiza constantemente, con la participación activa de los funcionarios atinentes, bajo el liderazgo de las autoridades organizacionales (jefe y demás titulares subordinados). - Existe plena conciencia sobre la importancia de que los funcionarios conozcan las actividades de control y su documentación, para que puedan hacer aportes de valor para su fortalecimiento constante. Por ello, constantemente se aplican métodos innovadores en procura de que el proceso de documentación y comunicación de las actividades de control sea participativo y generalizado.	
SELECCIONAR UNA OPCION		PENDIENTE

Usted como responsable del SCI indique que acción o acciones está dispuesto a emprender en cuanto a la Formalidad, según lo que establece el Componente Actividades de Control, para mejorar la condición de su Sistema de Control Interno.

FORMULACIÓN PLAN DE MEJORAS

PENDIENTE

SEGUIMIENTO PLAN DE MEJORAS

EVALUACIÓN PLAN DE MEJORAS

4.	Aplicación de las actividades de control	PENDIENTE
¿En qué consiste?	*Las actividades de control deben estar integradas a los procesos institucionales, y su aplicación convertirse en una práctica normal, casi cultural, por parte de los funcionarios de la institución.*	**Seleccionar una opción abajo**
Opciones	**Señale la opción que describa mejor la situación actual de su entidad, colocando una "X" en la celda correspondiente en la columna de la derecha:**	**Colocar una X**
A	- Se aplican solo algunas actividades de control obligatorias para proseguir con algún trámite específico. - Los supervisores o jefes son los encargados de asegurarse de que se cumplan las actividades de control vigentes, lo que realizan periódicamente.	
B	- Algunos funcionarios aplican Las actividades de control establecidas. - Los titulares subordinados han instaurado mecanismos para asegurar la aplicación de Las actividades de control.	
C	- Las actividades de control se han integrado a los procesos organizacionales. - Los funcionarios responsables de ejecutar las actividades de control están atentos a su efectividad y comunican sus recomendaciones a los titulares subordinados correspondientes.	
D	- La aplicación de las actividades de control contempla el comportamiento de los riesgos. - Los titulares subordinados han establecido y aplican mecanismos para la ejecución de revisiones periódicas de las actividades de control.	
E	- Los titulares subordinados han asumido un liderazgo compartido respecto del seguimiento del sistema de control interno; y han instaurado los mecanismos necesarios para la innovación y mejora continua del sistema.	
SELECCIONAR UNA OPCION		**PENDIENTE**

Usted como responsable del SCI indique que acción o acciones está dispuesto a emprender en cuanto a la Aplicación, según lo que establece el Componente Actividades de Control, para mejorar la condición de su Sistema de Control Interno.

FORMULACIÓN PLAN DE MEJORAS

PENDIENTE

SEGUIMIENTO PLAN DE MEJORAS

EVALUACIÓN PLAN DE MEJORAS

8.8 ENCUESTA SISTEMAS DE INFORMACIÓN

AUTOEVALUACIÓN CONTROL INTERNO

Instancia :

COMPONENTE SISTEMAS DE INFORMACIÓN

Los sistemas de información son los elementos y condiciones necesarias para que de manera organizada, uniforme, consistente y oportuna se ejecuten las actividades de obtener, procesar, generar y comunicar la información de la gestión institucional y otra de interés para la consecución de los objetivos institucionales. Los analizaremos según los siguientes atributos en relación con los sistemas de información:
1 - Alcance de los sistemas de información / 2 - Calidad de la información / 3 - Calidad de la comunicación / 4 - Control de los sistemas de información

1.	Alcance de los sistemas de información	PENDIENTE
¿En qué consiste?	*Los sistemas de información deben asegurar razonablemente la recopilación, el procesamiento y el mantenimiento de información sobre el entorno, la institución y su desempeño, así como la comunicación de esa información a las instancias internas y externas que la requieran.*	**Seleccionar una opción abajo**
Opciones	**Señale la opción que describa mejor la situación actual de su entidad, colocando una "X" en la celda correspondiente en la columna de la derecha:**	**Colocar una X**
A	- Se recopila, procesa y comunica información para cumplir con algunos requerimientos específicos que se presentan a la instancia. - La jefatura ha realizado esfuerzos aislados para el procesamiento, generación y comunicación de información relativa a las actividades a su cargo.	
B	- Se han establecido mecanismos para la comunicación de la información pertinente a los diferentes usuarios. - Los sistemas de información contemplan la mayor parte de las actividades organizacionales, y en el desarrollo de algunos de ellos se han incorporado componentes digitales, tomando como referencia la necesidad de una gestión documental que permita satisfacer los requerimientos de la organización.	
C	- El diseño y el desarrollo de los sistemas de información en la instancia se fundamentan en una estrategia formal debidamente armonizada con los objetivos institucionales. - Los sistemas de información cubren, de manera integrada, la mayor parte de las actividades que se realizan en la instancia. Como parte de ellos, el archivo de gestión funciona de manera técnica y profesional.	
D	- Los sistemas de información permiten obtener, procesar, almacenar y recuperar información relevante sobre la gestión y el entorno organizacionales, así como comunicarla a los usuarios que la requieren. - Los sistemas de información están incorporados en el accionar organizacional, tanto a nivel operativo como estratégico, y se someten constantemente a revisiones para incorporarles las mejoras pertinentes.	

E	- Los sistemas de información permiten una gestión de la información externa e interna con un nivel óptimo de seguridad en cuanto a su calidad y oportunidad, como medio para la toma de decisiones por todos los usuarios. - Los sistemas de información incorporan los mecanismos y previsiones necesarias para la incorporación de iniciativas innovadoras y proactivas.	
SELECCIONAR UNA OPCION		**PENDIENTE**

Usted como responsable del SCI indique que acción o acciones está dispuesto a emprender en cuanto al Alcance, según lo que establece el Componente Sistemas de Información, para mejorar la condición de su Sistema de Control Interno.

FORMULACIÓN PLAN DE MEJORAS

PENDIENTE

SEGUIMIENTO PLAN DE MEJORAS

EVALUACIÓN PLAN DE MEJORAS

2.	**Calidad de la información**	**PENDIENTE**
¿En qué consiste?	*Los SI deben recopilar, procesar y genera información que responda a la necesidad de los diversos usuarios, con un enfoque de efectividad y de mejoramiento continuo, y teniendo en cuenta los atributos de confiabilidad, oportunidad y utilidad que esa información debe reunir.*	**Seleccionar una opción abajo**
Opciones	**Señale la opción que describa mejor la situación actual de su entidad, colocando una "X" en la celda correspondiente en la columna de la derecha:**	**Colocar una X**
A	Algunos sistemas de información generan la información necesaria para la atención de ciertos requerimientos específicos.	
B	Se han instaurado algunos procesos para la generación de información que responda a las necesidades de los diferentes usuarios.	
C	Los sistemas de información generan la información requerida para el cumplimiento de los objetivos organizacionales. La información generada por los sistemas reúne los atributos de confiabilidad, oportunidad y utilidad.	
D	En el diseño y la mejora constante de los sistemas de información contemplan las necesidades según los fines institucionales, y se realizan los ajustes pertinentes en procura de una mayor utilidad y flexibilidad de la información.	
E	Los sistemas de información se basan en procesos que consideran la dinámica del entorno y la anticipación e innovación necesarias para la consecución de los fines institucionales.	
SELECCIONAR UNA OPCION		**PENDIENTE**

Usted como responsable del SCI indique que acción o acciones está dispuesto a emprender en cuanto a la Calidad de la Información, según lo que establece el Componente Sistemas de Información, para mejorar la condición de su Sistema de Control Interno.

FORMULACIÓN PLAN DE MEJORAS

PENDIENTE

SEGUIMIENTO PLAN DE MEJORAS

EVALUACIÓN PLAN DE MEJORAS

3.	**Calidad de la comunicación**	**PENDIENTE**
¿En qué consiste?	*La información debe comunicarse a las instancias pertinentes, en forma y tiempo propicios, con un enfoque de efectividad y mejoramiento continuo, y utilizando canales y medio que garanticen razonablemente su oportunidad y seguridad.*	**Seleccionar una opción abajo**
Opciones	**Señale la opción que describa mejor la situación actual de su entidad, colocando una "X" en la celda correspondiente en la columna de la derecha:**	**Colocar una X**
A	Se han definido algunos canales de comunicación para enviar la información requerida por las instancias internas únicamente.	
B	Se cuenta con canales de comunicación formalmente establecidos para la atención de los requerimientos de información tanto internos como externos.	
C	La información se comunica oportunamente a las instancias pertinentes. Al respecto, se cuenta con regulaciones precisas sobre la comunicación de información confidencial.	
D	Se han instaurado procesos para el seguimiento constante de la efectividad de la comunicación de la información, y oportunamente se toman las acciones para incorporar las mejoras necesarias.	
E	La comunicación de la información se realiza a las instancias competentes, de manera ágil, oportuna y correcta, y permite a la instancia desarrollar métodos novedosos de gestión, organización y rendición de cuentas.	
SELECCIONAR UNA OPCION		**PENDIENTE**

Usted como responsable del SCI indique que acción o acciones está dispuesto a emprender en cuanto a la Calidad de la Comunicación, según lo que establece el Componente Sistemas de Información, para mejorar la condición de su Sistema de Control Interno.

FORMULACIÓN PLAN DE MEJORAS

PENDIENTE

SEGUIMIENTO PLAN DE MEJORAS

EVALUACIÓN PLAN DE MEJORAS

4.	Control de los sistemas de información	PENDIENTE
¿En qué consiste?	*Deben establecerse, aplicarse y perfeccionarse los controles pertinentes para que los sistemas de información garanticen razonablemente la calidad de la información y de la comunicación, la seguridad y una clara asignación de responsabilidades y administración de los niveles de acceso a la información y datos sensibles, así como la garantía de confidencialidad de la información que ostente ese carácter.*	**Seleccionar una opción abajo**
Opciones	**Señale la opción que describa mejor la situación actual de su entidad, colocando una "X" en la celda correspondiente en la columna de la derecha:**	**Colocar una X**
A	Se cuenta con algunos controles en el proceso de generación de la información, definidos mediante esfuerzos aislados por parte de algunos titulares subordinados.	
B	Los titulares subordinados han definido y divulgado controles para asegurar la calidad de la información y su comunicación. Entre dichos controles se cuentan la definición de accesos a los sistemas de información que utilizan recursos tecnológicos, y la asignación de responsabilidades sobre la custodia de los acopios físicos de información, las cuales estas han sido asumidas por los funcionarios correspondientes.	
C	Los sistemas de información conllevan la definición de controles desde su diseño hasta su operación. Ello garantiza que posean los mecanismos de control apropiados para la generación de información confiable, oportuna y útil.	
D	Los controles establecidos en los sistemas de información se monitorean de manera permanente; y se adoptan oportunamente las mejoras necesarias, así como las medidas necesarias para garantizar la calidad, la disponibilidad y la comunicación de la información con la oportunidad requerida.	
E	Los sistemas de información cuentan con los controles necesarios para disminuir los riesgos de pérdida de información y de fallas en la recopilación, el procesamiento, el mantenimiento y la comunicación de información son mínimos. Además, la instancia cuenta con mecanismos que propician la respuesta y anticipación oportunas, a las condiciones cambiantes del entorno que afectan dichos sistemas.	
SELECCIONAR UNA OPCION		**PENDIENTE**

Usted como responsable del SCI indique que acción o acciones está dispuesto a emprender en cuanto al Control, según lo que establece el Componente Sistemas de Información, para mejorar la condición de su Sistema de Control Interno.

FORMULACIÓN PLAN DE MEJORAS

PENDIENTE

SEGUIMIENTO PLAN DE MEJORAS

EVALUACIÓN PLAN DE MEJORAS

8.9 ENCUESTA DE SEGUIMIENTOS

AUTOEVALUACIÓN CONTROL INTERNO

Instancia:

COMPONENTE SEGUIMIENTO

El seguimiento comprende las actividades que se realizan para valorar la calidad del funcionamiento del sistema de control interno, a lo largo del tiempo; asimismo, para asegurar que los hallazgos de la auditoría y los resultados de otras revisiones se atiendan con prontitud. El modelo de madurez incluye los siguientes cuatro atributos en relación con el seguimiento: 1 - Participantes / 2 - Formalidad / 3 - Alcance / 4 - Contribución a la mejora del sistema de control interno

1.	**Participantes en el seguimiento del sistema de control interno**	**PENDIENTE**
¿En qué consiste?	*El liderazgo por el seguimiento del sistema de control interno debe ser asumido por el jefe y compartido con todos los titulares subordinados. Por su parte, los funcionarios tienen una participación activa en las labores de seguimiento continuo y periódico.*	**Seleccionar una opción abajo**
Opciones	**Señale la opción que describa mejor la situación actual de su entidad, colocando una "X" en la celda correspondiente en la columna de la derecha:**	**Colocar una X**
A	El seguimiento del sistema de control interno es responsabilidad de una o varias unidades particulares.	
B	El seguimiento periódico del sistema de control interno es ordenado por el jefe a los demás titulares subordinados bajo su cargo, quienes a su vez solicitan a algunos funcionarios que participen en el seguimiento del control interno atinente a las actividades relacionadas con sus puestos. Esto ha generado un reforzamiento del criterio de que el seguimiento requiere la participación de todos los funcionarios.	
C	El seguimiento del sistema de control interno es asumido por el jefe, demás titulares subordinados y todos los demás funcionarios, cada quien en el ámbito de sus competencias.	
D	El seguimiento del sistema de control interno forma parte de las actividades diarias del jefe, demás titulares subordinados y los funcionarios en general, y se promueven revisiones independientes por parte de otras instancias.	
E	Los titulares subordinados han asumido un liderazgo compartido respecto del seguimiento del sistema de control interno; y han instaurado lo mecanismos necesarios para la innovación y MEJORAS continua del sistema.	
SELECCIONAR UNA OPCION		**PENDIENTE**
Usted como responsable del SCI indique que acción o acciones está dispuesto a emprender en cuanto a la Participación, según lo que establece el Componente Seguimiento, para mejorar la condición de su Sistema de Control Interno.		

FORMULACIÓN PLAN DE MEJORAS

PENDIENTE

SEGUIMIENTO PLAN DE MEJORAS

EVALUACIÓN PLAN DE MEJORAS

2.	**Formalidad del seguimiento del sistema de control interno**	**PENDIENTE**
¿En qué consiste?	*El seguimiento del sistema de control interno debe observar un proceso estructurado debidamente oficializado mediante las disposiciones administrativas pertinentes, en relación con el alcance, la periodicidad, las responsabilidades, los mecanismos y las herramientas correspondientes.*	**Seleccionar una opción abajo**
Opciones	**Señale la opción que describa mejor la situación actual de su entidad, colocando una "X" en la celda correspondiente en la columna de la derecha:**	**Colocar una X**
A	Para algunas unidades específicas de la instancia, existen disposiciones sobre el seguimiento que deben ejercer sobre el control interno aplicable a algunas de las actividades que realizan.	
B	El jefe ha emitido disposiciones de tipo general sobre la obligación de los titulares subordinados de dar seguimiento al sistema de control interno, con la colaboración de los funcionarios que corresponda.	
C	Los titulares subordinados han instaurado regulaciones formales sobre el seguimiento del sistema de control interno, requiriendo que éste se realice vigilando la eficacia de las actividades de control en las operaciones diarias y que se lleve a cabo una autoevaluación anual del sistema de control interno y se elabore un plan de mejoras.	
D	Las regulaciones cubren todos los aspectos relacionados con el seguimiento continuo y periódico interno y externo, así como con la implementación y la verificación de las mejoras que se determinen, sean éstas de carácter operativo o estratégico.	
E	El seguimiento del sistema de control interno es un proceso estructurado que incorpora revisiones de diversos tipos y herramientas flexibles. Los esfuerzos realizados en torno a este componente del control interno han contribuido a que se convierta en parte de la cultura institucional.	
SELECCIONAR UNA OPCION		**PENDIENTE**

Usted como responsable del SCI indique que acción o acciones está dispuesto a emprender en cuanto a la Formalidad, según lo que establece el Componente Seguimiento, para mejorar la condición de su Sistema de Control Interno.

FORMULACIÓN PLAN DE MEJORAS

PENDIENTE

SEGUIMIENTO PLAN DE MEJORAS

EVALUACIÓN PLAN DE MEJORAS

3.	Alcance del seguimiento del sistema de control interno	PENDIENTE
¿En qué consiste?	*El seguimiento del sistema de control interno debe abarcar el funcionamiento, la suficiencia y la validez del sistema, su contribución al desempeño institucional y al logro de los objetivos, y el grado en que los componentes funcionares se han establecido e integrado en el accionar institucional. Asimismo, debe comprender actividades permanentes y periódicas, y la implantación de las mejoras que se determinen.*	Seleccionar una opción abajo
Opciones	**Señale la opción que describa mejor la situación actual de su entidad, colocando una "X" en la celda correspondiente en la columna de la derecha:**	Colocar una X
A	Existen labores aisladas de seguimiento del sistema de control interno con un alcance limitado a algunos controles específicos, las cuales se ponen de manifiesto mediante la vigilancia que, de manera rutinaria, ejercen los titulares sobre el cumplimiento de algunas actividades.	
B	Los titulares subordinados vigilan las actividades bajo su control con una visión de corto plazo y en procura del cumplimiento de las obligaciones legales que establece el ordenamiento.	
C	El seguimiento del sistema de control interno y sus mecanismos se han integrado a las actividades organizacionales, y en lo procedente se han incorporado en la documentación de los puestos y procesos. En ese sentido, los funcionarios aplican las actividades de seguimiento que les corresponden, y en esos esfuerzos son supervisados por los titulares subordinados, quienes a su vez realizan un seguimiento general sobre las unidades a su cargo, con la orientación del jefe.	
D	El seguimiento del sistema de control interno se ha convertido en un proceso formal para una valoración y mejora permanente del sistema de control interno en el que todos los participantes asumen sus responsabilidades.	
E	El seguimiento del sistema de control interno se realiza con un enfoque estratégico, y cubre el control de las actividades cotidianas, revisiones puntuales y el monitoreo de las mejoras acordadas	
SELECCIONAR UNA OPCION		PENDIENTE

Usted como responsable del SCI indique que acción o acciones está dispuesto a emprender en cuanto al Alcance, según lo que establece el Componente Seguimiento, para mejorar la condición de su Sistema de Control Interno.

FORMULACIÓN PLAN DE MEJORAS

PENDIENTE

SEGUIMIENTO PLAN DE MEJORAS

EVALUACIÓN PLAN DE MEJORAS

4.	Contribución del seguimiento a la mejora del sistema de control interno	PENDIENTE
¿En qué consiste?	*Como resultado del seguimiento del sistema de control interno, deben determinarse las mejoras que procedan, las cuales se calendarizan en un plan de implementación que, a su vez, será objeto de verificación en términos de su aplicación conforme a lo planeado y de la efectividad de las medidas adoptadas para fortalecer dicho sistema.*	Seleccionar una opción abajo
Opciones	**Señale la opción que describa mejor la situación actual de su entidad, colocando una "X" en la celda correspondiente en la columna de la derecha:**	Colocar una X
A	La contribución del seguimiento a la mejora del sistema de control interno es mínima.	
B	El seguimiento y permite detectar algunas oportunidades de mejora del sistema de control interno.	
C	El seguimiento del sistema de control interno constituye una herramienta que permite la valoración y mejora de dicho sistema y de su contribución a la gestión.	
D	Mediante la ejecución cotidiana de labores de seguimiento en el desarrollo de las actividades organizacionales, constantemente se introducen mejoras sustanciales en el desempeño organizacional y en el sistema de control interno. Adicionalmente, se realizan valoraciones específicas del sistema de control interno, y se implementan las mejoras necesarias.	
E	El proceso de seguimiento se mejora constantemente, con lo que se incrementan sus aportes al valor, a la gestión y al sistema de control interno institucionales, así como la identificación de nuevos modos de gestión y de control.	
SELECCIONAR UNA OPCION		PENDIENTE

Usted como responsable del SCI indique que acción o acciones está dispuesto a emprender para el Fortalecimiento, según lo que establece el Componente Seguimiento, para mejorar la condición de su Sistema de Control Interno.

FORMULACIÓN PLAN DE MEJORAS

PENDIENTE

SEGUIMIENTO PLAN DE MEJORAS

EVALUACIÓN PLAN DE MEJORAS
