DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS E INFORMÁTICA

TEMA: AUDITORÍA INFORMÁTICA DEL SISTEMA DE INFORMACIÓN DE LA EMPRESA COCINAS INTERNACIONALES UTILIZANDO COBIT V.5

AUTOR: JIMÉNEZ CUESTAS, ANA LUCÍA

DIRECTOR: ING. SOLÍS FERNANDO

SANGOLQUI

2016

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

CERTIFICACIÓN

Certifico que el trabajo de titulación ***"AUDITORÍA INFORMÁTICA DEL SISTEMA DE INFORMACIÓN DE LA EMPRESA COCINAS INTERNACIONALES UTILIZANDO COBIT V.5"*** realizado por la Señorita ***JIMENEZ CUESTAS ANA LUCÍA***, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnico, metodológicos y legales establecidos por la Universidad de las Fuerza Armadas ESPE, por lo tanto me permito acreditarlo y autorizar a la Señorita ***JIMÉNEZ CUESTAS ANA LUCIA*** para que lo sustente públicamente.

Sangolqui, 28 de Junio del 2016

ING. FERNANDO SOLIS

TUTOR

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORÍA DE RESPONSABILIDAD

Yo, ***JIMENEZ CUESTAS ANA LUCÍA***, con cédula de identidad N° ***1710928332***, declaro que este trabajo de titulación ***"AUDITORÍA INFORMÁTICA DEL SISTEMA DE INFORMACIÓN DE LA EMPRESA COCINAS INTERNACIONALES UTILIZANDO COBIT V.5"*** realizado por la Señorita ***JIMENEZ CUESTAS ANA LUCÍA***, ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 28 de Junio del 2016

JIMÉNEZ CUESTAS ANA LUCÍA

C.C: 1710928332

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORIZACIÓN

Yo, ***JIMENEZ CUESTAS ANA LUCÍA***, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación ***"AUDITORÍA INFORMÁTICA DEL SISTEMA DE INFORMACIÓN DE LA EMPRESA COCINAS INTERNACIONALES UTILIZANDO COBIT V5"*** cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Sangolquí, 28 de Junio del 2016

JIMÉNEZ CUESTAS ANA LUCÍA

C.C: 1710928332

DEDICATORIA

Dedico este trabajo principalmente a Dios, que fue el que orquestó todo a fin de que pudiera cumplir con esta etapa de mi vida, a Dios quien me dio las fuerzas para continuar adelante en los momentos difíciles, a Dios que como padre sus pensamientos fueron tan altos que hicieron que pudiera cumplir con este sueño y este anhelo.

Dedico este trabajo a mis padres en retribución a todos sus esfuerzos y apoyo incondicional, que me permitieron llegar a este momento tan valioso de mi vida, que me enseñaron el valor del sacrificio para construir un futuro lleno de esperanza, que como parte de su herencia me están dejado algo más preciado que bienes, una educación basada en principios y valores.

Dedico también este trabajo a mis hermanos: Diana, Vinicio y Antonela, por estar presentes en todo este proceso, por su preocupación y por su ayuda invaluable.

Anita

AGRADECIMIENTO

Aunque el camino para llegar a este momento ha sido largo, quiero agradecer primeramente a Dios, que ha permitido que cumpla con esta etapa de mi vida, reconociéndolo como el dador de vida, reconociendo su favor y su gracia, para alcanzar esta meta, por haberme regalado tan maravillosa promesa que la estoy viendo cumplirse en mi vida. “Deja en manos de Dios todo lo que haces, y tus proyectos se harán realidad.” Prov. 16:3 TLA

Quiero agradecer a mis padres: Jorge e Inés, por todo su amor, reflejado en su apoyo incondicional, en sus múltiples consejos, en su paciencia a través de mis errores y equivocaciones, han sido mi segundo pilar y me han sostenido y acompañado en este proceso, no puedo decirles más que gracias Papi y Mami, esto es solo un pedacito de retribución de lo mucho que me han dado.

Agradezco a mis hermanos: Diana, Vinicio y Antonela, por estar siempre, por escucharme, acompañarme y animarme, por su amor y toda su preocupación.

Quiero agradecer igualmente a la Universidad de las Fuerzas Armadas ESPE por la contribución de conocimiento, a través de sus docentes, que han sido un elemento fundamental para la formación de una profesional.

Quiero hacer un agradecimiento especial al Ing. Mario Ron, por su confianza para realizar este trabajo y por todas las orientaciones, guías y ayudas brindadas en el proceso.

Quiero agradecer al Ing. Jairo Ron, por darme la oportunidad de realizar este trabajo en la empresa Cocinas Internacionales y entregarme la confianza para culminar este proyecto.

No me queda más que agradecer a mi director de tesis, Ing. Fernando Solís, que me apoyó durante todo el proceso de inicio, desarrollo y culminación del trabajo, que me animó y confió en los criterios que como profesional he brindado en este proyecto.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El proyecto de Titulación realizado en el presente trabajo tiene como finalidad la ejecución de la auditoría informática al sistema de información de la empresa Cocinas Internacionales, basándose en las directrices del marco metodológico de COBIT V5 para el gobierno y gestión de las tecnologías de la información en apoyo al negocio. La auditoría, tuvo como alcance la evaluación de controles existentes de seguridad de la información, mediante la selección de los procesos utilizando la metodología de Auditoría Basada en Riesgos, lo que permitió la selección de los procesos más críticos que forman parte del negocio en los que las tecnologías de la información se encuentran directamente involucradas. Se estableció el programa de auditoría y se elaboró los instrumentos que permitieron la recepción de los datos con lo que se logró agrupar la evidencia para el respectivo análisis. La auditoría fue desarrollada con el uso de los productos de ISACA: COBIT 5 para la Seguridad de la Información y COBIT 5 para el Aseguramiento. En cada proceso se evaluó la existencia de las herramientas de apoyo, determinando el nivel de capacidad de cada proceso. Los resultados de la auditoría informática se presentaron en el informe preliminar, mostrando los hallazgos que se encontraron por proceso, con sus respectivos criterios, causas efectos y recomendaciones, siendo sujetos de revisión y aprobación para dar lugar al informe de auditoría final.

PALABRAS CLAVES

- **COBIT**
- **AUDITORÍA BASADA EN RIESGOS**
- **SISTEMAS DE SEGURIDAD DE LA INFORMACION.**
- **SEGURIDADES INFORMÁTICAS**
- **TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN**

ABSTRACT

The project Titling made in the present work aims at the execution of information technology audit to the information system of the company Cocinas Internacionales, based on the guidelines of the methodological framework of COBIT V5 for the government and management of information technology in business support. The audit had as scope, the evaluation of existing controls of information security by selecting process using the methodology of The Risk-based Audit, which allowed the selection of the most critical processes that are part of the business in which information technologies are directly involved. The audit program was established and the instruments was made, that allowed the reception of the data with which was achieved grouping the evidence for the respective analysis. The audit was developed with the use of products: COBIT 5 for Information Security and COBIT 5 for Assurance. In each process we assessed the existence of support tools for the process, determining the level of capability of each process. The results of information technology audit were presented in the preliminary report, showing the findings that were found by the process, with their respective criteria, causes, effects and recommendations being subject to review and approval to give the final audit report.

KEYWORDS

- **COBIT**
- **RISK BASED AUDIT**
- **SYSTEM FOR INFORMATION SECURITY**
- **INFORMATION SECURITY**
- **INFORMATION TECHNOLOGY AND COMMUNICATION**

CAPÍTULO 1

INTRODUCCIÓN

1.1. Antecedentes

Cocinas Internacionales es una empresa que orienta su negocio a la fabricación de muebles modulares, se enfoca en la fabricación de cocinas closets y baños. Para cumplir con las exigencias de un mercado altamente competitivo, se aseguran de disponer de la materia prima de mejor calidad como: tableros, aglomerados, mdf y madera. Como gran parte de las organizaciones, tanto pequeñas como grandes, Cocinas Internacionales integra la tecnología en sus procesos de negocio, es por ello que actualmente al igual que la materia prima, la información y la tecnología que explotan se vuelven un activo valioso para la empresa.

A través de la combinación de información y tecnología se logra potenciar no solamente los procesos administrativos de la organización, sino que además permite desarrollar el proceso productivo de la misma, interviniendo en el diseño sofisticado de modulares que satisfacen los gustos más exigentes de sus clientes. Actualmente la tecnología juega un papel importante en los procesos de negocio, debido a que llega a constituirse en un recurso clave, formando una parte integral en el ciclo de vida del negocio.

Dentro de los objetivos y estrategias de la empresa se establece la necesidad de reducir sus perfiles de riesgo a través de la adecuada administración de la seguridad. La información específica y las tecnologías relacionadas son cada vez más esenciales para las organizaciones, pero la seguridad de la información es básica, para la supervivencia y desarrollo institucional. La propuesta de auditoría informática permitirá conocer el estado actual en el que se encuentra la empresa desde la perspectiva de seguridad de la información en su sistema de información, basándose en un modelo, como una guía para la evaluación que permitan el aseguramiento

de Tecnologías de la Información (TI), usando como marco metodológico de referencia COBIT V5.

1.2. Planteamiento del Problema

Se reconoce a la administración y gestión de la información como un tema importante y complejo. Por ello la empresa Cocinas Internacionales al poseer una infraestructura tecnológica que contribuye al proceso administrativo y productivo del negocio tiene la necesidad de iniciar un proceso de auditoría informática que le permita plantear una definición de la situación actual de la empresa con relación a las TI.

Las TI que actualmente participan en los procesos de negocio han sido primordiales para el desarrollo y cumplimiento de los objetivos de la empresa, sin embargo es necesario verificar que este recurso sea utilizado eficaz y eficientemente. Reduciendo el riesgo a través de una adecuada administración en cuanto a la seguridad de la información.

El no poseer un panorama claro de la condición actual de sus TI, impide activar controles que contribuyan en la disminución de riesgos por problemas de seguridad informática. Conocer la condición actual de la empresa permitirá tomar las acciones preventivas y correctivas que contribuirán con el establecimiento de controles garantizando la protección responsable de la información del negocio.

1.3. Justificación

El presente proyecto surge como una necesidad de la empresa Cocinas Internacionales por evaluar el estado actual del área tecnológica que salvaguarda un activo importante dentro de su modelo de negocio como lo es la información. La información es un activo invaluable, razón por la cual es responsabilidad de cada organización protegerla, gestionarla y usarla principalmente para generar valor en sus procesos de negocio.

Además, es responsabilidad de la empresa garantizar el correcto control y administración de la misma, por ello los procesos tecnológicos y su información deben ser evaluados permitiendo como resultado garantizar que existen lo procesos necesarios que contribuyan con la seguridad de esta información. El marco en referencia a utilizar para esta auditoría informática COBIT V.5, ha sido escogido debido a que es un marco de trabajo integral que permite crear un valor óptimo a las TI de las organizaciones, buscando satisfacer las necesidades de la organización. Además puede ser personalizado de manera que se adapte a las metas del negocio.

1.4. Objetivos

1.4.1. Objetivo General

Evaluar la condición actual del Sistema de Información de la empresa Cocinas Internacionales, utilizando Cobit V.5, para conocer las debilidades y riesgos a los que se encuentra expuesta su información.

1.4.2. Objetivos Específicos

- Realizar la selección de procesos prioritarios a ser evaluados, mediante el método de cascada de COBIT V.5.
- Elaborar el Plan de Investigación de Campo llegando al conocimiento y comprensión de la empresa.
- Elaborar y aplicar los instrumentos de Investigación de Campo.
- Realizar el análisis de la información a través de los resultados obtenidos en los instrumentos de Investigación.
- Elaborar y dar lectura al informe borrador de la Auditoría al personal interno de la institución.
- Entregar informe final que contendrá la inclusión de puntos de vista y justificaciones.

1.5. Alcance

El proyecto de tesis incluirá la revisión de los controles del Sistema de Información de la empresa Cocinas Internacionales, utilizando una metodología en base a riesgos ABR y su aplicación con el estándar internacional COBIT V.5, la auditoría se enfocará principalmente en la evaluación de seguridades en determinados módulos del sistema con el producto COBIT V.5 for Assurance. El proyecto de tesis será ejecutado en las instalaciones, principal y sucursales de la empresa en Quito y Cumbayá.

CAPÍTULO 2

MARCO TEÓRICO

2.1. Introducción

2.1.1. Conceptos de Auditoría y Auditoría Informática

> La auditoría en sí es una actividad que consiste en emitir un juicio y opinión profesional sobre el objetivo o la materia analizada indicando si se están cumpliendo los requisitos que procedan en cada temática. Esta opinión deberá fundamentarse en una serie de procedimientos que justifiquen y sirvan de soporte al análisis realizado. (Tejada, 2015)

Auditoría es una actividad necesaria que debe ser utilizada por las entidades cuyo objetivo estratégico es el aseguramiento de todos sus activos de manera apropiada. Es la alta dirección la que espera que tras una auditoría surjan recomendaciones que permitan a la entidad entrar en procesos que contribuyan a la mejora continua de las funciones de la organización.

Dicho esto, cabe mencionar que la Auditoría Informática (AI), es un proceso necesario, que debe ser llevado a cabo por personal técnico que se encuentre debidamente preparado y capacitado para recoger, agrupar y evaluar las evidencias a fin de determinar que los recursos tecnológicos sean gestionados en un ambiente de seguridad y control eficientes.

La AI, como tal, consiste en el estudio directo a los mecanismos de control implementados, determinando si los mismos son adecuados y cumplen con objetivos y estrategias, tanto en la gerencia de Tecnologías de la Información y Comunicación (TIC’s) como en la gerencia general. Un rol fundamental es el aportar con observaciones y recomendaciones que permitan el mejoramiento continuo de los sistemas de información en la institución.

2.1.2. Objetivos de la Auditoría Informática

La AI es un instrumento de evaluación que permite analizar resultados para conseguir los siguientes propósitos:

- Mayor satisfacción por parte de usuarios con acceso a los sistemas informáticos
- Aseguramiento de integridad, confidencialidad y confiabilidad de la información
- Conocimiento de situación actual, actividades y esfuerzos alineados a los objetivos del negocio de la institución
- Seguridad de personal, datos, hardware, software e instalaciones
- Disponibilidad de información oportuna en el ambiente informático
- Evaluación de controles implementados

2.1.3. Clasificación de la Auditoría

2.1.3.1. Auditoría Interna

> La base de las empresas para la planificación, ejecución y control de actividades que contribuyen al cumplimiento de metas y objetivos es la estructura organizativa. Una auditoría interna tiene como función examinar y construir una estructura organizativa que permita la correcta gestión de sus recursos materiales como humanos al igual que sus métodos de operación. (Proyectos fin de carrera).

Esta auditoría apunta a objetivos que permiten la detección de deficiencias o irregularidades y sobre la marcha, adecuar controles y acciones para asegurar la eficiencia y eficacia en el cumplimiento de metas y objetivos. Su evaluación abarca varios escenarios entre los que se encuentran involucrados el marco económico, la efectividad en la estructura organizacional, la observancia de políticas y procedimientos y la eficacia de controles a fin de que el personal, equipo y sistemas tengan un desempeño satisfactorio.

“Es fundamental considerar como una unidad parte de la entidad a la auditoría informática, esta unidad debe encontrarse dentro de la empresa llegando a ser lo suficientemente independiente para llevar a cabo sus objetivos, antes mencionadas.” (Actualidad Técnologica)

2.1.3.2. Auditoría Externa

La auditoría externa es proporcionada por una firma reconocida, misma que debe estar en capacidad de emitir opiniones imparciales y profesionalmente expertas acerca de los hallazgos encontrados en el examen, el auditor debe entregar sus opiniones y observaciones mediante la elaboración de informes que recopilen la información de sustento. A este tipo de auditoría no se le debe imponer restricciones para que pueda ser ejecutada en completa transparencia.

> La auditoría externa o también conocida como independiente tiene por objeto averiguar la razonabilidad, integridad y autenticidad de los estados, expedientes, documentos y toda aquella información producida por los sistemas de la organización. Una auditoría externa que se lleva acabo tiene la intención de publicar el producto del sistema de información examinado con el fin de acompañar al mismo de una opinión independiente que le de autenticidad y permita a los usuarios de dicha información tomar decisiones confiando en las declaraciones del auditor. (Auditoria Informatica)

2.1.4. Generalidades de la Auditoría Informática

La auditoría informática no es diferente de una auditoría financiera en sus objetivos, ambas buscan salvaguardar el recurso empresarial valioso. La auditoría informática se enfoca en procesos que permiten recoger, agrupar y evaluar las evidencias que permitan determinar si los sistemas de información de la organización, mantienen la integridad de datos y si estos llevan a cabo eficazmente los fines de la organización y la utilización eficiente de sus recursos.

La auditoría informática, consiste en el estudio que permite evaluar de una manera objetiva aquellos mecanismos de control utilizados en una

empresa u organización. Permitiendo sugerir cambios y adaptaciones a los mecanismos existentes para que se alineen a los objetivos y estrategias de la organización. Los beneficios que le ofrece la auditoría informática a las empresas u organizaciones, es que al finalizar estos procesos de estudio, análisis y recomendaciones, las mismas mejoran en eficiencia, eficacia, rentabilidad y seguridad de la información.

La información de la empresa debe contener algunos atributos los cuales son analizados por la auditoría informática (ver figura 1), estos atributos de la información deber ser: completos, es decir, no debería existir ocultamiento de la información, esto provocaría tomas de decisiones pobres que afectarían los objetivos de la empresa. La información debe ser exacta, los procesos, toman datos de entrada los cuales son transformados en información para la empresa. Esta información, debe ser el resultado del procesamiento de información correcto, ya que una información errada también afecta la toma de decisiones que involucran el curso del negocio.

Generar valor, en términos económicos debe generar valor a la empresa u organización, y al mismo tiempo equilibrar su coste de procesamiento. El coste de procesamiento de la información no debe exceder al coste de utilización del mismo. La información debe ser adecuada y estar disponible para quienes lo necesiten, asegurando una gestión eficiente de la misma. Oportuna y puntal, la información pierde valor si no es presentada oportunamente, afectando el negocio.

También es responsabilidad de la organización proteger la difusión responsable de información a personas no autorizadas. Garantizar la protección de datos contra destrucciones accidentales o voluntarias. Cuando los controles aplicados a la seguridad de la información no son efectivos pueden provocar pérdidas económicas a la organización.

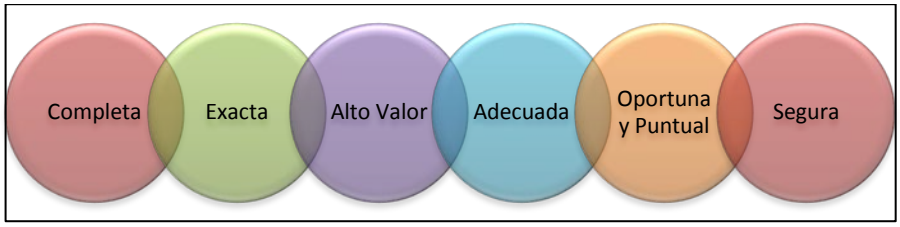


Figura 1: Características de la Información

Las características antes mencionadas hacen que la información sea un recurso de gran valor en la empresa, pero si no existen controles eficaces y adecuados en el manejo de la información este recurso también llega a ser crítico. La información se vuelve crítica por las siguientes razones listadas a continuación:

- Sectores financieros, productivos y de servicios.
- Pérdidas de Información en las Bases de Datos
- Instalaciones Físicas
- Control de Acceso a los Sistemas de Información

La auditoría permite cubrir temas como el aseguramiento, dicho de otra manera garantizar que la información que le llega a la dirección y a las diferentes áreas de la empresa sea la necesaria, exacta y oportuna, para una adecuada toma de decisiones. También permite reducir al máximo la pérdida de información. Por fallas de equipos, por fallas en los procesos o por la gestión errónea de archivos. Permite detectar manipulación de la información por acceso no autorizado de personal a transacciones que involucran responsabilidad

La auditoría informática recoge evidencias de riesgos y/o problemas que surgen del apoyo informático a los procesos de negocio, los cuales provienen generalmente del mal uso del recurso informático y la falta de eficiencia en los mecanismos de control aplicados. Además sugiere mejoras en los procesos actualmente manejados en la organización que permitan garantizar un mejor control sobre estos recursos.

Una auditoría informática externa consiste en la revisión de las TIC que permitan exponer si en el proceso se detectan violaciones, irregularidades, fraudes o errores en un momento dado entregando sus resultados y hallazgos en un periodo de tiempo determinado.

> Al realizar una auditoría el objetivo y el ámbito deben estar claros, en cada caso se realizará una revisión de control interno, su cumplimiento, sus costes, la eficacia y eficiencia de la gestión, todo ello nos aportará datos para poder comparar unos procesos con otros, unos departamentos con otros, e incluso personas, tanto en el tiempo, como en base a objetivos definidos. Una auditoría sea interna o externa genera un informe con una serie de recomendaciones en base a objetivos, ámbito y profundidad definiendo:
>
> - Planes y objetivos
> - Revisión de controles y planes de riesgo
> - Cumplimiento de procedimientos internos y base de la normativa externa
> - Administración de la seguridad
> - Proceso en entorno seguro
> - Desarrollo en entorno seguro
> - Continuidad
>
> Llegados a este punto, es donde la empresa debe decidir cómo abordar las recomendaciones definidas por el auditor para el bienestar de su empresa. (Ramírez, 2009)

Para llevar a cabo un proceso de auditoría se han desarrollado a través del tiempo diferentes mecanismos y herramientas que contribuyen con el ejercicio de la auditoría informática, promoviendo la creación y desarrollo de las mejores prácticas reconocidas a nivel mundial como: COBIT, ISO, COSO e ITIL. La auditoría informática estará dividida en tres etapas, las cuales se definirá más adelante: planificación, ejecución y finalización.

2.1.5. Alcance de la Auditoría Informática

> El alcance de la auditoría ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoría informática y se completa con los objetivos de esta. El alcance ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado, no solamente hasta que puntos ha llegado, sino cuales materias fronterizas han sido omitidas. (Moreno, 2012)

Es una función propia de la definición del alcance, el delimitar las áreas, funciones, procesos y las organizaciones que serán sometidos a la auditoría. Debe existir una comunicación clara entre el auditor y el cliente, donde queden formalmente establecidos con exactitud los límites de estudio.

El auditor debe conocer los objetivos hacia donde se orientan sus tareas, a fin de dar cumplimento a los requerimientos y pretensiones del cliente. Los límites a los que se llegue por mutuo acuerdo deberán ser incorporados al inicio del Informe Final de la Auditoría.

2.1.6. Importancia de la Auditoría Informática

Según Kuna, “La auditoría de sistemas es fundamental para garantizar el correcto funcionamiento de los Sistemas de Información al proporcionar los controles necesarios que permiten garantizar la seguridad, integridad, disponibilidad y confiabilidad de los mismos”. (Kuna, 2014)

Un proceso de auditoría informática permite reconocer debilidades y amenazas a los procesos de negocio de una empresa que se encuentra vinculados a las TIC, permite además evaluar, si las políticas adoptadas en la institución están siendo acatadas y cumplidas, determinando a la vez un examen detallado a los mecanismos de control adoptados, valorando si los mismos son idóneos o no para el escenario en el cual son aplicados

Analiza las posibles deficiencias o debilidades permitiendo a la dirección de la empresa tomar las medidas respectivas que disminuyan los impactos que provocan las amenazas. Es un estudio que presenta una visión amplia de la condición actual de las TIC, agregando sugerencias de mejora para garantizar la continuidad del negocio.

> Las TIC deben ser sometidas siempre a controles de calidad ya que en la actualidad son consideradas un blanco para la supervivencia de la organización. No se puede perder de vista la naturaleza y la calidad de datos de entrada porque esto puede provocar una generación de información errónea, estos y muchos casos más se exponen alrededor

del área informática del cual evidentemente las organizaciones cada día son más dependientes. (Fernández, 2008)

"Es de vital importancia que todo lo que se encuentre vinculado a las TIC funcionen de manera correcta e ininterrumpidamente para no afectar la productividad y supervivencia de una organización", según lo menciona Nubia Fernández. (Fernández, 2008)

2.1.7. Metodología de Desarrollo de la Auditoría Informática

Una metodología de auditoría define los procesos que se llevaran a cabo para el cumplimiento de la misma. Presentamos esta metodología en tres fases en la figura 2, dentro de las cuales se describirá las principales actividades que acogerán los procesos de la misma.

Figura 2: Metodología de Desarrollo de Auditoría

2.1.7.1. Planificación, Fase A o Fase 1

La primera fase contempla el establecimiento de relaciones entre auditor y entidad. Esta fase permitirá obtener una definición clara y precisa acerca del alcance y objetivos que busca como resultado la auditoría

informática. En esta fase se determinará los siguientes aspectos que permiten el conocimiento del estado actual de la entidad a ser auditada:

- Conocimiento y comprensión de la empresa
- Objetivos y Alcance de la Auditoría
- Análisis Preliminar

Conocimiento y Comprensión de la Empresa

Una de las actividades fundamentales previa a la realización de auditorías involucra el conocimiento y la comprensión de la empresa. Lo cual permitirá elaborar los planes específicos de manera objetiva para la auditoría. Este conocimiento y compresión implica la definición de: la naturaleza operativa, estructura organizacional, giro de negocio y sistemas que se contempla en el proceso de negocio.

Para llevar a cabo esta actividad se debe tomar en cuenta el uso de diferentes mecanismos y/o herramientas. El auditor debe conocer cuál y cómo aplicarlas según el programa de auditoría que se llevará a cabo a las diferentes áreas. Entre las herramientas que el auditor podrá utilizar se detallan a continuación las siguientes:

- Visitas al lugar
- Entrevistas y encuestas
- Análisis FODA (Fortalezas, oportunidades, debilidades, amenazas)
- Análisis Causa-Efecto o Espina de Pescado
- Árbol de Objetivos.- Desdoblamiento de Complejidad.
- Árbol de Problemas

Objetivos y Alcance de la Auditoría

Se realiza la definición con mayor precisión del entorno y los límites en los cuales ha de desarrollarse la auditoría, anticipando que el área de aplicación de la misma cumpla con los objetivos que tiene establecida la situación de auditoría que se lleva a cabo.

Análisis Preliminar

Esta actividad será fundamental, dado que permitirá obtener la información necesaria, que le permita tomar al auditor las decisiones de cómo proceder en la auditoría, siendo una base fundamental y sustentable de los pasos que se encuentran a continuación.

2.1.7.2. Desarrollo, Fase B o Fase 2

El desarrollo involucra la recopilación de la información, que mucho dependerá de las herramientas con las que se haya decido obtener esta base de información. Puede ser presentada como documentos o evidencias que brindarán al auditor la capacidad de fundamentar comentarios, sugerencias y recomendaciones con respecto a la gestión de las TI. En esta fase se llevará a cabo las siguientes actividades:

- Análisis de los Riesgos
- Planificación Específica de la Auditoría
- Elaboración de Programas de Auditoría
- Elaboración y Aplicación de Instrumentos para la Recopilación de Información

Análisis de los Riesgos

El auditor debe estar en la capacidad de realizar un análisis de los riesgos que con lleva la auditoría, estos pueden generarse el momento de la ejecución del trabajo y al momento de emitir informes. Por esta razón se debe desarrollar mecanismos que permitan la reducción máxima de estos riesgos a la hora de emitir los informes de auditoría

Planificación Específica de la Auditoría

Para cada auditoría se debe elaborar un plan, que debe ser tanto de orden técnico como administrativo. Cabe mencionar que dentro de los planes administrativos se debe contemplar todo lo referente a cálculos

monetarios a cobrar, personal que conformarán los equipos de auditoría, horas hombre, etc.

Elaboración de Programas de Auditoría

El auditor o grupo de auditores debe tener claro el programa detallado de los objetivos y procedimientos de auditoría objeto de su examen. El programa de auditoría debe contener dos aspectos fundamentales: Objetivos de la auditoría y procedimientos que se aplicarán durante el examen de auditoría. Estos programas deben ser documentados, exponiendo la naturaleza, el procedimiento y el alcance del plan, mismos que retroalimentarán el plan de auditoría general. Un programa de auditoría contribuye al desarrollo general del trabajo, pero su función es más específica y analítica.

Elaboración y Aplicación de Instrumentos para la Recopilación de Información.

Entre las técnicas más utilizadas para los procesos de recopilación de información en temas de auditorías, existen varios instrumentos como los que se detalla a continuación que contribuirán en el proceso de búsqueda de evidencias en la auditoría:

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

La información obtenida de estas técnicas debe atravesar un proceso de análisis que debe ser ejecutado por auditores o el equipo a cargo del proceso de auditoría, manejando un criterio profesional. Toda la información obtenida debe ser tipificada al grado de que se permita su fácil localización. La información obtenida se considera como evidencia la cual se clasifica de

la siguiente manera: evidencia física, evidencia analítica y evidencia testimonial. Posteriormente la evidencia permitirá la justificación de manera correcta las recomendaciones.

En este proceso, la información es evaluada y se comprueba la manera en la que han sido diseñados los controles en la organización para su mejoramiento continuo. Para dar un resultado definitivo, el auditor o grupo encargado, debe asegurar de que el funcionamiento sea correcto y fiable en los sistemas de aplicaciones y recursos informáticos involucrados en el proceso.

2.1.7.3. Finalización, Fase C o Fase 3

Los resultados de la auditoría realizada deben ser entregados en forma de informe, el cual debe contener la inclusión de conclusiones y recomendaciones que le permitan al ente auditado obtener una herramienta de información que permita el trabajo garantizado en el mejoramiento continuo en todos los procesos seleccionados en el que se encuentran implícitas las tecnologías de la información .

Por las características de la empresa en la que se aplica la presente auditoría, el informe será dirigido a la dirección de la empresa y los involucrados de la evaluación, donde se justificará los resultados obtenidos con las partes interesadas: personal administrativo encargado y equipo de auditoría ejecutor. El auditor es responsable de defender los puntos de vista que se exponen en el informe, tomando como evidencia los resultados obtenidos. Es preciso indicar que el informe debe incluir al menos la siguiente información como conocimiento base:

- Etapa de tiempo en el que se ha realizado la evaluación.
- Indicar los objetivos que se trataron alcanzar con el proceso de auditoría.
- Se indicará en base a que herramienta se realizó la auditoría, para este caso, debe incluirse la justificación para la utilización de Cobit

V5 y Cobit V5 para la Seguridad de la Información, especificando los dominios que fueron sujetos de evaluación, además estos deben estar especificados claramente en el plan de trabajo que también debe ser entregado a la gerencia de la empresa.

- Se debe indicar el criterio sobre el cual se está evaluando, para este caso de estudio se realiza la evaluación centrada en los aspectos de Seguridad de la información, que contempla en sus productos Cobit V5.
- Entrega del detalle de la condición inicial en la que se encontró la empresa u organización
- Descripción de causas de porque la organización se encontraba en ese estado, además se deberá entregar un detalle de las consecuencias que puede traer si la empresa continua manejándose de la misma forma.
- Detalle explícito de las recomendaciones que se hacen a la administración y que deberían adoptar para poder cumplir con los objetivos propuestos desde el inicio a fin de que la organización deje de ser afectada por circunstancias que fueron encontradas en la situación inicial.
- Dentro de los informes también incluye las opiniones y puntos de vista de la administración, debe especificarse si la organización va a adoptar o no las recomendaciones propuestas por el grupo de auditores.

2.1.8. Técnicas y Herramientas de Auditoría

Para llevar a cabo una auditoría se debe recurrir a métodos, técnicas y herramientas. El auditor debe conocer cada herramienta que existe al detalle para saber los beneficios de información con la que tendrá aportación para enriquecer sus hallazgos. Las herramientas conocidas para la recopilación de información en procesos son las siguientes:

- Entrevista

- Encuesta
- Cuestionario
- Pruebas de Observación y Sustantivas

2.2. Auditoría en Base a Riesgos

La Auditoría en Base de Riesgos (ABR) es considerada actualmente como una rama de la auditoría informática, su razón de ser, está enfocada en localizar las vulnerabilidades y amenazas de una organización o área específica de aplicación. La ABR permite que el auditor o auditores, se concentren en aquellos procesos críticos, que llegan a representar un mayor impacto para la organización.

El riesgo es generado mediante la combinación entre vulnerabilidad y amenaza. “Es preciso indicar que no existe riesgo, si alguno de estos dos factores no se encuentra presente.” (Calderón & Ocaña, 2014) Generalmente se ha considerado que las vulnerabilidades se encuentran dentro de la organización y que las amenazas son detectadas al exterior de la misma. Actualmente las cifras estadísticas han cambiando este hecho, por lo que en los últimos años se detecta un mayor trecho de fragilidad en estas afirmaciones, donde se determina que las amenazas también constituyen una gran parte del resultado poco eficiente en los mecanismos de control y políticas aplicadas, que se encuentran involucradas a la parte interna de la organización.

Una adecuada y eficiente ABR, permite tomar las medidas necesarias a la organización, construyendo y evaluando estrategias que permitan precautelar sus recursos más valiosos, como es en este caso y de manera globalizada, la protección de la información y su ciclo de vida. Permite además establecer un enfoque específico en las áreas de mayor riesgo, con lo que se logra establecer una planificación organizada para aplicar la metodología que brinde los beneficios esperados.

2.2.1. Análisis del Riesgo

> Los riesgos de negocio son aquellas amenazas que pueden impactar los activos, procesos u objetivos de una organización, la naturaleza de estas amenazas puede ser financiera, reglamentaria u operacional. Una clase particular de riesgos asociados con la información y los SI que la soportan es la que está definida por el potencial de pérdida de la confidencialidad, disponibilidad o integridad de la información. (Naveda, 2012)

Para llevar a cabo este proceso es indispensable tener claro cuáles son los objetivos del negocio y como intervienen las TIC en el cumplimiento de los mismos. Se entiende a las TIC como los activos de información, los sistemas y todo recurso tecnológico que contribuyen en la generación, almacenamiento, uso y manipulación de la información, esto permite la identificación de los procesos más críticos para el cumplimiento de los objetivos institucionales. Una vez definidos los procesos críticos, el siguiente paso es evaluar el grado de impacto o afectación a los objetivos del negocio analizando el momento en el que las amenazas se materialicen a causa de las vulnerabilidades detectadas en la entidad las cuales no han sido controladas.

2.2.2. Técnicas de Evaluación del Riesgo

Las técnicas para evaluación de riesgo proveen una visión más centralizada de las áreas que serán auditadas por su nivel de criticidad. Además proveen una base para una gestión adecuada de la función de auditoría. Las técnicas de evaluación de riesgos, permiten asegurar que han sido seleccionadas las áreas de mayor relevancia para el cumplimiento de los objetivos del negocio. Existen varios métodos, entre ellos un sistema de puntación que considera las siguientes variables: “dificultad técnica, nivel de los procedimientos de control establecidos y nivel de pérdidas financieras”. (Naveda, 2012)

Cobit 5 integra en su marco metodológico la evaluación en base a riesgos para determinar los procesos más críticos del negocio relacionados

directamente con las tecnologías de la información, para lo cual es necesario trabajar con la cascada de metas a fin de determinar los objetivos del Negocio y de TI de la empresa, estos deben ser alineados a las metas genéricas propuestas en COBIT 5 para el negocio y las tecnologías de la información, que reúnen la experiencia y el conocimiento de varios especialista de las TI y la gestión empresarial.

Esto permite crear matrices personalizadas que se ajustan a las necesidades de la empresa a la cual se aplica el programa de auditoría y permite la definición de una manera mucho más objetiva seleccionar los procesos de mayor riesgo que afectan directamente las actividades del negocio. Una vez obtenido este análisis se debe exponer a los auditados para su posterior revisión y aprobación en conformidad con los procesos identificados para la aplicación del trabajo de auditoría.

2.3. Cobit V5

2.3.1. Introducción

Es importante indicar que todas las empresas, actualmente manejan y gestionan datos e información. Este recurso es cada día más valioso y una adecuada gestión debe estar en capacidad de velar por un correcto ciclo de vida de la información, que debe involucrar su creación, uso, conservación, exposición y destrucción.

La tecnología viene desempeñando un papel importante en estas acciones. Se debe considerar que la tecnología se encuentra inmersa en todos los aspectos del negocio y de la vida de las personas. Toda empresa necesita ser capaz de confiar en información de calidad para apoyar los procesos de toma de decisiones de calidad.

Son objetivos de cada empresa incrementar sus logros en cuanto a beneficios, a través del uso adecuado de sus recursos tecnológicos, esta acción les permite generar valor a su negocio y atraer oportunidades de

inversión, logrando la excelencia operativa. Otro de los objetivos de la empresas es el de mantener a niveles aceptables y manejables los riesgos que implica las TI. Apuntando de la misma manera, a que sus clientes internos y externos experimenten satisfacción en los servicios ofertados.

Para lograr estos objetivos se requiere de un adecuado gobierno y gestión de la información y los activos tecnológicos. TI constituye actualmente una parte importante del negocio. Y debe ser gestionada y gobernada bajo el cumplimiento de normas. COBIT V.5 es presentado por ISACA (Information Systems Audit and Control Association) como un marco de referencia amplio, que busca ayudar a las organizaciones a cumplir con el alcance de sus objetivos, agregando un valor significativo, mediante la implementación de una adecuada gobernabilidad y gestión de las TI.

2.3.2. Cobit V5: Marco de Referencia para la Auditoría de Sistemas / TI

Cobit V.5, es uno de los últimos productos desarrollados por ISACA, con el objetivo de contribuir a la gestión adecuada y el control interno eficiente de las TI.

> COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público. (ISACA, 2012).

Este marco de referencia consolida la experiencia de al menos 15 años, que han sido acumulados a través de los resultados a las aplicaciones de marcos de referencia similares, teniendo una retroalimentación de los mismos e integrando conocimientos de las principales guías de ISACA. Cobit 5 logra incorporar la experiencia de las mejores prácticas y estándares.

Integra los principios y bases de marcos de referencia especializados y muestra además como los mismos, pueden quedar plenamente orquestados y ser utilizados en conjunto, para ofrecer un mejor control sobre las soluciones TI.

Estándares y guías como: “Information Technology Infrastructure Library (ITIL), The Open Group Architecture Framework (TOGAF), Project Management Body of Knowledge (PMBOK), PRojects IN Controlled Environments 2 (PRINCE2), Committee of Sponsoring Organizations of the Treadway Commission (COSO) y la Organización Internacional de Estándares de normalización (ISO)” (ISACA, 2012), quedan alineados a este marco de referencia y pueden ser vinculados según sea la necesidad de la empresa.

2.3.3. Principios

Los principios que se muestran en la Figura 3, son claves para esta versión de COBIT. “Estos cinco principios habilitan a la empresa a construir un marco de gestión de gobierno y gestión efectivo que optimiza la inversión y el uso de información y tecnología para el beneficio de las partes interesadas” (ISACA, 2012)

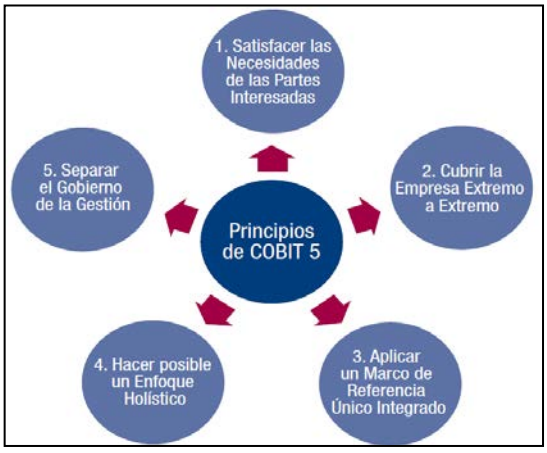


Figura 3: Principios de COBIT 5

Fuente: (ISACA, 2012)

2.3.3.1. Principio 1: Satisfacer las Necesidades de las Partes Interesadas

Toda empresa constituida tiene como importante objetivo la creación de valor, que dependiendo de la naturaleza de la organización puede ser traducido en términos económicos y/o de servicio. Para poder generar este valor se debe encontrar un equilibrio entre la realización de los beneficios, optimización de riesgos y optimización de los recursos tecnológicos como se muestra en la figura 4.

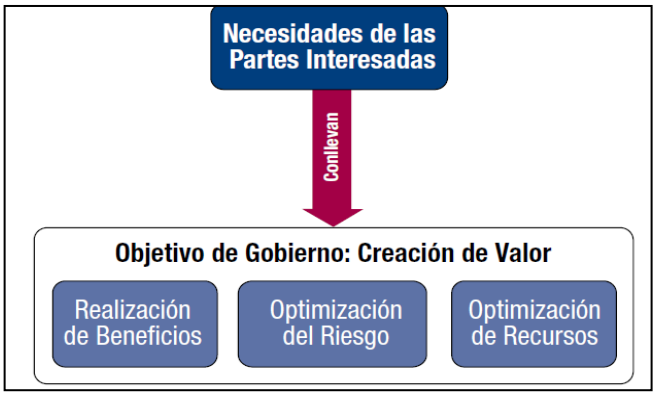


Figura 4: Creación de Valor

Fuente: (ISACA, 2012)

Por la naturaleza de cada organización, es indispensable el desarrollo de sistemas personalizados que contribuyan con el gobierno y la gestión de las entidades, los sistemas deben ser desarrollados de manera que se ajusten al contexto de las mismas, este contexto es afectado tanto internamente como externamente.

CASCADA DE METAS COBIT 5

> Las necesidades de las partes interesadas deben transformarse en una estrategia corporativa factible. La cascada de metas de COBIT 5 es el mecanismo para traducir las necesidades de las partes interesadas en metas corporativas, metas relacionadas con las TI y metas catalizadoras específicas, útiles y a medida. Esta traducción permite establecer metas específicas en todos los niveles y en todas las áreas de la empresa en apoyo de los objetivos generales y requisitos de las

> partes interesadas y así, efectivamente, soportar la alineación entre las necesidades de la empresa y las soluciones y servicios de TI. (ISACA, 2012)

La cascada de Metas de la figura 5 comprende el siguiente proceso que se detalla a continuación:

1. Establecer los motivos de las partes interesadas, estas son generadas a partir de las necesidades de las partes interesadas para crear valor

2. Definir la relación de las partes interesadas con las metas empresariales genéricas. Estas metas corporativas pueden estar vinculadas a su vez con uno o más objetivos genéricos de la empresa.

3. Las metas empresariales tienen una fuerte relación con los resultados que se obtiene de las TI, es por ello que se vincularán con las metas de TI. En donde se podría encontrar que más de una meta corporativa puede estar siendo soportada por una meta de TI.

4. Identificar la metas que se relacionan directamente con TI, identificar los catalizadores (pueden ser descritos como procesos, estructuras organizativas e información), que se están vinculan a las metas de TI.

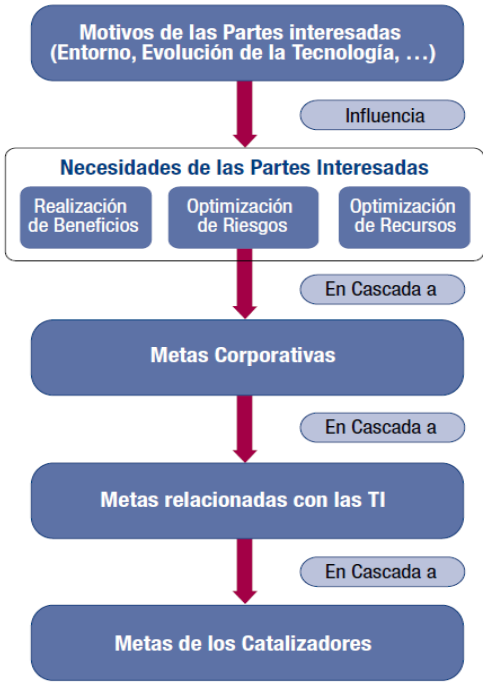


Figura 5: Cascada de Metas

Fuente: (ISACA, 2012)

Principio 2: Cubrir la Empresa de Extremo a Extremo

COBIT integra la gobernabilidad de las TI en el gobierno corporativo. No es un enfoque dedicado únicamente a las TI, por el contrario se ve relacionada corporativamente. Llegando a tratar a las TI como cualquier otro activo de la organización.

> Cubre todas las funciones y procesos necesarios para gobernar y gestionar la información corporativa y las tecnologías relacionadas donde quiera que esa información pueda ser procesada. Dado este alcance corporativo amplio, COBIT 5 contempla todos los servicios TI internos y externos relevantes, así como los procesos de negocio internos y externos. (ISACA, 2012)

Mediante la figura 6, se expone en enfoque de gobierno extremo a extremo que posee COBIT 5, comprendido por los catalizadores de

gobierno, el enfoque de gobierno y la definición de roles, actividades y relaciones

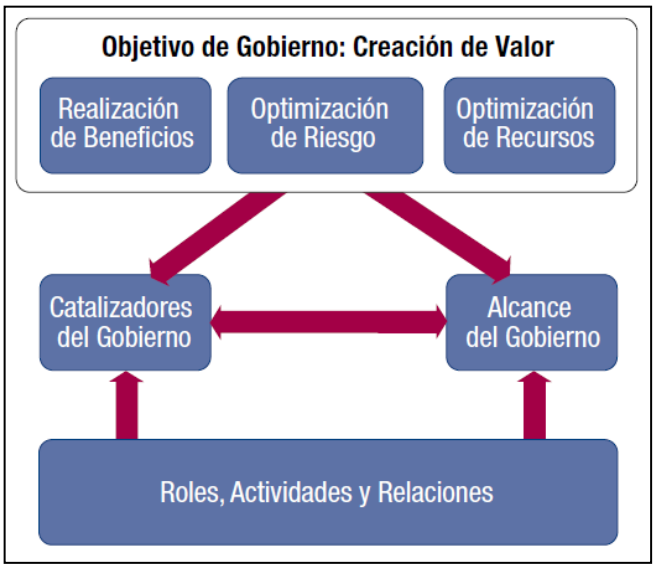


Figura 6: Gobierno y Gestión en COBIT 5

Fuente: (ISACA, 2012)

Catalizadores de Gobierno

Son considerados catalizadores de gobierno aquellos recursos mediante los cuales, es posible alcanzar los objetivos. Estos recursos pueden ser: políticas, lineamientos, principios, estructuras, procesos y prácticas. La ausencia de estos elementos puede provocar una seria afectación a la capacidad de entrega de valor por parte de la empresa

Alcance de Gobierno

El marco de gobierno de COBIT 5 puede ser aplicado a toda una organización, a determinadas áreas de la organización o inclusive a activos tangibles como intangibles. Es importante tener una definición clara del alcance al sistema de gobierno que se va a realizar.

Roles, Actividades y Relaciones

Define quien está involucrado en la gobernabilidad, como se encuentra involucrado, cuales son las actividades y cómo interactúan. Realiza de una manera clara la diferenciación de los dominios tanto de gestión como de gobierno. Apoyándose del principio 5 de COBIT. La figura 7 indica cómo se establecen estas interacciones claves entre roles, actividades y relaciones

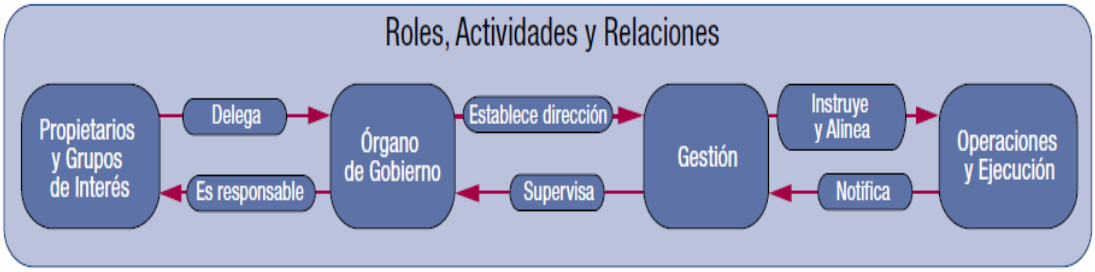


Figura 7: Roles, Actividades y Relaciones Clave de COBIT 5

Fuente: (ISACA, 2012)

2.3.3.2. Principio 3: Aplicar Marco de Referencia Único e Integrado

COBIT 5, es un marco de trabajo que incorpora normas y estándares aceptados, además acopla armónicamente los productos dispersos de ISACA. Es un marco de trabajo para la gestión y gobernabilidad que involucra estándares y guías de una manera eficiente

> Integra todo el conocimiento disperso previamente en los diferentes marcos de ISACA. ISACA ha investigado las áreas clave del gobierno corporativo durante muchos años y ha desarrollado marcos tales como COBIT, Val IT, Risk IT, BMIS, la publicación Información sobre Gobierno de TI para la Dirección (Board Briefing on IT Governance) e ITAF para proporcionar guía y asistencia a las empresas. COBIT 5 integra todo este conocimiento. (ISACA, 2012)

2.3.3.3. Principio 4: Hacer Posible un Enfoque Holístico

Para hacer posible este principio, COBIT 5 recurre a los catalizadores anteriormente ya definidos como factores que influyen de manera individual y/o colectivamente en el éxito o fracaso de algo, en este ámbito en el éxito o fracaso del gobierno y la gestión de las TI. Los catalizadores son guiados a través de la cascada de objetivos revisado en el principio 1. Se tiene una clasificación genérica de 7 tipos para definir la naturaleza del catalizador corporativo según lo indica la figura 8, propuesta por COBIT 5.

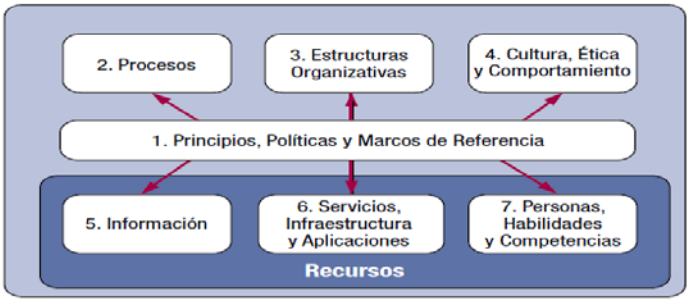


Figura 8: Catalizadores Corporativos COBIT 5

Fuente: (ISACA, 2012)

Dimensiones de los Catalizadores

Mediante la Figura 9, podemos apreciar que COBIT 5, contempla 4 dimensiones genéricas mediante las cuales se tiene la capacidad de entregar una manera sencilla, simple y estructurada el tratamiento de los catalizadores, esto permite a las organizaciones obtener el mando de interacciones complejas, ofreciendo con ello la facilidad de resultados satisfactorios y exitosos.

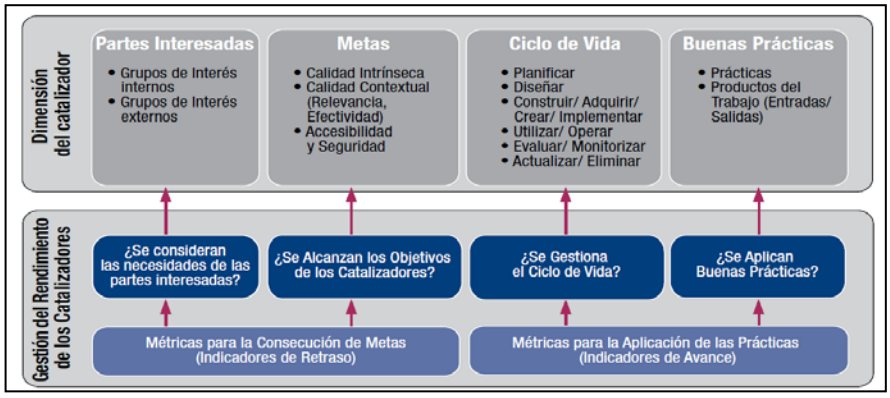


Figura 9: Catalizadores Genéricos de COBIT 5

Fuente: (ISACA, 2012)

Partes interesadas

Cada catalizador tiene vinculado un grupo de interés, estos grupos de interés son parte de las estructuras organizacionales, que juegan un papel activo en el mismo. Los grupos de interés pueden ser tanto internos como externos a la organización. Una meta corporativa muchas veces es la traducción de las necesidades de las partes interesadas sean estas externas o internas.

Metas

Los resultados esperados están estrechamente relacionados con las metas de los catalizadores, su razón de ser radica en la medición y valoración de la consecución de dichas metas. Las metas de los catalizadores son uno de los componentes base de la cascada de metas de COBIT 5. Se encuentran clasificadas en 3 grupos

- Calidad Intrínseca: los resultados miden el nivel de precisión, objetividad y confianza
- Calidad Contextual: se determina que los resultados obtenidos sean útiles en el contexto que fueron requeridos
- Accesibilidad y Seguridad: determina que los resultados fueron obtenidos sean entregados a las áreas autorizadas vigilando que

cumpla con las normativas de seguridad aplicadas a al entorno y que estén disponibles en el momento de su requerimiento.

Ciclo de Vida

Los catalizadores cumplen ciclos de vida que deben tener un seguimiento correcto y completo. Este ciclo de vida comienza desde el momento en que se planifica hasta su eliminación y está conformado por todo el proceso que soporta su vida útil y operacional. Según ISACA, en su artículo COBIT5: Un Marco de Negocio para el Gobierno y la Gestión de la TI para las empresas, se debe considerar las siguientes fases de manera global para el ciclo de vida de un catalizador:

- Planificación
- Diseño
- Construcción / adquisición / creación / implementación
- Utilización / operación
- Evaluación / monitorización
- Actualización / eliminación (ISACA, 2012)

Buenas Prácticas

Las buenas prácticas apoyan y soportan el cumplimiento de las metas y objetivos de los catalizadores. A través de demostraciones prácticas se constituyen en los elementos que indican cómo deben ser implementados los catalizadores, señalando y/o sugiriendo para ello productos, entradas y/o salidas necesarias.

Las buenas prácticas se encuentran conformadas por Marcos de Control, principios, políticas, alcance y validez. ISACA afirma en su publicación que: “Las políticas son un componente clave de los sistemas de control interno en la empresa, cuyo propósito es gestionar y contener el riesgo”. (ISACA, 2012)

Una vez afinadas e integradas con éxito a la empresa sirven como una plataforma de aplicación a toda la organización dentro de un entorno que evoluciona ajustándose a las necesidades del negocio.

2.3.3.4. Principio 5: Separa Gobierno de la Gestión

COBIT 5, enfatiza en una clara distinción entre gobierno y gestión. Cada una engloba sus propias actividades, propósitos y estructuras que no son similares. El Gobierno como tal está enfocado en la evaluación del cumplimiento de metas a través de la medición del rendimiento. En el gobierno por lo general se encuentran involucrados las Juntas, Comités o Consejos de administración.

Por otro lado la gestión implica: planificación, desarrollo, ejecución y supervisión o control de las metas impuestas por la dirección que se establecen por los cuerpos de gobierno con el fin de alcanzar los objetivos de las instituciones.

"El modelo de referencia de procesos de COBIT 5 divide los procesos de gobierno y de gestión de la TI empresarial en dos dominios principales de procesos" (ISACA, 2012). A continuación se muestra en la figura 10, la división descrita

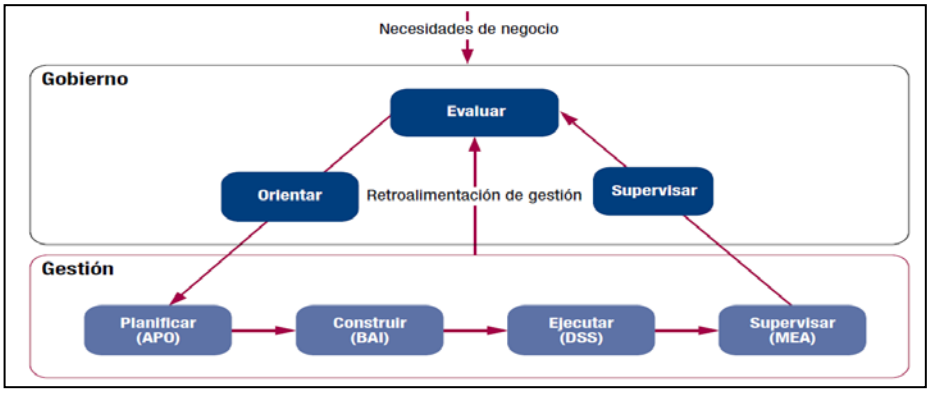


Figura 10: Las Áreas Clave de Gobierno y de Gestión de COBIT 5

Fuente: (ISACA, 2012)

2.3.4. Catalizadores

2.3.4.1. Principios, Políticas y Marcos de Referencia

Principios, políticas y Marcos de referencia son los medios a través de los cuales se traduce el desarrollo del comportamiento que se espera por la autoridad de Gobierno y Dirección de la empresa y de las TI. Son los instrumentos mediante los cuales se socializa el conocimiento y el regimiento de reglas, las cuales contribuyen con metas de gobierno y creación de valor para la empresa.

2.3.4.2. Procesos

“Los procesos describen un conjunto organizado de prácticas y actividades para alcanzar ciertos objetivos y producir un conjunto de salidas como apoyo para alcanzar el total de las metas relacionadas con TI.” (ISACA, 2012) El modelo de referencia de COBIT 5, emplea una distinción de procesos tanto de gestión como de gobierno para las TI, no es una camisa de fuerza para todas las empresas, cada empresa puede organizar sus procesos a la medida según sus necesidades, teniendo en cuenta de que todos sus procesos deben cubrir temas básicos tanto de gobierno como de gestión.

2.3.4.3. Estructuras Organizativas

Las estructuras organizativas son elementos clave en la toma de decisiones de toda organización, COBIT 5 provee a través de matrices RACI, una serie de roles y estructuras predefinidas. Estas estructuras pueden no estar presentes actualmente en todas las empresas por lo que deben ser personalizadas a la dimensión y necesidad de cada organización, las matrices de COBIT 5 son el resultado de un trabajado basado en la experiencia de grupos expertos, en donde se encuentra una generalización de las estructuras, que proveen un valor en el contexto del propósito para las estructuras organizacionales y roles vinculados a los responsables.

2.3.4.4. Cultura, Ética y Comportamiento

Este catalizador hace referencia y se asienta sobre normas de comportamiento en los individuos, tanto unitariamente como colectivamente. “Los objetivos de este catalizador se relacionan con la ética de la organización (determinada por los valores que la empresa quiere vivir), la ética individual (determinada por los valores personales de cada individuo en la empresa) y los comportamientos individuales.” (ISACA, 2012) A través de este catalizador se mide la capacidad de influencia que puede tener un individuo sobre su colectividad o entorno que promueva al comportamiento deseable requerido en toda institución.

2.3.4.5. Información

El siguiente catalizador hace referencia no solo a la información que se obtiene y se procesa por medios automatizados. Sino a la información no estructurada o informal. Que se encuentra generando valor a la empresa.

> Las inversiones en información y tecnologías relacionadas se basan en los casos de negocio, que incluyen análisis coste-beneficio. El coste y beneficio no se refiere sólo a factores tangibles y medibles, sino que también tiene en cuenta factores intangibles tales como la ventaja competitiva, la satisfacción del cliente y la incertidumbre de la tecnología. Sólo cuando se aplica o se utiliza el recurso de la información es cuando una empresa genera beneficios de la misma, por lo que el valor de la información está determinado únicamente a través de su uso (internamente o mediante su venta), ya que la información no tiene valor intrínseco. Es sólo cuando se pone la información en acción cuando se puede generar ese valor. (ISACA, 2012)

2.3.4.6. Servicios, Infraestructura y Aplicaciones

La capacidad de este catalizador se expresa en calidad de servicios, que describen una arquitectura base que soporta las mismas. Los servicios se encuentran generalmente dividido en tres bloques que son: aquellas aplicaciones que proporcionan funcionalidad, infraestructura tecnológica e infraestructura física. En este apartado se determina que “los principios de

arquitectura son directrices generales que rigen la implementación y utilización de los recursos relacionados con las TI dentro de la empresa". (ISACA, 2012)

2.3.4.7. Personas, Habilidades y Competencias

En este catalizador se mide la capacidad del recurso humano, sus habilidades, conocimientos, experiencia y comportamiento que son necesarios e indispensables para el cumplimento de las responsabilidades que exigen las funciones y procesos que realiza la organización a fin de crear valor en sus servicios.

2.3.5. Dominios y Procesos

COBIT V5 maneja 5 dominios dividiendo en dos procesos principales su enfoque : Gobierno de la TI empresarial y Gestión de la TI empresarial, donde Gobierno posee un dominio y Gestión contiene 4 dominios, separados tal como lo muestra la figura 11.

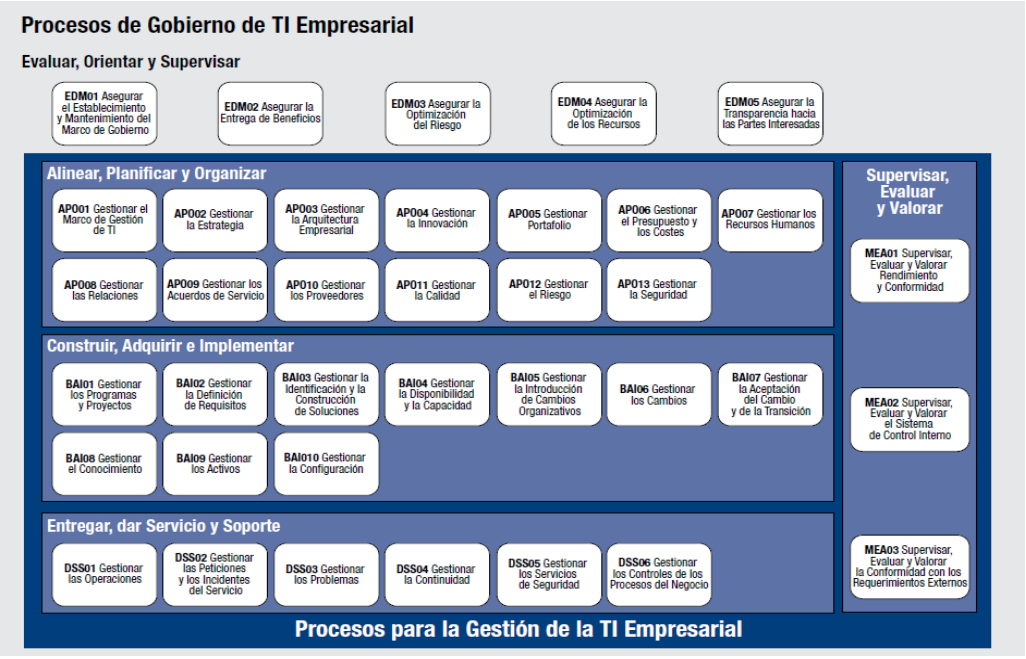


Figura 11: Modelo de Referencia de Procesos de COBIT 5

Fuente: (ISACA, 2012)

COBIT 5 establece al dominio EDM como dominio de Gobierno de las TI, en el que se contempla la Evaluación, Orientación y Supervisión de 5 procesos exclusivos de gobierno. Por otro lado en la Gestión de las TI, COBIT describe 4 dominios en los que a continuación se indica los procesos que contempla:

- Alinear, Planificar y Organizar (APO), contempla 13 procesos de la Gestión de TI
- Construir, Adquirir e Implementar (BAI), contempla 10 procesos de la Gestión de TI
- Entregar, Dar Servicio y Soporte (DSS), contempla 6 procesos de la Gestión de TI
- Supervisar, Evaluar y Valorar (MEA), contempla 3 procesos de la Gestión de TI

COBIT maneja 5 dominios claramente identificados, los cuales se encuentran subdivididos en 37 procesos. “El modelo de referencia de procesos de COBIT 5 es el sucesor del modelo de procesos de COBIT 4.1 e integra también los modelos de procesos de Risk IT y Val IT.” (ISACA, 2012)

2.3.6. Mapeo

Para realizar el mapeo de metas se requiere cruzar las metas corporativas junto con las metas de TI, para ello COBIT 5, en su base de conocimiento reúne todas las metas de estos dos ámbitos que permite una gestión adecuada de la información.

2.3.6.1. Metas Corporativas de Cobit V5

COBIT 5 con el objetivo de dar soporte con las metas empresariales ha establecido al menos 17 metas genéricas de negocio, estas metas encajan en la dimensión del CMI que es un cuadro de mando basado en Balance Score Card (BSC). El CMI es un sistema de administración que permite medir las actividades de una compañía en términos de visión y de estrategia.

CMI sugiere el tener una vista desde cuatro perspectivas que son: Financiera, del cliente, Interna, de Conocimiento y Aprendizaje.

A continuación en la Figura 12 se muestra cuales son estas 17 metas corporativas y como están estas encajadas en el CMI, la figura incluye columnas que indican la relación que tiene con los objetivos de gobierno. Básicamente se definen tres calificativos que son:

- P: Relación primaria, relación directa
- S: Relación secundaria, indirecta
- Ninguna: no existe relación con ningún objetivo

Dimensión del CMI	Meta Corporativa	Relación con los Objetivos de Gobierno		
		Realización de Beneficios	Optimización de Riesgos	Optimización de Recursos
Financiera	1. Valor para las partes interesadas de las Inversiones de Negocio	P		S
	2. Cartera de productos y servicios competitivos	P	P	S
	3. Riesgos de negocio gestionados (salvaguarda de activos)		P	S
	4. Cumplimiento de leyes y regulaciones externas		P	
	5. Transparencia financiera	P	S	S
Cliente	6. Cultura de servicio orientada al cliente	P		S
	7. Continuidad y disponibilidad del servicio de negocio		P	
	8. Respuestas ágiles a un entorno de negocio cambiante	P		S
	9. Toma estratégica de Decisiones basada en Información	P	P	P
	10. Optimización de costes de entrega del servicio	P		P
Interna	11. Optimización de la funcionalidad de los procesos de negocio	P		P
	12. Optimización de los costes de los procesos de negocio	P		P
	13. Programas gestionados de cambio en el negocio	P	P	S
	14. Productividad operacional y de los empleados	P		P
	15. Cumplimiento con las políticas internas		P	
Aprendizaje y Crecimiento	16. Personas preparadas y motivadas	S	P	P
	17. Cultura de innovación de producto y negocio	P		

Figura 12: Metas Corporativas de COBIT 5

Fuente: (ISACA, 2012)

2.3.6.2. Metas de TI de Cobit V5

Las metas TI de COBIT 5 han sido igualmente agrupados en la dimensión del CMI. A continuación en la Figura 13 se muestra cuales son estas 17 metas de TI.

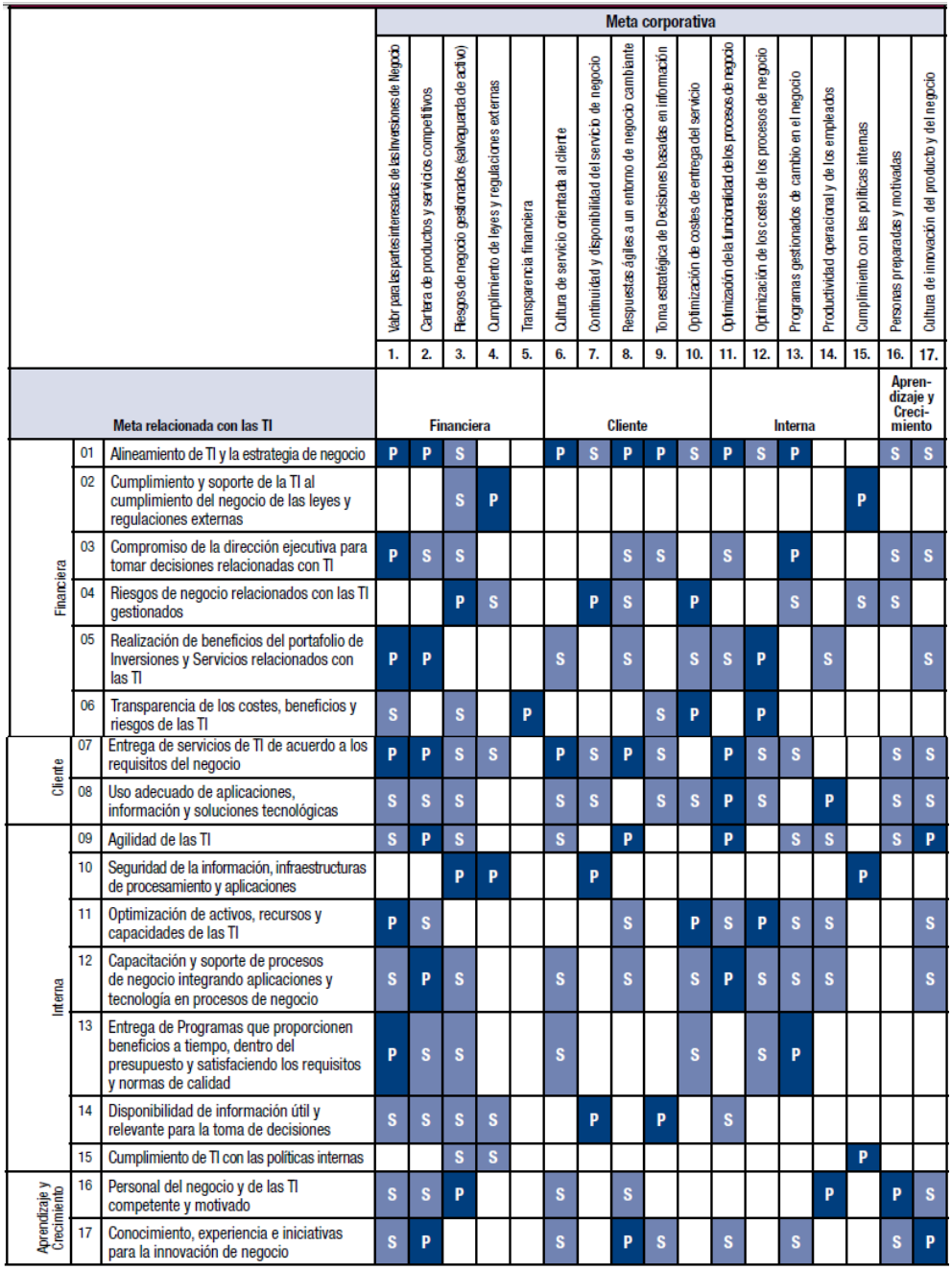
Dimensión del CMI TI	Meta de Información y Tecnología Relacionada	
Financiera	01	Alineamiento de TI y estrategia de negocio
	02	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
	03	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI
	04	Riesgos de negocio relacionados con las TI gestionados
	05	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI
	06	Transparencia de los costes, beneficios y riesgos de las TI
Cliente	07	Entrega de servicios de TI de acuerdo a los requisitos del negocio
	08	Uso adecuado de aplicaciones, información y soluciones tecnológicas
Interna	09	Agilidad de las TI
	10	Seguridad de la información, infraestructura de procesamiento y aplicaciones
	11	Optimización de activos, recursos y capacidades de las TI
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.
	14	Disponibilidad de información útil y fiable para la toma de decisiones
	15	Cumplimiento de las políticas internas por parte de las TI
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio

Figura 13: Metas Relacionadas con las TI en Cobit V5

Fuente: (ISACA, 2012)

2.3.6.3. Mapeo Detallado de Metas

Es preciso indicar que cada compañía debe ajustar las metas según las necesidades de sus negocios, estableciendo las metas genéricas tanto del negocio como de TI para poder realizar el mapeo detallado de metas, tal como se muestra en la figura 14.



		Meta corporativa																
		Valor para las partes interesadas de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activo)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basadas en información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personas preparadas y motivadas	Cultura de innovación del producto y del negocio
		1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
	Meta relacionada con las TI	Financiera					Cliente					Interna					Aprendizaje y Crecimiento	
Financiera	01 Alineamiento de TI y la estrategia de negocio	P	P	S			P	S	P	P	S	P	S	P			S	S
	02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P											P		
	03 Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S
	04 Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S	
	05 Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	P	P				S		S		S	S	P		S			S
	06 Transparencia de los costes, beneficios y riesgos de las TI	S		S		P				S	P		P					
Cliente	07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	08 Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interna	09 Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10 Seguridad de la información, infraestructuras de procesamiento y aplicaciones			P	P			P								P		
	11 Optimización de activos, recursos y capacidades de las TI	P	S						S		P	S	P	S	S			S
	12 Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S
	13 Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	P	S	S			S				S		S	P				
	14 Disponibilidad de información útil y relevante para la toma de decisiones	S	S	S	S			P		P		S						
	15 Cumplimiento de TI con las políticas internas			S	S											P		
Aprendizaje y Crecimiento	16 Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S
	17 Conocimiento, experiencia e iniciativas para la innovación de negocio	S	P				S		P	S		S		S			S	P

Figura 14: Mapeo Detallado de Metas de Cobit V5

Fuente: (ISACA, 2012)

2.4. Cobit V5 para la Seguridad de la Información

2.4.1. Introducción

COBIT 5 for Information Segurity o traducido al idioma Español, *COBIT 5 para la Seguridad de la información* es un producto de la familia de COBIT, que sirve como una guía para profesionales de COBIT 5. ISACA define a seguridad de la información de la siguiente manera: “Asegura que dentro de la empresa, la información está protegida contra su divulgación a usuarios no autorizados (confidencialidad), modificación inadecuada (integridad) y su falta de acceso cuando se la necesita (disponibilidad).” (ISACA, 2012)

Cabe señalar que la característica de integridad de la información, es algo más amplia, involucrando aspectos como la completitud y precisión de dicha información, donde adquiere una relevancia diferente en el ámbito del negocio. En este producto ISACA, se enfoca en una perspectiva que apoya con el cumplimiento para lo que determina Seguridad de la Información.

Esta guía sobre Seguridad de la Información, se encuentra vinculada fuertemente a la confianza de las partes interesadas donde interactúan conjuntamente para obtener el equilibrio del riesgo del negocio o agregando valor al mismo. Seguridad de la información tiene mucho que ver con mitigación de riesgos. Su función es la de proteger la información y todo activo de TI de toda amenaza que se presenta en una sociedad tan cambiante. Es prioritario y de vital importancia preservar el activo de información, no solo para entornos de negocios, sino además para entornos privados.

El Marco de trabajo de COBIT 5 contempla 3 procesos definidos y orientados a la seguridad, estos procesos son: APO13 relacionado al proceso de *Gestionar la Seguridad*, DSS04 relacionado al proceso *Gestionar la Continuidad* y DSS05 relacionado con el *Gestionar los Servicios de Seguridad.* El producto COBIT 5 para la Seguridad de la Información es desarrollado bajo el objetivo que contempla no solo 3 procesos específicos

sino que provee un enfoque general y global que cubre todos los procesos de COBIT 5 de extremo a extremo, de principio a fin y durante todo el ciclo de vida de los 37 procesos que contempla COBIT 5.

2.4.2. Principios Aplicables a la Seguridad de la Información

COBIT 5 para la seguridad de la información, contempla los mismos principios de COBIT 5, ver la figura 5. Para el enfoque de seguridad de la información se agrega una visión específica y marcada para algunas áreas y recursos como se mencionan a continuación:

2.4.2.1. Principio 1: Satisfacer las Necesidades de las Partes Interesadas

COBIT 5 para la Seguridad de la Información considera a la Seguridad de la Información una necesidad de las partes interesadas que provee confianza tanto en clientes internos como externos de una organización. Seguridad de la información debe ser tratada como una necesidad, debe estar presente en la cascada de metas (ver figura 5), debido a que se considera un objetivo tanto interinstitucional como del departamento de TI.

COBIT 5 para la Seguridad de la Información considera una definición de metas específicas tanto para los procesos de apoyo, como para los catalizadores que intervienen en el aseguramiento de dicha información.

2.4.2.2. Principio 2: Cubrir la Empresa de Extremo a Extremo

En este contexto y desde este principio COBIT 5 para la seguridad de la información cubre la empresa de extremo a extremo, integrando todo y todos de las partes interesadas, funciones y procesos que se relacionan con la Seguridad de la Información.

2.4.2.3. Principio 3: Aplicar un Marco de Referencia Único Integrado

COBIT 5 para la Seguridad de la Información contiene una base sólida de conocimientos, que han sido integrados de diferentes marcos de ISACA, estos marcos reconocidos para Seguridad de la Información son: COBIT,

ValIT, RiskIT y BMIS. Adicional se sustenta en el conocimiento de estándares enfocados a cuestiones de Seguridad “tales como la serie ISO/IEC 27000, el Estándar de Buenas Prácticas para Seguridad de la Información de ISF y el SP800-53A del U.S. National Institute of Standards and Technology (NIST).” (ISACA, 2012)

2.4.2.4. Principio 4: Hacer Posible un Enfoque Holístico

COBIT 5 promueve un enfoque holístico, que debe tener en cuenta todas las partes que interactúan. Para el alcance de este objetivo este marco administra 7 catalizadores que desde este enfoque serán factores que individual y colectivamente afectarán el rendimiento de los procesos, provocando el funcionamiento o no funcionamiento del gobierno y la gestión de las TI vinculado con un gobierno de aseguramiento de la Información.

A través de la figura 15, se plantea el modelo sistémico para dar lugar a un enfoque holístico orientados a velar por la seguridad de la información a través de los 7 catalizadores que maneja COBIT 5

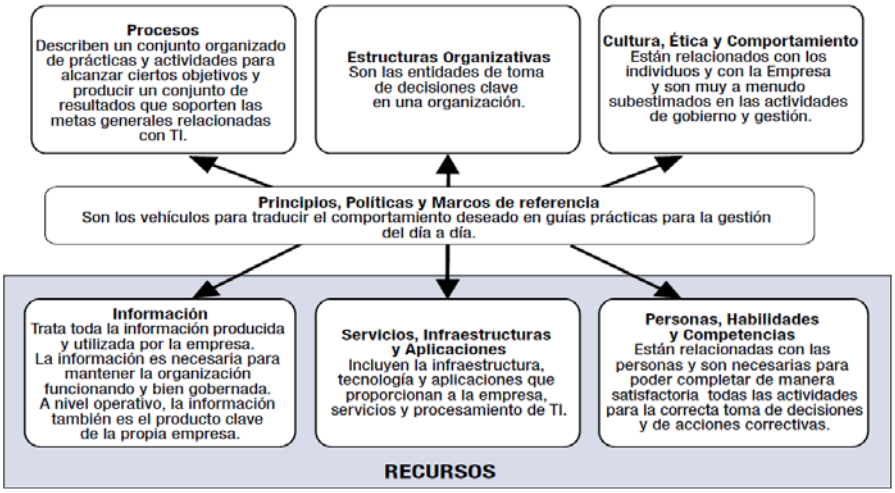


Figura 15: Modelo Sistémico con Interacción de Catalizadores

Fuente: (ISACA, 2012)

2.4.2.5. Principio 5: Separa Gobierno de Gestión

"En la práctica, los diferentes roles del gobierno y gestión de la seguridad de la información se hacen visibles mediante el modelo de procesos de COBIT 5, que incluye procesos de gestión y procesos gobierno, cada grupo con sus propias responsabilidades". (ISACA, 2012). Estos roles tanto de gobierno como de gestión están presentes en la Figura 6.

2.4.3. Catalizadores para la Seguridad de la Información

2.4.3.1. Principios, Políticas y Marcos de Referencia

Modelo de Principios, Políticas y Marco de Referencia

De acuerdo a este modelo se contempla la definición y establecimiento de políticas por un grupo de las partes interesadas, mientras que las otras partes se encargan del cumplimiento de las mismas. Todo principio, política o marco de referencia constituye un mecanismo de comunicación que contribuye al soporte para cumplimiento de metas de gobierno y que generen valor a las instituciones.

> Los principios deberían estar limitados en número y expresados en un lenguaje sencillo. Las políticas proporcionan una directriz más detallada respecto a cómo llevar a la práctica los principios; influyen respecto a cómo la toma de decisiones se alinea con dichos principios. (ISACA, 2012)

Este marco de referencia requiere la determinación de personal que valida las políticas, la determinación de consecuencias en caso de no cumplimiento con la normativa establecida, aclaración específica de excepciones y fijación de los mecanismos que hagan posible la medición y comprobación del cumplimiento de las políticas. Se debe contemplar que al surgir un problema operacional, las primeras herramientas de consulta deben ser los requisitos y documentación correspondiente a la seguridad de la información, en el supuesto que no se cuente con esta información las

siguientes herramientas de apoyo son los procedimientos de seguridad de la información y las políticas vinculadas a los mismos.

El desarrollo de guías específicas para las empresas en cuanto a políticas, procedimientos y requerimientos de seguridad, puede tener en cuenta los diferentes estándares de seguridad, marcos de referencia y/o estándares obligatorios. Es importante aclarar que si una entidad decide obtener la certificación de ISO/IEC 27001, dicha organización deberá validar y comprobar que la empresa cumple con la norma.

Principios de Seguridad de la Información

Los principios son considerados como las reglas que establece cada institución para dar un soporte efectivo a los objetivos de gobierno y generación de valor. Debe existir un número determinado de principios, así como también los mismos deben ser expresados en un lenguaje claro y entendible, de fácil asimilación, sin que se requiera un conocimiento técnico para ser entendible. ISACA realiza la siguiente afirmación:

> Tres organizaciones globales líderes en seguridad de la información el año 2010, consolidaron esfuerzos y experiencia para el desarrollo de al menos 12 principios independientes y no propietarios que han sido una contribución para los profesionales de seguridad de la información al añadir valor a sus organizaciones mediante el apoyo al negocio con éxito y la promoción de las buenas prácticas de seguridad de la información. (ISACA, 2012)

Estos 12 principios han sido separados en tres grupos por COBIT 5, los cuales centran su esfuerzo en áreas de Soporte del Negocio, defensa del negocio y la promoción para un comportamiento responsable en temas vinculados a la seguridad de la información. En la figura 16, se presentan 6 de los 12 principios clasificados para el área de soporte del Negocio

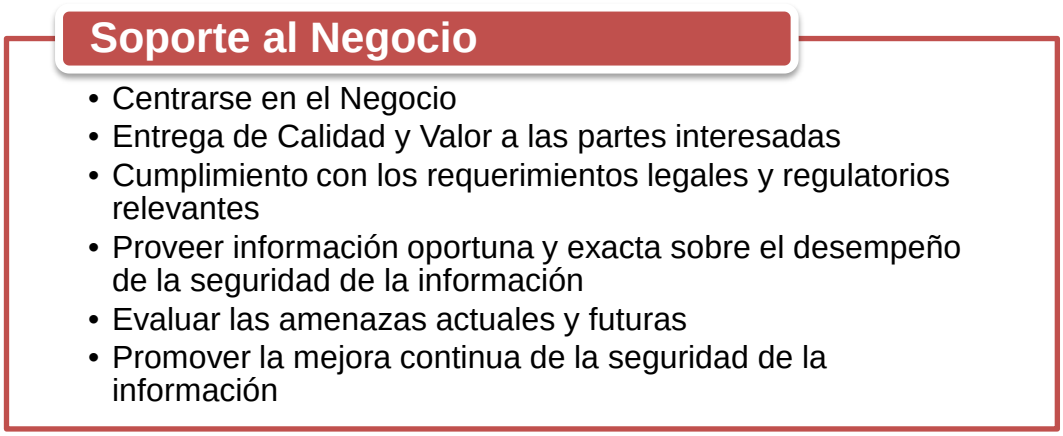


Figura 16: Principios de Soporte al Negocio

Fuente: (ISACA, 2012)

La figura 17 muestra como se encuentran divididos los principios para el área de defensa del negocio:

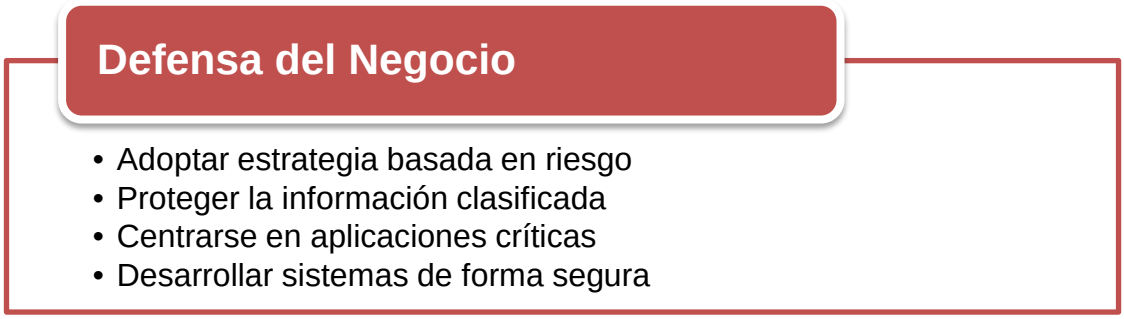


Figura 17: Principios de Defensa del Negocio

Fuente: (ISACA, 2012)

La figura 18 muestra como se encuentran divididos los principios para el área de promoción de comportamiento responsable para la seguridad de la información de las organizaciones, indicadas de una manera genérica:

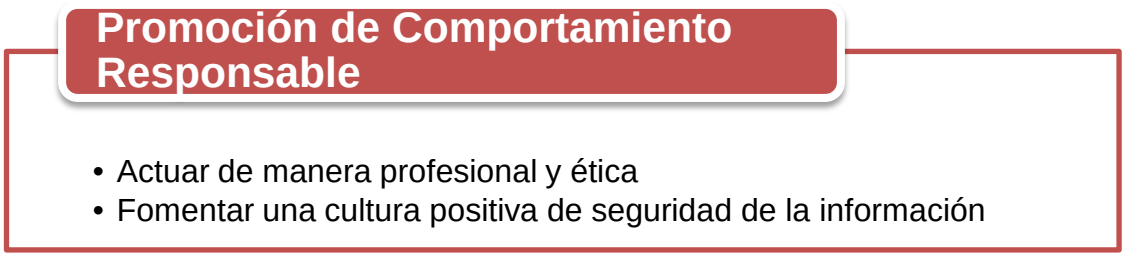


Figura 18: Principios de Promoción Comportamiento Responsable

Fuente: (ISACA, 2012)

Políticas de Seguridad de la Información

Las políticas son consideradas aquellas guías que brindan una orientación sobre cómo poner en práctica los principios establecidos por los organismos de dirección de la empresa. Las políticas deben contener atributos como los siguientes: alcance, validez y metas. Cabe indicar que no todas las políticas están en capacidad de presentar todos los atributos y son las excepciones que se clasifican a las políticas como políticas que están dirigidas por otras funciones que no son las de seguridad dentro de la empresa

A continuación se describe una serie de políticas relacionadas con el ámbito de seguridad que pueden ser consideradas en las organizaciones dependiendo de su naturaleza y control:

- Política a la seguridad de la Información
- Política de Control de Accesos
- Política de la Seguridad de la Información Personal
- Política de la Seguridad Física y Ambiental
- Política de la Gestión de Incidencias
- Política de la Continuidad del Negocio
- Política de la Gestión de Activos
- Reglas de Comportamiento

- Política de Adquisición, Desarrollo de Software y Mantenimiento de Sistemas
- Política de Gestión de Proveedores
- Política de la Gestión de Comunicaciones y operaciones
- Política de Cumplimiento
- Política de la Gestión de Riesgos

Adaptación de Políticas al Entorno

"El contenido de las políticas de la empresa cambiará dependiendo del contexto de la organización y del entorno en el que opera." (ISACA, 2012) Al momento de implementar una política se debe considerar el ambiente y escenario de la empresa ya que existen factores que afectan su implantación y desarrollo como los que a continuación se expone:

Regulación a medida de la empresa, es decir, únicamente aplicables a la empresa, toma de los requerimientos tanto funcionales como operacionales del negocio, necesidad de normas aplicables a propiedad intelectual y protección de datos. Además no se debe obviar factores como la existencia de políticas que garanticen un alto nivel y cultura corporativa. También se debe tomar en cuenta el diseño especializado y único de arquitecturas tecnológicas, tampoco se deberá dejar por fuera regulaciones gubernamentales que abarquen el contexto de la seguridad de la información. Ni estándares aceptados.

COBIT 5 para la Seguridad de la Información propone algunas alternativas sobre el posible contenido que debe ser contemplado en las políticas de Seguridad de la Información como se indica a continuación:

- "Cobertura dentro de la empresa
- Presupuesto y gestión de costes del ciclo de vida de la seguridad de la información
- Planes estratégicos y gestión de cartera de la seguridad de la información
- Visión, metas y métricas
- Innovación y buenas prácticas

- Creación de valor
- Comunicación e información a las partes interesadas
- Gobierno de la tecnología y la arquitectura
- Cultura y concienciación en seguridad de la información
- Propiedad atribuida a las partes interesadas relevantes sobre la información crítica
- Proveedores y terceros” (ISACA, 2012)

Ciclo de Vida de las Políticas

Uno de los procesos considerados en APO01 define: Mantener los catalizadores del sistema de gestión. Para ello es imprescindible una adecuada gestión de las políticas lo que implica supervisar el ciclo de vida de las mismas. La tecnología avanza constantemente y cada día está expuesta a innovaciones y por consiguiente, si no son evaluadas las políticas corren el riesgo de quedar obsoletas. La evolución acarrea actualizaciones necesarias que son parte del ciclo de vida de las políticas. Es necesaria una revisión permanente de vigencia y efectividad de las políticas que validen el cumplimiento de las regulaciones locales y de orden gubernamental.

2.4.3.2. Procesos

Modelo de Procesos

El modelo de procesos está compuesto por las partes interesadas que se dividen en internas y externas. Cada parte interesada juega un rol y posee responsabilidades específicas. Toda la responsabilidad se encuentra documentada a través de las matrices RACI, las cuales conservan la información de quién realiza, quién es el responsable, a quién se le consulta o quién se le informa.

Los procesos son clasificados por sus metas, se identifica las metas intrínsecas, contextuales, de accesibilidad y seguridad. Por cada nivel las metas definen una métrica a través de la cual es posible verificar hasta donde fue alcanzada dicha meta. Los procesos siempre están definidos por

un ciclo de vida que se constituye en su creación, operación, supervisión, mantenimiento y/o retiro. Las prácticas genéricas ayudan a los procesos a ejecutar un correcto ciclo de vida.

Los procesos siempre deberán estar identificados a través de su etiqueta de proceso, nombre de proceso, área a la que corresponde; sea esta de gobierno o de gestión y estará identificada al dominio al que pertenece. Los procesos deben estar siempre descritos, conteniendo una descripción de la visión general y una visión de alto nivel, que significa de cómo el proceso lleva a cabo su propósito.

La declaración del proceso permite conocer el propósito general del proceso. Las metas y métricas del proceso están orientadas a la seguridad de la información del proceso específico. El proceso deberá tener la información adicional que mencione: título y descripción de la práctica, sus respectivas entradas y salidas y sus actividades del proceso, todas estas vinculadas a la seguridad de la información.

Procesos de Gobierno y de Gestión

COBIT 5 para la Seguridad hace una clara diferenciación de aquellos procesos que deben ser considerados en el ámbito tanto de gestión como de gobierno respectivamente. Al final la orquestación de ambos tipos de procesos tiene como acometido, el gobierno y gestión integral de lo que respecta a la seguridad de la información.

Los procesos de gobierno en el ámbito de la seguridad de la información se centran en temas claves como: proveer valor y generar una optimización de riesgos y recursos. Evalúa las estrategias adoptadas tanto para prácticas como para actividades, con el fin de proporcionar una guía clara, que se oriente a la seguridad de la información, apoyándose en conceptos con base en estándares como la norma internacional ISO/IEC 38500 de Gobierno de las TI en la organización.

Para temas de procesos de gestión se entiende que los mismos se orientan a cubrir de extremo a extremo a la empresa, velando por que las actividades y prácticas cubran las áreas que involucran responsabilidad tanto en su planificación, construcción, ejecución y supervisión. Los resultados que se obtienen de ambos procesos son diferentes entre sí y tienen una audiencia diferente.

2.4.3.3. Estructuras Organizativas

Modelo de Estructuras Organizativas

El modelo de estructuras organizativas de COBIT 5 para la seguridad se compone de los siguientes elementos: partes interesadas, metas, ciclo de vida y buenas prácticas. Las partes interesadas tienes un rol importante pero es variable ya que dependen del papel que jueguen, en este contexto sus actividades podrían ser en forma de toma de decisiones, asesoramiento o influencia.

En cuanto a las metas el catalizador debe considerar la aplicación de varias actividades y la toma de buenas decisiones respaldadas por mandatos adecuados, principios operativos bien declarados e implementación de buenas prácticas. El ciclo de vida de una estructura organizativa debe tener un inicio y un fin o la justificación adecuada de su permanencia, además deberá probar su razón de ser, es decir, deberá tener una razón definida y el propósito de su existencia.

Los roles de las estructuras organizativas desde el punto de vista de seguridad de la información están definidas en dos categorías. La primera corresponde a roles y estructuras específicas, que son estructuras internas en funciones de seguridad. La segunda categoría pertenece a roles y estructuras relacionadas, que hacen referencia a miembros que no se encuentran implícitos dentro de las funciones de seguridad donde, pueden ser considerados: usuarios como propietarios de los procesos de negocio.

Roles y Estructuras de la Seguridad de la Información

COBIT 5 para la Seguridad de la información define varias estructuras con sus respectivos roles para empresas normales que pueden ser consideradas empresas medianas a grandes, sin embargo, dependiendo de la empresa se puede ajustar los roles de seguridad a los siguientes:

“Administrador de Seguridad de la Información, Arquitectos de la Seguridad de la Información y Oficiales de cumplimiento y auditorias de seguridad de la información” como lo menciona ISACA (ISACA, 2012). Esto no es una camisa de fuerza en la estructura de la organización en todas las empresas, ya que si hablamos de una empresa pequeña, todas las tareas llegan a ser de responsabilidad del gerente de seguridad de la información.

Para empresas grandes se debe concentrar un mayor esfuerzo en la seguridad de la información, deberá inclusive llegar a ser más elaborada, incluyendo la adición tanto de estructuras como roles. Se debe hacer una especial distinción de la relación de la seguridad de la información con las TI. Cuando la seguridad de la información se encuentra comprometida y afectada por las TI, es posible que se deba a intereses de TI. Mientras las TI por cumplimiento, ofrecen el servicio a la empresa o gestionan el riesgo relacionado con la protección de la información, pueden recurrir a una falta de prácticas de seguridad de la información, anteponiendo el servicio.

Responsabilidad Sobre la Seguridad de la información

Cada posición en funciones de seguridad, es un factor clave que permite determinar el grado en la estructura organizativa que vigilia la seguridad a fin de mantener una protección correcta y eficaz de su información. Esta unidad marca una gran diferencia entre una posición de vigilancia proactiva y no solo una que se activa o entra en operación el momento de mitigar los riesgos, que son muy limitadas. El consejo de dirección tiene la responsabilidad final de todos los temas, incluyendo la seguridad de la información.

> Esta responsabilidad puede y debe ser delegada en el nivel adecuado dentro de la empresa. Teniendo en cuenta que la seguridad de la información es una cuestión crítica para el negocio, la organización siempre debe asignar la responsabilidad final sobre la seguridad de la información a un alto miembro de la dirección ejecutiva. De no hacerlo, se puede exponer al consejo directivo a las reclamaciones por negligencia por parte de los reguladores o de otros grupos de interés, en caso de que ocurra un incidente. (ISACA, 2012)

2.4.3.4. Cultura, Ética y Comportamiento

Modelo Cultural

El modelo de cultura para la seguridad de la información en COBIT 5 interactúa con los siguientes componentes: partes interesadas, objetivos, ciclos de vida y buenas prácticas. Las partes interesadas constituyen un todo en el aspecto de cultura, ética y comportamiento, por un lado son los grupos de las partes interesadas quienes se encargan de establecer, ejecutar y vigilar el cumplimiento de los comportamientos deseados en una institución.

Por otro lado otra parte de las partes interesadas se encargan de ajustarse a los reglamentos y conductas establecidas a través de normas. Todos los grupos de interés son regidos e influenciados para cumplir con una cultura que en caso de Seguridad de la Información actuará para concienciar sobre las situaciones de seguridad.

Este catalizador tiene como objetivo, influenciar en el comportamiento colectivo organizacional que está determinado y establecido en los valores que la empresa desea evidenciar en el ambiente laboral. También son influenciados como individuos, alineados a los objetivos individuales de la empresa, así como en el comportamiento deseado de cada individuo ante sus responsabilidades.

La cultura, la ética y el comportamiento tienen un ciclo de vida que a partir del momento en que una cultura existe es valorada para ejecutar los diferentes mecanismos a fin de aplicar cambios que sean necesarios para obtener los resultados esperados en este catalizador. Para ello existe el

apoyo de normativas que contribuyen para el mejoramiento del la misma. Las buenas prácticas para generar un resultado deseable a nivel de este catalizador, involucran las siguientes actividades que deben ser tomadas en cuenta para la creación, apoyo y mantenimiento de un patrón de comportamiento deseado:

- “Comunicación de comportamientos deseados y valores corporativos de la empresa.
- Conocimiento de conducta deseada
- Motivaciones e Incentivos para promover el cumplimientos de normas y reglas “ (ISACA, 2012)

Se debe tener presente que el recurso humano y su comportamiento son variables que afectan el éxito en toda organización, por pequeña que sea. Determinan el nivel cultural a nivel de las empresas. Existen muchos aspectos que los influencian: política religión, raza, pensamiento, experiencias, objetivos e inclusive hasta ambiciones a nivel individual como a nivel colectivo.

Es importante resaltar que las organizaciones deben adoptar y educar hacia una cultura orientada a la seguridad de la información. Logrando que esta sea intencional, consistente, capaz de ser una guía para las actividades diarias de todos los recursos humanos implícitos en el desarrollo de la seguridad de la información.

Ciclo de Vida de la Cultura

Es importante comprender que existe ya una cultura formada en cada individuo y esta es el resultado de la evolución en el tiempo. De la misma forma existe también ya una cultura organizacional. Ambas de acuerdo al comportamiento y conciencia de cada individuo pueden ser más asertivas que otras. Esta es la razón que motiva la evaluación de una cultura ya presente.

Existen varios métodos que nos permiten cumplir con este objetivo de evaluación como los que se detalla a continuación: calidad y consistencias de contraseñas, políticas para la utilización de dispositivos USB en ordenadores, identificación de información sensible, disponibilidad de información a personal autorizado, candados de protección para equipos e información, etc.

No se trata de un listado que debe ser cumplido al pie de la letra sino más bien de una orientación en la que pueden ser tomados o no en cuenta todos los parámetros indicados. Cabe recalcar que la información que se puede obtener a través de estos parámetros susceptibles de medición, ofrece muy poco valor. Es necesaria que esta medición sea evaluada a lo largo de un periodo de tiempo, donde ofrecerán un conocimiento más sólido y consistente de sus resultados.

Líderes y Campeones

Como parte de la creación de una cultura para la seguridad de la información, se requiere personas con disposición de diálogo, que puedan ser considerados como modelos de comportamiento al personal que está detrás. Lo roles más calificados para estas personas están definidos en el perfil de Gestores de Proyectos, ejecutivos de alto nivel, directores entre otros generalmente reconocidos en posiciones de autoridad con un alto grado de influencia en el comportamiento de los patrones humanos.

La influencia es una aptitud muy bien catalogada para los representantes de las diferentes unidades de dirección quienes tienen una carga de responsabilidad con la toma de decisiones, dentro de este ámbito juega un rol importante la preservación de la seguridad de la información. Según ISACA en su artículo de COBIT 5 para la Seguridad de la información el liderazgo puede ser catalogado de tres tipos: “de dirección ejecutiva, dirección de negocio y CISO/ISM” (ISACA, 2012)

Comportamiento Deseable

Un comportamiento deseable es obtenido mediante la interacción y coordinación de Ética Organizativa, ética individual y el liderazgo. Esto provoca una influencia considerada positiva para el desarrollo de una cultura sostenible, en temas de seguridad se debe considerar aspectos como los siguientes en la práctica de actividades que fortalezcan una cultura de seguridad:

- Prácticas de seguridad involucradas en operaciones diarias
- Un concienciación sobre el porqué de las políticas y principios de seguridad deben existir y deben ser cumplidos
- Una adecuada socialización de políticas y principios
- Concienciación sobre la importancia del rol de seguridad que cada uno cumple en sus actividades por mínimas que sean.
- Respuesta inmediata, eficaz y responsable ante amenazas.

2.4.3.5. Información

Modelo de Información

La información como catalizador es un parámetro clave para la seguridad de la información, implica la guía base mediante la cual se gestiona la toma de decisiones, teniendo en cuenta que esta puede ser una plataforma para el desarrollo de estrategias que den lugar a la seguridad de la información. En cuanto al catalizador los elementos que intervienen y se valoran son: partes interesadas, metas, ciclo de vida completo y buenas prácticas.

Puede estar constituida de partes interesadas tanto internas como externas, donde se debe determinar, cual es su grado de preocupación y la causa de su interés sobre dicha información. Sus metas dependiendo del tipo de información pueden ser clasificadas como metas intrínsecas, contextuales, de seguridad y accesibilidad. Se deben considerar todas las

etapas del ciclo de vida que contempla la información, este es un ciclo muy general que cruza, desde su inicio hasta su fin. Se considera en este ciclo las siguientes fases: planificación, diseño, construcción, operación, supervisión y eliminación.

La información es presentada mediante seis capas, desde el contexto físico en donde son capturadas y vinculadas a las herramientas tecnológicas hasta el mundo social donde cobran valor y dan sentido a la información propiamente dicha. Las buenas prácticas se encargan de presentar de una manera continua los atributos que tiene la misma mientras a traviesa dichas capas.

Tipos de Información

La información puede ser de ámbito de gestión o de gobernabilidad en la seguridad de la información. Cada información sirve para un propósito específico que es utilizado dentro de los ámbitos indicados antes. En la figura 19, se presenta una lista que no es una camisa de fuerza, pero que busca proveer una visión más detallada de cómo la seguridad de la información se expande a toda la organización.

Esta lista presentada en la figura 19, puede ser más reducida o extensa, esto depende mucho del entorno de la empresa en el cual se está valorando la existencia de la información catalizadora por lo que debe ser considerado según la capacidad de cada empresa.

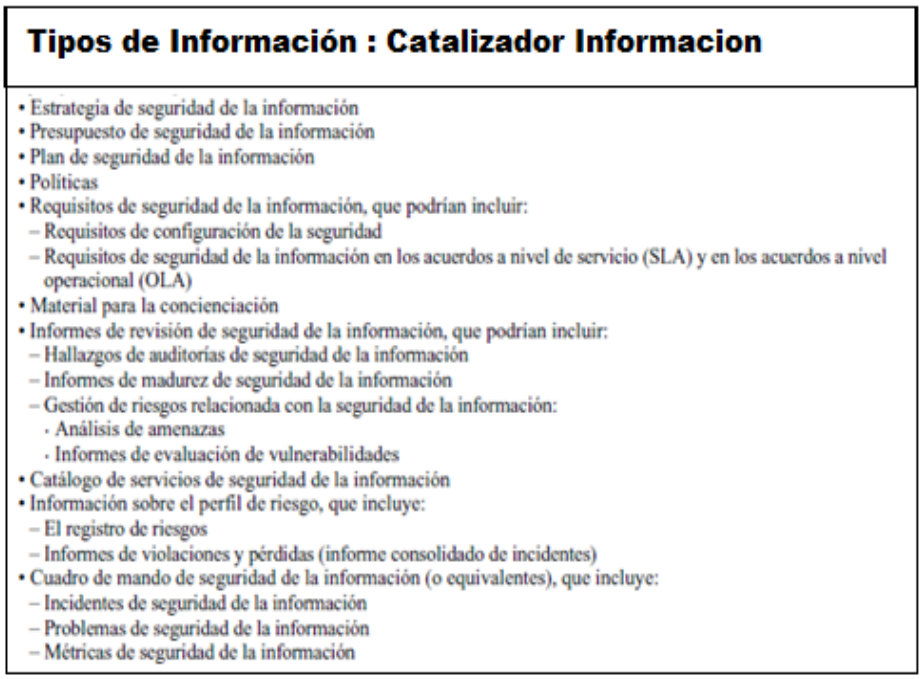


Figura 19: Tipos de Información

Fuente: (ISACA, 2012)

2.4.3.6. Servicios, Infraestructura y Aplicaciones

Modelo de Servicios, Infraestructuras y Aplicaciones

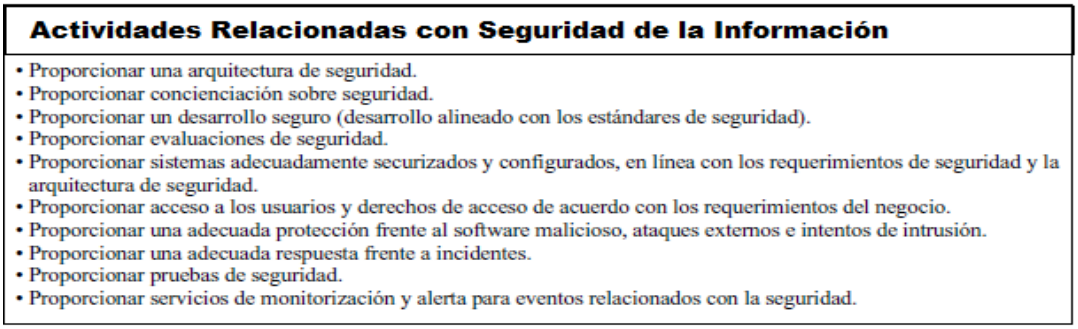
Las partes interesadas de este modelo indican la evidencia de la calidad de los servicios que brindan, sean que estos se encuentren provistos de una manera interna o externa. El enfoque central de las partes interesadas estará definido por el tipo de interesados, que al ser grupos de interés internos se centrarán en la valoración de los servicios ofertados. Por otro lado los grupos de interés externos validarán que son adecuados los niveles y la calidad de servicios que a su vez son entregados a los usuarios.

Los objetivos de este catalizador medirán que los servicios provistos a través de aplicaciones, infraestructura y tecnología sean satisfactorias y se encuentren debidamente sustentados. El ciclo de vida de este catalizador es sustentado básicamente en una arquitectura objetivo, donde se contempla la adquisición y/o implementación de aplicaciones describiendo sus diferentes nexos y relaciones.

La capacidad de los servicios debe contener al menos la descripción de los principios de arquitectura utilizados, sus perspectivas, que deben ser lo más adecuadas y efectivas posibles al contexto de la organización y adicional poseer un respaldo de arquitecturas antiguas. Todo lo descrito anteriormente constituye la definición de una buena práctica que se debe contemplar para la medición de las capacidades de servicio de una organización con relación a sus TI orientadas al aseguramiento de la información.

Servicios, Infraestructuras y Aplicaciones de Seguridad de la Información

Los servicios requieren la interacción de varios catalizadores para proveer capacidades y funcionalidades relacionadas con la seguridad de la información. Generalmente se debe tener en cuenta que cada servicio se encuentra enlazado a uno o más procesos, cada uno con sus respectivas prácticas y actividades. Como parte del resultado, los servicios al final se componen de entradas y salidas, donde también se tiene la intervención de las estructuras organizativas. A través de la siguiente lista se enumera un detalle de actividades que están relacionadas a la seguridad de la información dentro de los servicios. Este detalle es solo una visión general de las actividades contemplada en Cobit 5 para la seguridad de la información en el catalizador servicios, infraestructuras y aplicaciones, ver figura 20.



Actividades Relacionadas con Seguridad de la Información

- Proporcionar una arquitectura de seguridad.
- Proporcionar concienciación sobre seguridad.
- Proporcionar un desarrollo seguro (desarrollo alineado con los estándares de seguridad).
- Proporcionar evaluaciones de seguridad.
- Proporcionar sistemas adecuadamente securizados y configurados, en línea con los requerimientos de seguridad y la arquitectura de seguridad.
- Proporcionar acceso a los usuarios y derechos de acceso de acuerdo con los requerimientos del negocio.
- Proporcionar una adecuada protección frente al software malicioso, ataques externos e intentos de intrusión.
- Proporcionar una adecuada respuesta frente a incidentes.
- Proporcionar pruebas de seguridad.
- Proporcionar servicios de monitorización y alerta para eventos relacionados con la seguridad.

Figura 20: Actividades Relacionadas con la Seguridad de la Información
Fuente: (ISACA, 2012)

2.4.3.7. Personas, Habilidades y Competencias

Modelo de Personas, Habilidades y Competencias

Este catalizador involucra a todas las partes interesadas que existen con el objetivo de cumplir un rol específico, para los cuales existe un perfil de habilidades y capacidades específicas. El objeto de este catalizador busca la medición de los niveles de preparación académica y la demostración de los mismos, también contempla la definición de las habilidades técnicas, la habilidad del recurso humano basado en la experiencia adquirida a lo largo de sus oportunidades laborales.

Además de ello se toma en cuenta el conocimiento adquirido y sus destrezas de comportamiento. Todo este conjunto de parámetros permiten una visión más amplia del cumplimiento satisfactorio en las actividades de cada proceso para el que es diseñado el rol de cada parte. El ciclo de vida de este catalizador determina que las habilidades actuales llegan a representar su línea base en la organización, y solo a través de esta es posible realizar las capacitaciones necesarias de lo que se quiere lograr.

Sobre este catalizador se deriva la influencia de las metas y estrategias de la organización. A través de la capacitación, es posible lograr un desarrollo de habilidades mediante la formación de recursos. También en este catalizador se considera la incorporación de de recursos ya capacitados, el reconocimiento de todos los roles necesarios para cumplir con los procesos de la organización y la disminución consciente de recurso subutilizado, debido a la inclusión de procesos automatizados, externalización de servicios, entre otros. El catalizador requiere de la adopción de buenas prácticas que favorezcan las destrezas y competencias, a través de una adecuada definición de necesidades en requisitos objetivos que debe cumplir el perfil de cada rol.

Habilidades y Competencias Relacionadas con la Seguridad de la Información

En temas de seguridad de la información se presenta una serie de habilidades y competencias deseables que debe tener el personal a cargo de la seguridad de la información, según lo establece Isaca en su artículo "COBIT 5 para la Seguridad de la información". Ver Figura 21.

Habilidades/Competencias
Gobierno de seguridad de la información
Formulación estratégica de seguridad de la información
Gestión del riesgo de la información
Desarrollo de la arquitectura de seguridad de la información
Operaciones de seguridad de la información
Evaluación, pruebas y cumplimiento de la información

Figura 21: Habilidades/Competencias de la Seguridad de la Información

Fuente: (ISACA, 2012)

Las competencias y habilidades expresadas en la figura 21, cabe aclarar que, en empresas de gran tamaño pueden estar definidas o ser equivalentes a puestos específicos de trabajo. En empresas medianas y pequeñas la realidad de estas características, se encuentran delimitados sobre puestos o cargos de seguridad de información general, estos son más localizados en recursos que los de una gran organización.

2.4.4. Mapeo Detallado de Procesos de Cobit V5

COBIT 5 for Security Information entrega en sus guías un aporte que permite a los auditores y/o expertos en seguridad realizar un mapeo de alto nivel a cada procesos de los dominios de COBIT. Este es un mapeo detallado tomado de los documentos guías que ofrece la base de conocimiento de ISACA, detalla el último mapeo de COBIT 5 donde se alinea con la norma internacional ISO/IEC 27001:2013, que es una norma aceptada y validada internacionalmente para cubrir el tema de seguridades de la información.

Por enfoque del tema de proyecto, esta auditoría se encuentra centrada en el catalizador de procesos, estará basada en los requerimientos de la gerencia de la empresa y su entorno operativo que en términos de seguridad concluirá con los criterios sólidos sobre la aplicación de guías, normas, estándares y/o reglamentos alineados a la seguridad de la información.

2.4.5. Norma ISO/IEC 27001:2013

En el año 2004 se publica el primer documento relacionado a los Sistemas de Gestión de Seguridad de la Información (SGSI), este documento se convierte en una adopción a la norma británica reconocida como BS 7799-2-2002 y se considera por primera vez la posibilidad de certificación. Posteriormente esta norma es adoptada por Organismo Internacional de Estandarización (ISO) y por la Comisión Electrónica Internacional (IEC), dando lugar a la norma ISO/IEC 27001:2005 la cual llega a ser lo suficientemente consistente con la norma ISO 27002:2005 que se basa también en la norma británica BS 7799-1-2002. Se desarrolla una nueva versión y es publicada La norma ISO/IEC 27001:2013 posee varios cambios significativos y como principales cambios se consideraron los siguientes:

Tabla 1

Resumen de cambios Norma ISO/IEC 27001

ISO 27001 VERSIÓN 2005	ISO 27001 VERSIÓN 2013
Estructura no alineada con otras normas	Estructura alineada con Anexo SL
12 páginas de SGSI	9 páginas de SGSI
Anexo A • 11 Cláusulas • 133 Controles	Anexo A • 14 Cláusulas • 113 Controles
	Anexo A referenciado a ISO 27002:2013
Referencia directa a PDCA	Sin referencia a PDCA
Referencia a principios OECD	No hay referencia a principios OECD

Fuente: (Buges, 18)

Un anexo SL es un documento que define la estructura y formato común que deben tener las normas de sistemas de gestión ISO que logra la homologación de títulos de las cláusulas, secuencias de títulos, texto y definiciones. PDCA, más conocido por circulo Deming que consiste en un proceso de mejora continua, sus siglas hacen referencia a: Planificar, Hacer, Verificar y Actuar que consiste en la aplicación sistemática de 4 pasos, esta es una metodología no referenciada en la última versión de ISO 27001.

2.4.6. Mapeo de Procesos Cobit V5 con la Norma ISO/IEC 27001:2013

Para realizar el presente trabajo de Auditoría Informática orientado a seguridades de la Información se ha utilizado la norma de Seguridades Informáticas actualizada y vigente para el Ecuador siendo esta la norma internacional ISO/IEC 27001:2013. La norma ha sido consultada y obtenida del Instituto Ecuatoriano de Normalización (INEN). El mapeo de la norma para los procesos de COBIT 5 se establece de la siguiente manera, siendo utilizada la guía presentada por ISACA en el documento Mapeo de Cobit 5 con ISO 27001:2013

Tabla 2

Mapeo de COBIT 5 con ISO/IEC 27001:2013

COBIT 5 Seguridad de la Información		ISO/IEC 27001:2013
Evaluar, Orientar y Supervisar		
EDM01	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	5.1 Liderazgo y compromiso 5.2 Política 5.3 Roles, responsabilidades y autoridades organizacionales 6.2 Objetivos de Seguridad de la Información y la planeación para su logro 7.4 Comunicación A.5 Política de Seguridad de Información
EDM02	Asegurar la entrega de beneficios	4.1 Entendiendo a la organización y su contexto 4.2 Entender las necesidades y expectativas de las partes interesadas

Continua

		6.1.1 General 9.3 Revisión Gerencial 10 Mejoramiento
EDM03	Asegurar la Optimización del Riesgo	5.2 Política 6.1 Acciones para abordar los riesgos y las oportunidades 7.5 Información Documentada 8.1 Plan operacional y de control 8.3 Tratamiento al riesgo de seguridad de información 9.1 Monitoreo, medición, análisis y evaluación 9.3 Revisión general
EDM04	Asegurar la optimización de recursos	4.4 Sistema de administración de la seguridad 7.1 Recursos 7.2 Competencia 7.3 Concientización
EDM05	Asegurar la Transparencia hacia las Partes Interesadas	A.12 Operaciones de Seguridad
Alinear, Planificar y Organizar		
APO01	Gestionar el marco de gestión de TI	5 Liderazgo A.5 Política de seguridad de la información A.6 Organización de seguridad de la información
APO02	Gestionar la estrategia	4 Contexto de la organización 5.2 Política 6 Planeación
APO03	Gestionar la Arquitectura Empresarial	
APO04	Gestionar la Innovación	
APO05	Gestionar el Portafolio	
APO06	Gestionar el Presupuesto y los Costes	
APO07	Gestionar los recursos humanos	7.2 Competencia 7.3 Concientización A.7 Seguridad de los Recursos Humanos
APO08	Gestionar las Relaciones	A.6.1 Organización Interna

Continua

APO09	Gestionar Acuerdos de Servicios	
APO10	Gestionar los Proveedores	A.15 Relación con los proveedores
APO11	Gestionar la Calidad	4.1 Entendiendo la organización y su contexto 4.2 Entender las necesidades y expectativas de las partes interesadas 6.1.1 General 9.3 Revisión General 10 Mejoramiento
APO12	Gestionar el Riesgo	5.2 Política 6.1 Acciones para abordar los riesgos y las oportunidades 7.5 Información Documentada 8.1 Plan operacional y de control 8.3 Tratamiento al riesgo de seguridad de la información 9.1 Monitoreo, medición, análisis y evaluación 9.3 Revisión gerencial
APO13	Gestionar la seguridad	Considerado en todo el estándar
Construir, adquirir e implementar		
BAI01	Gestionar Programas y proyectos	
BAI02	Gestionar la definición de requisitos	A.18 Cumplimiento
BAI03	Gestionar la identificación y construcción de soluciones	A.14 Adquisición, desarrollo y mantenimiento de sistemas
BAI04	Gestionar la disponibilidad y la capacidad	A 12.1.3 Administración de capacidad
BAI05	Gestionar la introducción de cambio organizativo	
BAI06	Gestionar los cambios	A 12.1.2 Administración de Cambios
BAI07	Gestionar la aceptación del cambio y la transición	A 12.1.4 Separación de ambientes de desarrollo, pruebas y operaciones
BAI08	Gestionar el	7.5 Información documentada

Continua

	conocimiento	
BAI09	Gestionar los activos	A.8 Administración de los activos
BAI10	Gestionar la configuración	
Entrega, Servicio y Soporte		
DSS01	Gestionar operaciones	6.1 Acciones para abordar los riesgos y oportunidades 8 Operaciones A.11 Seguridad Física y Ambiental A.12.3 Respaldos A.12.4 Monitoreo y Registro A.15 Relación con los proveedores
DSS02	Gestionar Peticiones e Incidentes de Servicio	A.16 Administración de incidentes de seguridad de la información
DSS03	Gestionar Problemas	
DSS04	Gestionar la Continuidad	4.1 Entiendo la organización y su contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 7.5 Información documentada 10 Mejoramiento
DSS05	Gestionar Servicios de Seguridad	Considerado en todo el estándar
DSS06	Gestionar controles de procesos de negocio	6.1.2 Evaluación de riesgo de seguridad de la información 9 Evaluación del rendimiento A.8.2 Clasificación de la información A.9.4 Control de Acceso a los sistemas y aplicaciones
Supervisar, Evaluar y Valorar		
MEA01	Supervisar, evaluar y valorar el rendimiento y la conformidad	4.1 Entendiendo la organización y su contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 9 Evaluación del rendimiento
MEA02	Supervisar, evaluar y valorar el sistema de control interno	4.1 Entendiendo la organización y su contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 9 Evaluación del Rendimiento A.18.2 Revisiones de seguridad de la información
MEA03	Supervisar, evaluar y	4.1 Entendiendo la organización y su

Continua

	valorar la conformidad con los requerimientos externos	contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 9 Evaluación del Rendimiento A.18.1 Cumplimiento con requerimientos legales y contractuales

Fuente: (Meryk, 2014)

Como parte de la actividad de este proyecto, se debe verificar la existencia de normas, políticas, planes, reglamentos internos, etc. que se apeguen a la norma ISO/IEC: 27001, con el fin de salvaguardar la información con regulación y controles que permitan medir su eficacia y eficiencia.

2.5. Cobit V5 para el Aseguramiento

2.5.1. Introducción

COBIT 5 for Assurance o traducido al idioma Español, *COBIT 5 para Aseguramiento* es un producto de la familia de COBIT, que sirve como una guía para profesionales de COBIT 5. Está basado en el marco de COBIT 5 y posee un enfoque orientado al apoyo de actividades que permitan la contribución del aseguramiento de las TI. Mediante esta guía se orienta al establecimiento eficaz y eficiente de las iniciativas que involucran aseguramiento. Es una guía que orienta una planificación eficiente, un estudio profundo, una ejecución eficaz y un seguimiento controlado de las actividades de aseguramiento.

Todo lo nombrado anteriormente se logra mediante la implementación de una hoja de ruta que contiene enfoques de aseguramiento aceptados. Los motivos que promueven la creación de este producto son varios, tomando en cuenta que se toma en consideración diferentes puntos de vista. Demostrar que las iniciativas de aseguramiento se encuentran involucradas y en línea con los objetivos de la empresa es uno de sus objetivos y garantizar el cumplimiento de normativas y contratos.

Este producto permite a los auditores tener un mejor entendimiento de las responsabilidades y roles que se vinculan a la provisión de aseguramiento. Además le permitirán tener un enfoque exhaustivo, correctamente ilustrado y estructurado en función de aseguramiento. COBIT 5 para el Aseguramiento trabaja sobre los siete catalizadores de COBIT 5. El ambiente en que se implemente y como se usen los catalizadores en cada empresa entregarán un resultado específico relacionado al tema de aseguramiento, procurando que sea el óptimo esperado.

2.5.2. Aseguramiento

Aseguramiento implica una revisión de conformidades en relación de responsabilidad de las partes a través de una persona capacitada para la realización de auditorías de las TI y de Aseguramiento. Está relacionado con diversas actividades que permiten emitir un informe sobre el tema en referencia, para este caso el tema de aseguramiento, el cual debe brindar tranquilidad a los lectores.

Son varios aspectos que se toman en cuenta para la elaboración de estos informes de aseguramiento que pueden incluir desde la intromisión en ámbitos financieros por temas de inversión de TI versus aporte hacia la empresa. También la realización de revisiones que permitan determinar que se cumple con los controles establecidos, cumplimiento de normas, estándares, acuerdos, licencias, legislación, entre otros. ISACA, en su artículo técnico de COBIT 5 para el Aseguramiento señala sobre la definición de cinco componentes clave para trabajar sobre el tema de aseguramiento, tal como lo podemos observar en la figura 22

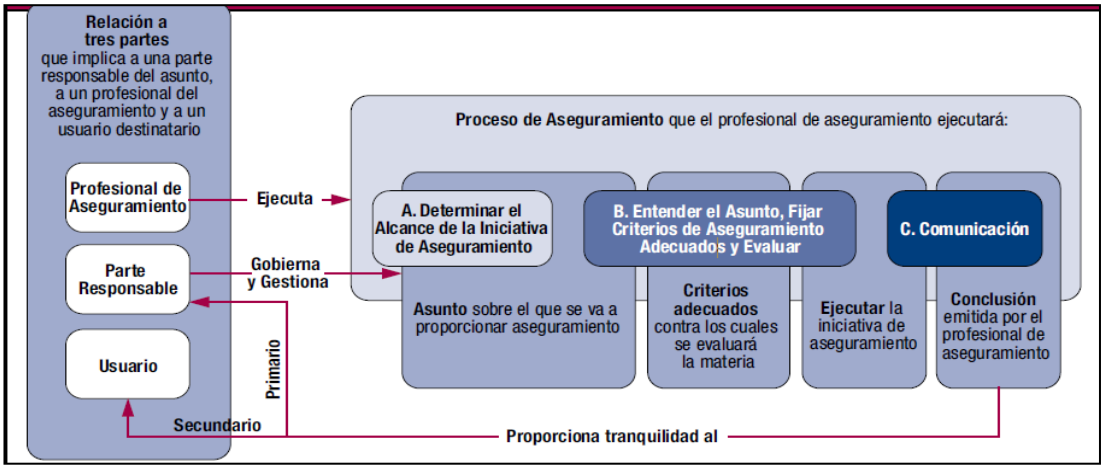


Figura 22: Componentes de Aseguramiento

Fuente: (ISACA)

De acuerdo a la figura indicada anteriormente se tiene que un trabajo de aseguramiento se compone de la relación de partes, del asunto, de criterios, ejecución y exposición de conclusiones. La relación de las partes implica la responsabilidad que recae sobre los profesionales de aseguramiento, la parte responsable que es sometida a la auditoría y el usuario que indirectamente es auditado.

La relación para establecer el resultado de este componente puede verse reflejado en la declaración de acuerdos contractuales o de legislación, así como también tiene que ver con la responsabilidad que se tiene frente a los asuntos estipulados, es decir cuando una de las partes tiene responsabilidades frente a otra, como en casos generales la parte auditada con el usuario.

El asunto mencionado en el anterior párrafo corresponde a otro componente del aseguramiento que según el artículo de ISACA lo define de la siguiente manera:

> Es la información, prácticas o controles específicos, como cualquiera de los siete catalizadores de COBIT 5, que son objeto de una revisión por parte de un profesional de auditoría o aseguramiento. Este asunto puede incluir el diseño o la operación de controles internos y prácticas

> de gestión sobre cualquier aspecto de la empresa, o el cumplimiento con prácticas de privacidad, o estándares, o leyes y normas específicas. (ISACA)

Los criterios adecuados, se relacionan a los estándares debido a que permiten medir y presentar el asunto. Por esta razón los criterios deben reunir algunas características que se mencionan a continuación, para ser considerados criterios adecuados. Los criterios que se utilicen deben ser objetivos, deben ser medibles en cuanto a consistencias, calidad y cantidad. Deben ser comprensibles, es decir, su comunicación no debe ser ambigua y deben estar presentados en forma clara.

Además deben de ser muy exhaustivos, sin dejar aspectos por fueran que afecten de una manera significativa la conclusión y/o resultados acerca de un tema o asunto específico. También deberán ser relevantes tomando en cuenta el grado de interés e importancia para el tema en cuestión. Otro de los componentes de aseguramiento es la ejecución, que deberá poseer un enfoque estructurado. Deberá estar enfocado con los catalizadores ya que de esta manera se podrá obtener una valoración más acertada y cercana a los asuntos propuestos.

Un último componente de aseguramiento, está definido como las conclusiones. Cabe recalcar que el proceso de auditorías para llegar hasta la parte de conclusiones y recomendaciones, puede llegar a ser complicado. El profesional de auditoría debe seguir los pasos adecuadamente a fin de que pueda confirmar los hechos clave con las personas responsables que están involucradas en el proceso de auditoría hasta la determinación de las consideradas causas fundamentales.

Un auditor debe tener una completa comprensión del entorno empresarial. Relacionar el impacto tanto de cuestiones como resultados en los objetivos estratégicos de la organización, comunicando aquellas percepciones que agreguen valor a la misma. La dirección de las empresas por lo general no se interesan en las observaciones de los hallazgos, lo que

realmente les interesa y les preocupa es como estas afectan al valor del negocio detrás de los resultados obtenidos.

2.5.3. Perspectivas de Aseguramiento

Aseguramiento se encuentra enfocado hacia dos perspectivas en COBIT 5, tal como se muestra en la figura 23.

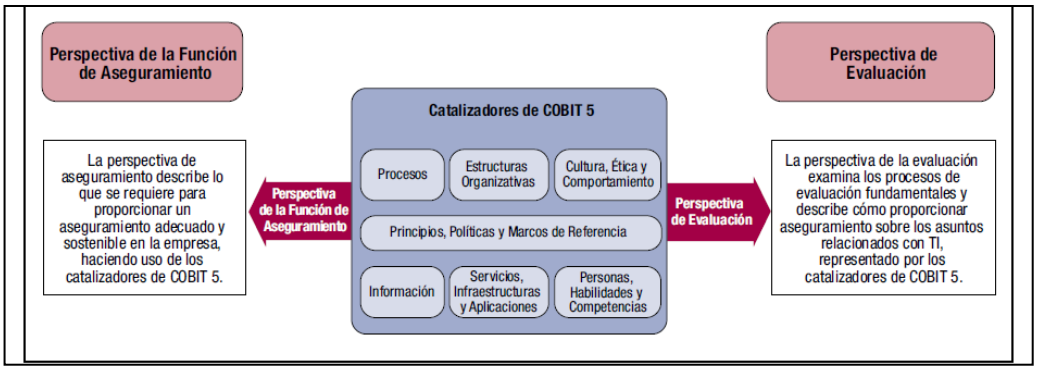


Figura 23: Perspectivas de Aseguramiento de Cobit V5

Fuente: (ISACA)

2.5.3.1. Perspectivas de la Función de Aseguramiento

Esta función permite que las organizaciones establezcan cuáles son sus necesidades para contribuir a la creación y promoción de las respectivas funciones de aseguramiento. Establece que organizaciones están involucradas para la provisión de aseguramiento, así como también la determinación de información clave que es requerida para la provisión de esta función.

2.5.3.2. Perspectiva de Evaluación

Esta perspectiva se encuentra vinculada con el objeto de aseguramiento. Consiste en cómo se encuentran interconectados y su comportamiento en conjunto de los catalizadores a fin de que generen o promuevan un acercamiento de aseguramiento sobre los catalizadores.

2.5.4. Principios para Proporcionar Aseguramiento

Los principios que se establecen para proporcionar aseguramiento son los mismos que plantea COBIT 5 de la figura 3. A continuación se realiza una breve descripción de como se puede proporcionar aseguramiento sobre estos 5 principios bases de COBIT 5.

2.5.4.1. Satisfacer Necesidades de las Partes Interesadas

Las partes interesadas se describe en dos grupos claramente identificados, estas partes interesadas pueden ser internas (comisión de auditoría y Consejos de Administración, grupos específicos de auditoría, riesgos y cumplimiento, también ejecutivos de negocio y además también se encuentran involucrados los responsables de negocio)

El otro grupo identificado es el externo (accionistas, inversionistas, auditores externos, reguladores y además clientes). Es importante hacer esta diferenciación ya que dependiendo del grupo de interesados se podrá determinar de manera correcta los encargos de aseguramiento en los que estarán interviniendo.

Las actividades que permiten dar cumplimiento y seguimiento al aseguramiento, se encuentran señaladas en tres categorías como lo indica la publicación de ISACA, COBIT 5 para el Aseguramiento. Auto-Evaluaciones, permite la definición de los criterios de evaluación y la ejecución de las tareas de evaluación. Permite determinar el cumplimiento de guías existentes que trazan el camino de la empresa.

Revisión de Auditoría Interna/Cumplimiento, estas actividades son llevadas a cabo por terceros, aquellos que no están directamente en el funcionamiento de los catalizadores, pero que al mismo tiempo pertenecen a la empresa. Puede llegar a tratarse de una unidad, departamento o persona que dependerá del tamaño de la organización y que se encarga de la evaluación de cumplimiento y de la revisión de las actividades de desarrollo.

Al no estar involucrado en el funcionamiento de los catalizadores este encargo de aseguramiento posee mayor credibilidad que el anterior frente a resultados, sin embargo, es necesario manejar un grupo consistente de guías y buenas prácticas. Auditoría Externa, se trata de las mismas actividades que la Auditoría interna, en lo que se diferencia es que el equipo de trabajo que lo lleva a cargo es un ente externo de la organización, el cual debe ser regulado.

2.5.4.2. Cubrir la Empresa de Extremo a Extremo

Su razón debe ser consiste en dar a la información un tratamiento igual de cuidadoso como cualquier otro activo de la empresa, para cumplir una función de aseguramiento define que deben ser consideradas las partes interesadas desde el alcance hasta su ejecución. Para ello se considera la aplicación de aseguramiento no solo a catalizadores, sino además se extiende a partes interesadas, funciones y procesos que pueden ser considerados relevantes en la empresa.

2.5.4.3. Aplicar una Marco de Referencia Único Integrado

Hablando más específicamente se puede señalar que COBIT 5 para el aseguramiento reúne conocimiento y experiencia de los diferentes marcos publicados por ISACA, entre ellos BMIS, ValIT y RiskIT quienes están vinculados a los principales estándares relacionados a aseguramiento.

2.5.4.4. Hacer Posible un Enfoque Holístico

Los mismos siete catalizadores definidos por COBIT 5 son aplicables para la promoción de aseguramiento que contribuye a respaldar el cumplimiento establecido para el alcance de metas de la organización cubriendo el todo de la empresa desde las diferentes perspectivas que define COBIT 5.

2.5.4.5. Separa el Gobierno de la Gestión

El gobierno como tal se asegura de la evaluación de necesidades, condiciones que permiten valorar el alcance equilibrado y acordado para las metas corporativas. Se encuentra vinculado el gobierno a un consejo de administración, que a su vez es quien define las funciones de auditoría. Por otro lado se había mencionado anteriormente que la gestión es la función donde se encarga de planificar, construir, ejecutar y controlar aquellas actividades que deben estar alineadas con la dirección en la búsqueda de alcanzar con el cumplimiento de las metas corporativas.

2.5.5. Catalizadores desde la Perspectiva de Aseguramiento

2.5.5.1. Principios, políticas y Marcos de Referencia

El objetivo en este catalizador es dar a conocer de manera general los principios, políticas y marcos de referencia que proveen aseguramiento. Se puede indicar que gracias al trabajo y experiencia de años anteriores ISACA tiene un marco conocido como ITAF que es lo suficientemente robusto en normas y políticas, considerando una estructura apropiada, a la vez que puede ser sustentado en otros estándares siempre que fuere necesario.

A continuación en la Tabla 3, se presenta una serie de Principios, políticas y marcos de referencia que según ITAF podemos aplicar en este catalizador para proveer aseguramiento:

Tabla 3

Principios, Políticas y Marcos de Referencia Tratados por ITAF

Principios, Políticas y Área de Trabajo	Cubierto por:
Código de Ética Profesional	ITAF, 2da. Edición, Sección 1
Estándares Generales	1001 Estatuto de la Función de Auditoría
	1002 Independencia Organizativa
	1003 Independencia Profesional

Continua

	1004 Expectativa Razonable
	1005 Debido Cuidado Profesional
	1006 Competencia
	1007 Declaraciones de la Dirección
	1008 Criterios
Estándares de Rendimiento	1201 Planificación de los Trabajos
	1202 Gestión de Riesgos en la Planificación de Auditoría
	1203 Rendimiento y Supervisión
	1204 Materialidad de Auditoría
	1205 Evidencia de Auditoría
	1206 Utilización del Trabajo de otros Expertos
	1207 Irregularidades y Actos Ilegales
Estándares sobre Informes	1401 Informes
	1402 Actividades de Seguimiento

Fuente: (ISACA)

2.5.5.2. Procesos

Lo que se hace a través de este catalizador y por medio de esta guía es proporcionar una identificación de procesos considerados como necesarios para la construcción y mantenimiento de aseguramiento de una manera tanto eficaz como efectiva. La información con respecto a los procesos no se encontraría completa si esta no describe al menos: metas, métricas y descripción detallada del proceso. De la figura 23, ISACA describe todos los dominios de COBIT 5 con sus respectivos procesos, existen procesos que se encuentran remarcados en un color vino fuerte, estos procesos se identifican como necesarios para el aseguramiento.

Figura 24: Procesos de COBIT 5 que Apoyan Aseguramiento

Fuente: (ISACA)

En la tabla 4, que se presentará a continuación se realizará el detalle de los procesos de apoyo clave, que permiten proveer aseguramiento a las entidades en general.

Tabla 4

Procesos Clave de Apoyo a la Provisión de Aseguramiento

Identificación del Proceso	Razonamiento	Resultados específicos de Aseguramiento
EDM01 Asegurar el establecimiento y mantenimiento del marco de gobierno	La función de aseguramiento requiere el establecimiento de una estructura de gobierno	• Requisitos de las partes interesadas en relación con el gobierno del aseguramiento • Principios rectores de aseguramiento • Mandato para la función de aseguramiento y la comisión de auditoría • Documentación formal de las decisiones de aseguramiento • Actas formales de las reuniones de gestión del aseguramiento

Continua

EDM02	Asegurar la entrega de beneficios	La empresa debe cerciorarse de que la función de aseguramiento genera valor	• Documentación formal de los requisitos de las partes interesadas • Documentación formal de la contribución de la función de aseguramiento a los objetivos de negocio • Comentarios sobre la entrega de las iniciativas de aseguramiento
EDM03	Asegurar la optimización del riesgo	La empresa debe cerciorarse de que el riesgo relacionado con aseguramiento está gestionado	• Medidas correctivas para hacer frente a las desviaciones de aseguramiento indicadas
EDM05	Asegurar la transparencia hacia las partes interesadas	La función de aseguramiento es un proveedor importante de las partes interesadas	• Evaluación de los requisitos de los informes de aseguramiento • Resumen de actividades de aseguramiento de la Comisión de Auditoría
APO02	Gestionar la estrategia	La función de aseguramiento debe desarrollar una estrategia para proporcionar aseguramiento. La estrategia debe estar alineada con la estrategia de negocio.	• Lista de posibles disparidades de cobertura en la función de aseguramiento • Capacidades de la función de aseguramiento • Criterios para la priorización de las disparidades en la cobertura de aseguramiento • Requisitos de la función de aseguramiento en las capacidades esperadas de TI • Deficiencia de la función de aseguramiento que se quieren cerrar • Comparativa de capacidades de la función de aseguramiento • Plan estratégico de Aseguramiento Plan Anual de la función aseguramiento
APO06	Gestionar el presupuesto y los costes	La función de aseguramiento debe presupuestar sus actividades y las de	• Priorización de actividades de aseguramiento • Presupuesto de la función de aseguramiento

Continua

		sus sistemas de soporte	
APO07	Gestionar los Recursos Humanos	La función de aseguramiento requiere la cantidad adecuada de personas y habilidades	• Requisitos de la función de aseguramiento para el proceso de gestión personal • Plan de formación de la función de aseguramiento • Evaluación del personal de la función de aseguramiento. • Plan de seguimiento del rendimiento de los recursos e indicadores, plan de asignación de recursos
APO08	Gestionar las relaciones	La relación entre la función de aseguramiento y el negocio es crítica	• Conocimiento de los procesos de negocio de la empresa • Estrategia para obtener el compromiso de las partes interesadas • Estrategia de comunicación de aseguramiento • Planes de acción de aseguramiento para el negocio
APO11	Gestionar la calidad	La mejora de la calidad es un componente esencial en la provisión efectiva de aseguramiento	• Estándares y buenas prácticas relacionadas con el aseguramiento • Estándares de calidad de la función de aseguramiento • Métricas de calidad consensuadas sobre la función de aseguramiento • Resultados de las revisiones externas de calidad de la función de aseguramiento • Métricas de calidad de la función de aseguramiento implementadas de acuerdo con las buenas prácticas de la industria. • Causas raíz documentadas responsables de problemas de aseguramiento con las métricas de calidad

Continua

APO12	Gestionar el riesgo	El riesgo de aseguramiento (riesgo de auditoría) debe ser gestionado	• Datos para el análisis del riesgo de aseguramiento • Resultados del análisis del riesgo de la función de aseguramiento • Perfil de riesgo empresarial que incluye aspectos relacionados con el aseguramiento • Evaluación de riesgos y estrategias de valoración • Perfil de riesgo empresarial actualizado
BAI08	Gestionar el conocimiento	La función de aseguramiento debe ser proporcionada con el conocimiento requerido para apoyar al personal de aseguramiento en sus actividades laborales	• Clasificación actualizada de la información de la función de aseguramiento • Repositorios de conocimiento publicados • Control de acceso actualizado sobre la información de aseguramiento • Reglas actualizadas para la eliminación de información de aseguramiento.

Fuente: (ISACA)

A continuación se presentará la tabla 5 que maneja e indica los procesos adicionales de COBIT 5 en los que se requiere también involucrar aseguramiento

Tabla 5

Otros procesos de COBIT 5 para aseguramiento

Identificación del Proceso		Razonamiento
EDM04	Asegurar la optimización de recursos	Esto se contempla gestionando la optimización de recursos en la función de aseguramiento
APO01	Gestionar el marco de gestión de TI	El marco de gestión de TI en la función de aseguramiento debe ser gestionado

Continua

APO03	Gestionar la arquitectura empresarial	La función de aseguramiento debería seguir la arquitectura empresarial global y usar la arquitectura empresarial como una fuente principal de información.
APO04	Gestionar la innovación	La innovación debe ser gestionada en la función de aseguramiento, p. ej. La función de aseguramiento no solamente debería mantenerse al corriente de las nuevas tecnologías, sino que también debería aprovecharse de la tecnología y herramientas emergentes para mejorar su eficiencia y efectividad.
APO05	Gestionar portafolio	El portafolio de aseguramiento de sistemas debe ser gestionado y considerado como una fuente principal de información
APO09	Gestionar los acuerdos de servicio	La función de aseguramiento puede usar proveedores de servicios (internos o externos), p.ej. Una función mixta de aseguramiento TI
APO10	Gestionar Proveedores	La función de aseguramiento puede usar proveedores de servicios (internos o externos), p.ej. Una función mixta de aseguramiento TI
APO13	Gestionar la Seguridad	La función de aseguramiento tiene requerimientos de seguridad que necesitan ser gestionados
BAI01	Gestionar los programas y proyectos	Deben implantarse nuevas herramientas y software de aseguramiento
BAI02	Gestionar la definición de requisitos	Deben desarrollarse requisitos para el nuevo software de aseguramiento
BAI03	Gestionar la identificación y construcción de soluciones	El nuevo software de aseguramiento necesitará la identificación y construcción de soluciones

Continua

BAI04	Gestionar la disponibilidad y capacidad	Debe gestionarse la disponibilidad y capacidad del software de aseguramiento
BAI05	Gestionar la introducción de cambios organizativos	El nuevo software de aseguramiento necesitará gestión de cambios
BAI06	Gestionar los cambios	El software de aseguramiento necesitará un proceso definido de cambios.
BAI07	Gestionar la aceptación de cambio y la transición	El software de aseguramiento necesita un proceso definido de aceptación de usuario
BAI09	Gestionar los activos	La función de aseguramiento debe gestionar sus activos de TI
BAI10	Gestionar la configuración	La función de aseguramiento debe gestionar la configuración de TI
DSS01	Gestionar las operaciones	La función de aseguramiento debe gestionar las operación de sus activos de TI
DSS02	Gestionar las peticiones y los incidentes de servicio	La función de aseguramiento debe gestionar las peticiones de servicio e incidentes para sus activos de TI
DSS03	Gestionar los problemas	La función de aseguramiento debe gestionar problemas para sus activos de TI
DSS04	Gestionar la continuidad	La función de aseguramiento debe gestionar su propia continuidad de negocio
DSS05	Gestionar los servicios de seguridad	La función de aseguramiento debe gestionar la seguridad para sus activos de TI
DSS06	Gestionar los controles de los procesos del negocio	La función de aseguramiento debe gestionar los controles de procesos del negocio para sus activos de TI

Fuente: (ISACA)

2.5.5.3. Estructuras Organizativas

Construir y sostener las iniciativas es la función de las estructuras organizativas en el enfoque de aseguramiento que debe caracterizarse por ser efectivo y eficiente. A continuación en la figura 25, se listarán y detallarán las principales estructuras organizativas que apoyan y dan soporte a la promoción de aseguramiento según la publicación de ISACA, COBIT 5 para el Aseguramiento.

Estructura	Definición/Descripción
Consejo de Administración/Comisión de Auditoría	El cuerpo de gobierno que tiene la responsabilidad de evaluar, dirigir y supervisar las funciones de auditoría, gestión del riesgo y control de la organización. El consejo (o la función equivalente a cargo del gobierno de la empresa) a menudo delega la responsabilidad de proveer aseguramiento a la comisión de auditoría, cuyos miembros a menudo se reclutan del Consejo de Administración (miembros no ejecutivos). La responsabilidad final, sin embargo, permanece en el Consejo.
Departamento de auditoría	La función que es responsable en la empresa de la provisión de auditoría interna en la empresa.
Departamento de cumplimiento •Regulatorio •Interno	• **Regulatorio**—La función en la empresa responsable de la orientación sobre los requerimientos legales, regulatorios y estatutarios, y del cumplimiento contractual • **Interno**—El grupo responsable de verificar el cumplimiento con las políticas y estándares de la organización
Auditoría externa	La función responsable de la provisión de autoría externa y servicios asociados

Figura 25: Estructuras Organizativas de Apoyo al Aseguramiento

Fuente: (ISACA)

2.5.5.4. Cultura, Ética y Comportamiento

El propósito de este catalizador es el de influenciar de manera positiva en los comportamientos relevantes que dan apoyo a la función de aseguramiento. Una de las unidades de aseguramiento es la auditoría interna, que debe tener ciertos comportamientos y elementos culturales que afirmen el aseguramiento del gobierno de TI como de seguridad de la información verificando que cumpla con la construcción y el apoyo efectivo y eficiente en el aseguramiento de las organizaciones.

2.5.5.5. Información

En este catalizador se debe identificar todos los elementos de información necesarios para el diseño y la construcción de una función de aseguramiento efectivo dentro de la organización. Esta información necesaria debe estar reflejada en la existencia de documentos claramente definidos como por ejemplo: Buenas Prácticas y regulaciones, Registro de hallazgos, Estándares de calidad, Plan de auditoría, planes de cumplimiento, planes de inversiones, gestión del riesgos, gestión de las TI, gestión de las seguridades de la información, entre otros que deben ser desarrollados y documentados según la necesidad de la empresa.

Es necesario considerar que información de entrada es importante para soportar las funciones de aseguramiento. Existe información documentada que la empresa debe poseer y esta debe estar de forma clara, completa y actualizada. El plan estratégico del negocio, Plan estratégico de TI, Plan de Riesgos, Plan de inversiones, Registro del seguimiento de los planes y resultados. Esta información se constituye en la plataforma para un diseño de gobierno tecnológico que apoye las estrategias de negocio y son elementos esenciales para partir.

2.5.5.6. Servicios, Infraestructuras y Aplicaciones

De acuerdo a la perspectiva de aprovisionamiento del presente catalizador, busca identificar y tratar con todos los servicios, infraestructuras y aplicaciones que permitan el diseño, mejoramiento y soporte de la empresa en el ámbito tecnológico

Cobit 5 para el aseguramiento determina los servicios que se relacionan directamente con TI a los cuales se debe poner atención como son: Información y comunicación, aseguramiento de la calidad y el registro de notificación y tiempos, capacidad para evaluar la necesidad, identificación y adquisición de recursos, servicio para el acceso eficaz a la información, existencia de programas que apoyen el seguimiento de leyes y sus

regulaciones, servicios de alerta ante riesgos emergentes y programas para la evaluación de rendimiento.

Existen algunos requerimientos de aplicaciones que dan soporte a la función de aseguramiento como: Un repositorio del modelo de riesgos, una herramienta de técnicas de auditoría asistida por ordenadores, registro de los hallazgos de auditorías anteriores, herramientas para una gestión documental, herramientas de planificación, sistemas para el registro de incidencias TI, entre otras recomendadas por Cobit 5 descritas en el producto COBIT 5 para el Aseguramiento.

2.5.5.7. Personas, Habilidades y Competencias

Aseguramiento requiere identificar y tratar con un conjunto de habilidades y competencias que permitan diseñar, implementar y sostener una adecuada función de aprovisionamiento por lo que se requiere ciertas destrezas como lo explica COBIT 5 para el aseguramiento en este catalizador. Se debe contar con habilidades y competencias para: estrategia y planificación, gestión para el compromiso de recursos, Evaluación y pruebas, Gestión del riesgo, gestión de las relaciones, prácticas de auditoría, Análisis, gestión de proyectos, conceptos básicos de TI, resiliencia y experiencia técnica muy específica para la función, entre otras habilidades y competencias que se resaltan como necesarias para la función.

Es necesario que exista la definición de cada rol para poder determinar de una manera efectiva el nivel de habilidad que requiere la empresa, donde cada rol debe tener definido al menos una descripción de la habilidad deseada, experiencia, educación y cualificaciones requeridas junto con el conocimiento y habilidades tanto técnicas como las de comportamiento relacionado.

CAPITULO 3

ESTUDIO ACTUAL

3.1. Caracterización Preliminar

3.1.1. La Empresa

Cocinas Internacionales bajo la razón social Modulares Iván Ron Egas Cia. Ltda. (MIRE Cia. Ltda.) Se establece el año de 1995, su Gerente General Ing. Iván Ron Egas apertura su propia empresa logrando permanecer en el mercado cerca de 20 años. Actualmente la institución cuenta con 141 empleados, distribuidos de la siguiente manera: 74 empleados en planta, 60 empleados en instalación y 7 empleados para las áreas administrativas.

Cocinas Internacionales, se encuentra ubicada en Quito, sector de la Ofelia en las calles Juncal N65-130 y Los Eucaliptos, en donde realiza actividades de: comercialización de sus productos, recepción de órdenes de producción para elaboración de muebles modulares y envío de las distintas obras de los pedidos, cabe indicar que la empresa cuenta con transporte propio para la entrega de sus pedidos. Además posee un almacén para ventas al público ubicado en la Av. Republica y Alemania (esquina), en este lugar se exhibe los productos y también se realiza las diferentes órdenes de producción que son enviadas a fábrica.

3.1.2. Naturaleza de la empresa

La industria de la carpintería y del mobiliario de madera, es una de las actividades más antiguas de la humanidad, con el transcurrir de los tiempos ha ido evolucionando con el avance industrial y con el recurso de la materias disponibles durante las diferentes épocas. El desarrollo de este sector depende en gran medida de la situación económica y, está muy relacionado con el conocimiento y disponibilidad de las tecnologías de proceso y

producto, el diseño, la promoción comercial, la cooperación empresarial, las materias primas disponibles y los suministros complementarios.

El crecimiento del sector del mueble se asienta en la demanda, determinada por movimientos cíclicos en función de la saturación del mercado, de la situación económica en general de los países de la zona y, muy particularmente, de la evolución de los ingresos domésticos y de la coyuntura del sector de la construcción. Se puede considerar al mueble tanto un bien de inversión para hogares y empresas, como un artículo de consumo, sensible en parte a los efectos de la moda y/o ser un bien caracterizado por un alto precio y una prolongada vida.

La rápida evolución del sector ha sido posible en las últimas décadas gracias a la aparición en el mercado de productos homogéneos y normalizados, los conocidos tableros derivados de madera, que han hecho posible incorporar a este sector los procesos de fabricación en cadena, la automatización, la disminución de los costes de producción y la racionalización en el trabajo. Cocinas Internacionales es una industria manufacturera dedicada a la producción, comercialización e instalación de muebles modulares1, siendo básicamente su materia prima los tableros aglomerados y tableros de Fibraplac o MDF y en ciertas ocasiones madera sólida.

3.1.3. Productos

Cocinas Internacionales comercializa una gran variedad de muebles, modelos y diseños que se acomodan a los gustos de los consumidores entre ellos:

- Muebles de Cocina
- Baños
- Puertas de Paso

1 Pieza o conjunto de piezas que se repiten en una construcción

- Clósets
- Muebles Especiales

3.1.4. Organización Interna

La distribución de personal de la empresa Cocinas Internacionales se constituye de la manera en la que se encuentra descrita en la Tabla 6.

Tabla 6

Distribución de Personal

Área		Personal	Total
Administrativo			**8**
	Gerente	1	
	Asistente Gerencia	1	
	Contador (Externo)	1	
	Diseñador	1	
	Jefe de Personal	1	
	Jefe de Planta	1	
	Jefe de Despachos	1	
	Asistente de contabilidad	1	
Planta			**93**
	Instalación	**60**	
	Supervisores	2	
	Personal	31	
Total			**101**

Fuente: (Cocinas Internacionales, 2005)

3.1.5. Organigrama Institucional

En la figura 26, se muestra la estructura organizacional de la empresa facilitado por la empresa que aunque no está definido formalmente este es esquema estructural que maneja actualmente la organización para ejecutar sus actividades de negocio.

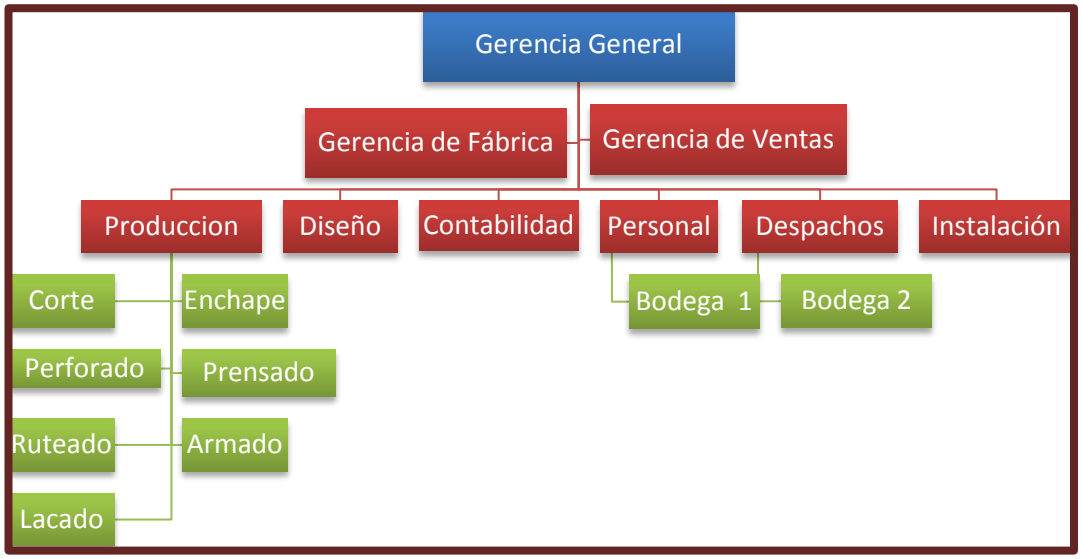


Figura 26: Organigrama de MIRE Cia. Ltda.
Fuente: (Cocinas Internacionales, 2005)

3.1.6. Filosofía Corporativa

La filosofía corporativa de MIRE Cia. Ltda., se encuentra constituida por valores, principios, creencias, misión y visión de la empresa, los mismos que se encuentran evidenciados en la documentación que es propiedad de la misma.

Tabla 7

Valores Corporativos de MIRE Cia. Ltda

VALORES	
Honestidad	En el trato con los clientes, con los proveedores y con todo el personal que trabaja directa o indirectamente en la empresa.
Fe	Para fortalecer la cultura de la empresa. "El trabajador se siente satisfecho de su trabajo pues participa también de esta ilusión y de este esfuerzo colectivo por conseguir la misión de la empresa"[2].

Continua

[2] VIETMA José María. La Excelencia Empresarial. McGraw Hill. 2da. edición. España. 1992, Pág. 323

Seriedad	Desde que el cliente ingresa a la empresa hasta que la operación de venta se ha cerrado.
Lealtad	Para con la empresa y en el cumplimiento con los clientes.
Responsabilidad	En cada una de las tareas encomendadas para beneficio de todos.

Fuente: (Cocinas Internacionales, 2005)

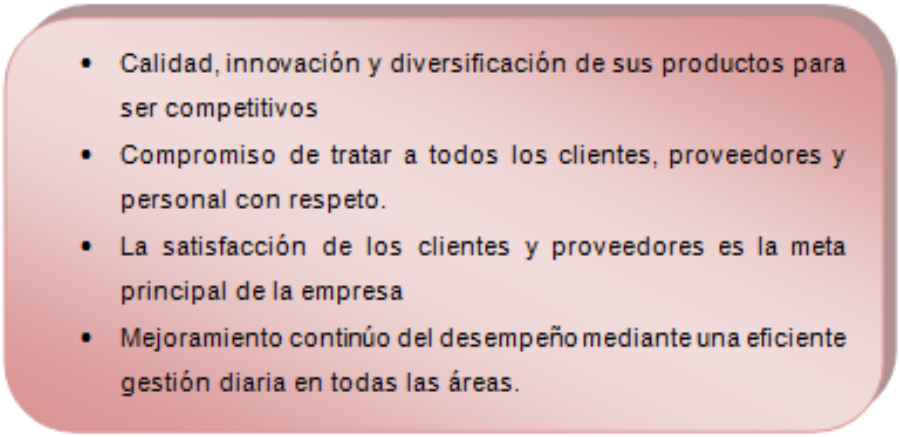


Figura 27: Principios de MIRE Cia. Ltda.

Fuente: (Cocinas Internacionales, 2005)

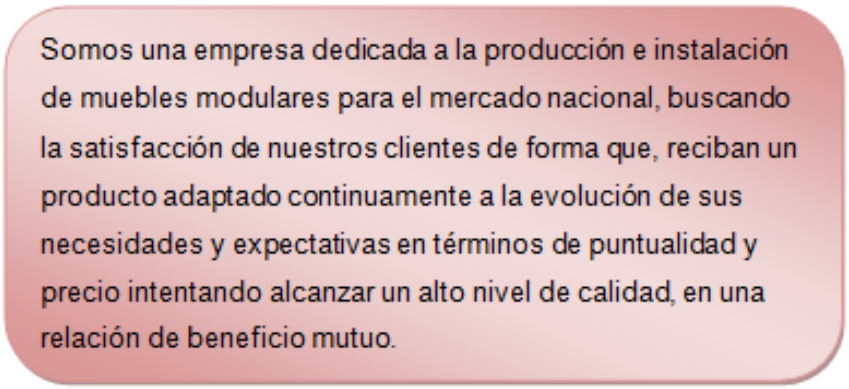


Figura 28: Misión

Fuente: (Cocinas Internacionales, 2005)

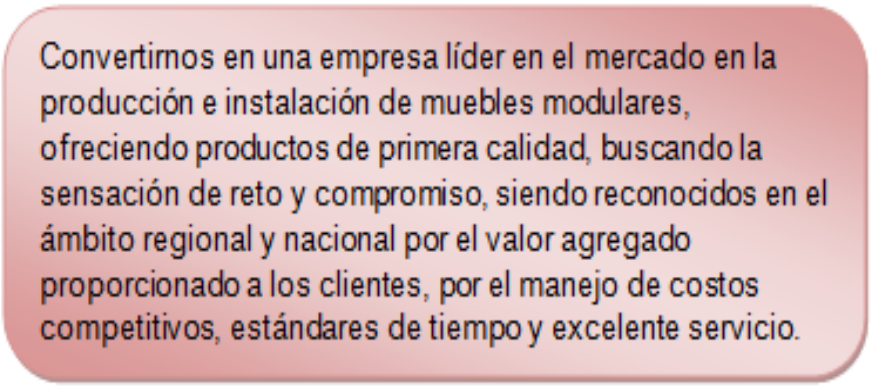


Figura 29: Visión

Fuente: **(Cocinas Internacionales, 2005)**

3.2. Estudio de la Situación Actual del Área Informática

Cocinas Internacionales no dispone de un área específica de informática, es una PYMES (Pequeña y Mediana Empresa), que puede ser considerada una empresa de tamaño mediano, la cual tiene limitaciones de orden tanto ocupacional como financiero.

Como PYMES tiene una gran desventaja en el ámbito tecnológico debido a que por el volumen de beneficios que percibe la empresa no llegan a ser los suficientes para dedicar fondos que estén enteramente enfocados a las TI y la gestión de sus seguridades. De acuerdo al organigrama institucional se puede evidenciar claramente que no se tiene contemplado ni definido un área o departamento que se encuentre a cargo de las TI de la empresa su gestión y seguridad.

3.3. Conocimiento y comprensión de las actividades TI

Cocinas Internacionales pese a no tener definido un departamento de tecnología, maneja recursos informáticos a través de los cuales se procesa información pertinente al negocio, lo que convierte a los recursos informáticos en centros de información.

Las TI se encuentran implícitas de manera informal en las actividades de cada empleado del área administrativa, puesto que realizan varias actividades de donde dependen del activo informático para poder ejecutar las tareas que tienen asignadas. Cocinas Internacionales maneja dos Sistemas de información: uno dedicado al área de Contabilidad y otro dedicado al área de diseño y producción de bienes.

Adicional cuenta con el servicio de una página web, donde se coloca información únicamente de carácter publicitario e informativo de la empresa. Las tecnologías de la información de la empresa cumplen con un rol muy importante para mantener operativo el negocio, permiten que los productos de la empresa se mantengan a la vanguardia con la finalidad de satisfacer a los clientes, así como también son una importante herramienta para la gestión administrativa.

La divulgación responsable de información y almacenamiento, no se encuentra normado ni registrado bajo ninguna política para el uso de los recursos tecnológicos, así como tampoco se tiene definida una cultura de la responsabilidad de manejo del recurso informático. El respaldo de la información que se realizada no posee criterios claros para la creación de respaldos según el área que se requiere, lo que podría suponer un riesgo alto en la conservación de la información.

No cuentan con el personal capacitado para la gestión tecnológica, así como para la gestión de la seguridad de la información. No se tiene definido controles que permitan la supervisión del rendimiento que permitan establecer un criterio detallado de las deficiencias y vulnerabilidades que podría poseer la empresa dentro de todas las operaciones del negocio en el entorno de seguridad de la información. TI, apoya las unidades de gerencia, asistencia de gerencia general, gerencia de ventas, diseño, producción, recepción, órdenes de producción, contabilidad, recursos humanos, publicidad, administración y ventas, pero su arquitectura no tiene una

definición formal establecida por lo que la evaluación de rendimiento es imprecisa.

3.4. Alcance de la Auditoría Informática

El presente trabajo de auditoría está delimitado a la evaluación de controles en los diferentes procesos seleccionados que se constituyeron en procesos de riesgos altos por tener un efecto de alto impacto sobre las operaciones de la empresa basados, los cuales han sido obtenidos desde el producto de Isaca, Cobit 5 para la seguridad de la Información, que se considera un elemento de trabajo extendido de COBIT 5.

Esta auditoría tiene como alcance los procesos seleccionados, se centra además en la evaluación de la información relativa a seguridad de la información, considerando que se cumplan con los requisitos mínimos que deben cumplir cada catalizador o elemento con el que se interactúa de una forma holística de las TI para la seguridad de la información.

Por lo tanto se evaluará la existencia, aplicación y nivel de capacidad de cada proceso con la participación de los catalizadores como son: políticas, principio y marcos de referencia, estructuras organizativas, cultura, ética y comportamiento, información, servicios, infraestructura y aplicaciones, personas, habilidades y competencias relacionadas explícitamente a la seguridad de la información.

3.4.1. Metas Corporativas

COBIT 5 es un marco metodológico que permite gestionar las TI en las diferentes organizaciones independientemente de su tamaño y actividad económica. Cocinas Internacionales es una PYME. Los Objetivos Corporativos de Cocinas Internacionales, se encuentran determinados desde el plan de mejoramiento continuo realizado en el año 2004, donde fue utilizado Balance Score Card (BSC), para la definición de la filosofía corporativa de la empresa y objetivos estratégicos desde cuatro perspectivas, como se indica en la tabla 8.

Tabla 8

Objetivos Corporativos de Cocinas Internacionales

Perspectiva	Objetivo Estratégico
Financiera	Implementar tácticas y políticas en el área administrativa - financiera para mantener y mejorar el uso efectivo de los recursos financieros que son la base del posicionamiento económico
Cliente	Optimizar el uso de los recursos tecnológicos que la empresa posee para mantener la innovación constante, la diversificación de productos, la satisfacciones de los clientes, el establecimiento de estrategias de diferenciación y la calidad total
Interna	Consolidar la filosofía corporativa de la organización y la clara definición de las tareas, funciones y responsabilidades de las áreas para lograr el compromiso del personal con la empresa, la realización de actividades dentro de los valores y los principios institucionales, el mejor aprovechamiento del recurso humano, la integración y la canalización correcta de actividades
Aprendizaje y Crecimiento	Desarrollar los procesos de la empresa que permitan el mejoramiento continuo de sus operaciones, el incremento de la productividad y una excelente administración

Fuente: (Cocinas Internacionales, 2005)

Dichas metas corporativas han sido aprobadas por el Gerente Fábrica de Cocinas Internacionales y han sido localizadas en la documentación de la organización.

3.4.2. Mapeo de Metas Corporativas de COBIT 5 para la empresa

Una vez especificadas las Metas Corporativas se establece una relación con las 17 Metas del Negocio genéricas de COBIT 5 que señalan metas y/o objetivos muy específicos de las organizaciones, basados en las dimensiones de Balance Score Card (Financiera, Cliente, Interna y de Aprendizaje y Crecimiento).

Estas metas se encuentran definidas de una manera genérica en base al estudio de factores externos que influencian la ruta que sigue la empresa para conseguir sus metas y objetivos. Para determinar estas metas genéricas, COBIT 5 toma factores externos como: ambientes de regulación,

tendencias tecnológicas, la competencia y demanda de mercado y también la visión que se tiene del negocio.

Estas metas se encuentran definidas en la figura 14, se ha tomado como referencia esta guía que ofrece Cobit 5 para crear una matriz donde se realiza el mapeo de los objetivos estratégicos de negocio de la empresa Cocinas Internacionales con las metas del Negocio Genéricas de COBIT 5, ver tabla 9.

Tabla 9

Metas Corporativa de Cocinas Internacionales y de COBIT 5

	OBJETIVO CORPORATIVOS DE COBIT 5																
	Valor para las partes interesadas	Cartera de Productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de decisiones basadas en información	Optimización de costes de entrega de servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personal motivado y entrenado	Cultura de innovación del producto y del negocio
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
OBJETIVOS CORPORATIVOS DE COCINAS INTERNACIONALES			**Financiera**					**Cliente**					**Interna**			**Aprendizaje y Crecimiento**	
Objetivo Corporativo Financiero	X			X	X												
Objetivo Corporativo Orientado al Cliente						X	X		X	X	X			X			
Objetivo Corporativo Interno											X	X		X	X	X	
Objetivo Corporativo de Aprendizaje y Crecimiento																X	X

Como resultado del mapeo realizado de metas corporativas, 13 metas de 17 metas genéricas han sido aceptadas y aprobadas por el Gerente de Fábrica, el Ingeniero Jairo Ron, teniendo en cuenta que son metas que están involucradas dentro de su organización del marco metodológico de COBIT 5. En la siguiente tabla se encuentran enlistadas las 13 metas genéricas de COBIT aplicables a la empresa:

Tabla 10

Metas de Negocio de COBIT 5 para Cocinas Internacionales

Financiero	1	Valor para las partes interesadas
	4	Cumplimiento de leyes y regulaciones externas
	5	Transparencia Financiera
Cliente	6	Cultura de servicio orientada al cliente
	7	Continuidad y disponibilidad del servicio de negocio
	9	Toma estratégica de decisiones basada en la información
	10	Optimización de costes de entrega de servicios
Interna	11	Optimización de la funcionalidad de los procesos de negocio
	12	Optimización de los costes de los procesos de negocio
	14	Productividad operacional y de los empleados
	15	Cumplimiento con las políticas internas
Aprendizaje y Crecimiento	16	Personal motivado y entrenado
	17	Cultura de innovación del producto y del negocio

Fuente: (ISACA, 2012)

Dichas metas corporativas de COBIT 5 han sido aprobadas por el Gerente Fábrica de Cocinas Internacionales puesto que involucran el cumplimiento de sus metas organizacionales.

3.4.3. Metas Estratégicas de TI de la empresa

Debido a la ausencia de un enfoque tecnológico por parte de la empresa, no dispone de ninguna meta estratégica de TI, sin embargo, como parte del aporte de este trabajo y por requisitos del procedimiento de metas en cascada es imprescindible que la empresa disponga de metas de TI. Como aporte para la continuidad de este trabajo se establecen metas

estratégicas de TI, que tiene como objetivo fortalecer el aspecto tecnológico de la empresa.

Los objetivos propuestos a continuación guardan relación con las metas genéricas que COBIT las cuales han sido propuestas para contribuir con un adecuado gobierno y gestión de las TI en el negocio, los siguientes objetivos, serán sometidos a validación, estarán dirigidos a las autoridades de la institución para determinar su aceptación para adopción de las mismas como objetivos corporativos del negocio vinculados a las TI de Cocinas Internacionales.

Tabla 11

Metas Estratégicas de TI de Cocinas Internacionales

NRO	OBJETIVOS ESTRATEGICOS DE TI PROPUESTOS
1	Establecer una planificación estratégica y Operativa de TI, para el período 2015-2018.
2	Definir las estrategias y políticas corporativas TI, que se enfoquen en principales temas de seguridad informática y de comunicaciones, para el período 2015-2018
3	Elaborar programas de capacidad y darle seguimiento para asegurar la operación de los servicios de TI conforme a compromisos y niveles de servicio acordados como requisitos para el negocio, para el período 2015-2018.

Dichas metas estratégicas de TI han sido aprobadas por el Gerente Fábrica de Cocinas Internacionales puesto que involucran el cumplimiento de sus metas organizacionales.

3.4.4. Mapeo de Metas de TI de COBIT 5 y Metas de Negocio para la empresa

El siguiente paso de este proceso es la definición de metas de TI de COBIT 5 que se ajusten a la empresa, para ello se realiza el mapeo de las metas del negocio de la empresa Cocinas Internacionales identificadas en las metas del Negocio Genéricas de COBIT 5 con las metas de COBIT 5

Genéricas para TI. Para este proceso se toman las 17 metas genéricas de TI definidas por COBIT, metas que se encuentran en la Figura 14. A continuación se presenta en la tabla 14 el mapeo de las metas tanto de TI como de Negocio.

Tabla 12

Matriz de Metas de TI y Metas de Negocio de COBIT5

		METAS DE TI DE COBIT 5																
	OBJETIVOS CORPORATIVOS DE COBIT 5	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
FINANCIERA	1	P		P		P	S	P	S	S		P	S	P	S		S	S
	4		P		S			S			P				S	S		
	5						P											
CLIENTE	6	P				S		P	S	S			S	S			S	S
	7	S			P			S	S		P				P			
	9	P		S			S	S	S						P			S
	10	S			P	S	P		S			P	S	S				
INTERNA	11	P		S		S		P	P	P		S	P		S			S
	12	S				P	P	S	S			P	S	S				
	14					S			P	S		S	S				P	
	15		P		S						P					P		
APRENDIZAJE Y CRECIMIENTO	16	S		S	S			S	S	S							P	S
	17	S		S		S		S	S	P		S	S				S	P

La relación de las metas tanto de negocio como de TI siguen un patrón que establece la relación entre las mismas, COBIT identifica en este ámbito 3 relaciones muy definidas que son las que se representan en la figura 13. Estas relaciones son las siguientes: Relación Directa (P), Relación Secundaria (S) y ninguna relación.

3.5. Matriz de Riesgo

COBIT 5 maneja la matriz de riesgo que parte del resultado de la cascada de metas, donde se compara con la base de conocimiento de COBIT y se refina, hasta ajustarla a las necesidades de la empresa. Se ha

utilizado las matrices para refinar y ajustar los objetivos de TI con los de COBIT 5 y también para filtrar la selección de los diferentes dominios con sus procesos más críticos para la auditoría.

3.5.1. Matriz de Riesgos de COBIT 5 con Metas de TI

Una vez realizado el mapeo de los objetivos estratégicos de negocio de la empresa Cocinas Internacionales con las metas del Negocio Genéricas de TI de COBIT 5, realizamos una ponderación numérica. Esta ponderación ha sido tomada en base a lo recomendado en COBIT, donde cada meta tanto de negocio como de TI se apoyan en niveles de relaciones que han sido definidos en base al conocimiento y experiencia formada a través de las aplicaciones profesionales de TI:

- Relación Directa: 2 puntos
- Relación Indirecta: 1 puntos
- Ninguna Relación: 0 puntos

Mediante la utilización de esta ponderación se puede establecer la relaciones de las metas que mayor riesgo y criticidad deben ser considerados para efectos de este proyecto, por lo que al pie de la tabla 13, se encontrará la sumatoria de puntajes con más alto valor, las cuales llegan a representar los objetivos de más riesgo de TI dentro del negocio, estos serán sometidos a la auditoría informática.

Tabla 13

Matriz de Riesgos de COBIT para Cocinas Internacionales

		METAS COBIT 5 DE TI																
	METAS COBIT 5 DE NEGOCIO	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
1	**Valor para las partes interesadas**	2	0	2	0	2	1	2	1	1	0	2	1	2	1	0	1	1
4	**Cumplimiento de leyes y regulaciones**	0	2	0	1	0	0	1	0	0	2	0	0	0	1	1	0	0

Continua

	externas																	
5	**Transparencia financiera**	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0
6	**Cultura de Servicio Orientada al Cliente**	2	0	0	0	1	0	2	1	1	0	0	1	1	0	0	1	1
7	**Continuidad y disponibilidad del servicio de negocio**	1	0	0	2	0	0	1	1	0	2	0	0	0	2	0	0	0
9	**Toma estratégica de decisiones basadas en información**	2	0	1	0	0	1	1	1	0	0	0	0	0	2	0	0	1
10	**Optimización de costes de entrega de servicio**	1	0	0	2	1	2	0	1	0	0	2	1	1	1	0	0	0
11	**Optimización de la funcionalidad de los procesos de negocio**	2	0	1	0	1	0	2	2	2	0	1	2	0	0	0	0	1
12	**Optimización de los costes de los procesos de negocio**	1	0	0	0	2	2	1	1	0	0	2	1	1	0	0	0	0
14	**Productividad operacional y de los empleados**	0	0	0	0	1	0	0	2	1	0	1	1	0	0	0	2	0
15	**Cumplimiento con las políticas internas**	0	2	0	1	0	0	0	0	0	2	0	0	0	0	2	0	0
16	**Personal motivado y entrenado**	1	0	1	1	0	0	1	1	1	0	0	0	0	0	0	2	1
17	**Cultura de innovación del producto y del negocio**	1	0	1	0	1	0	1	1	2	0	1	1	0	0	0	1	2
		13	4	6	7	9	8	12	12	8	6	9	8	5	7	3	7	7

Los objetivos resultantes con mayor ponderación que se exponen a continuación, fueron sometidos a validación, estuvieron dirigidos a las autoridades de la institución para determinar su aceptación para adopción de las mismas como objetivos de TI de Cocinas Internacionales, tabla 14. Como

parte de este estudio se tomo los objetivos de TI que reunieron un puntaje superior al 8 que se consideraron de alto riesgo.

Tabla 14

Metas de TI de COBIT de Cocinas Internacionales

Nro.	Metas de TI para la Empresa Cocinas Internacionales
1	Alineamiento de TI y la Estrategia de Negocio
5	Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI
6	Transparencias de los costes, beneficios y riesgos de las TI
7	Entrega de servicios de TI de acuerdo a los requisitos del negocio
8	Uso adecuado de las aplicaciones, información y soluciones tecnológicas
9	Agilidad de las TI
11	Optimización de activos, recursos y capacidades de las TI
12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio

Dichas metas estratégicas de TI han sido aprobadas por el Gerente Fábrica de Cocinas Internacionales, y han sido consideradas metas de alto riesgo en la organización.

3.5.2. Matriz de Riesgos de COBIT 5 con los Procesos de COBIT 5

Una vez realizada la validación y aprobación de las metas de TI de COBIT 5 para el negocio, se procede a realizar la matriz de ponderaciones cruzando la información de las metas de TI con los procesos por dominio validados en COBIT 5 para la empresa.

Tabla 15

Matriz de Riesgos de COBIT 5 con Procesos

	PROCESOS COBIT 5		METAS COBIT TI DEL NEGOCIO								SUMATORIA
DOMINIO	**CÓDIGO**	**PROCESOS**	**1**	**5**	**6**	**7**	**8**	**9**	**11**	**12**	
Evaluar, Orientar y Supervisar	**EDM01**	Asegurar el establecimiento y Mantenimiento del Marco de Gobierno	2	1	1	2	0	1	1	1	**9**

Continua

	EDM02	Asegurar la entrega de Beneficios	2	2	2	2	1	0	1	1	**11**
	EDM03	Asegurar la Optimización del Riesgo	1	0	2	1	1	0	0	0	**5**
	EDM04	Asegurar la Optimización de Recursos	1	1	1	1	1	2	2	0	**9**
	EDM05	Asegurar la Transparencia hacia las partes interesadas	1	0	2	2	0	0	0	0	**5**
Alinear, Planificar y Organizar	**APO01**	Gestionar el Marco de Gestión de TI	2	0	0	1	0	2	2	1	**8**
	APO02	Gestionar la Estrategia	2	1	0	2	1	1	1	1	**9**
	APO03	Gestionar la Arquitectura Empresarial	2	1	1	1	1	2	2	1	**11**
	APO04	Gestionar la Innovación	1	2	0	0	2	2	2	1	**10**
	APO05	Gestionar el Portafolio	2	2	0	0	2	2	2	1	**11**
	APO06	Gestionar el Presupuesto y los Costes	1	2	2	1	1	0	1	0	**8**
	APO07	Gestionar los Recursos Humanos	2	0	0	1	0	1	2	0	**6**
	APO08	Gestionar las Relaciones	2	1	1	2	1	0	1	2	**10**
	APO09	Gestionar los Acuerdos de Servicio	1	1	1	2	1	1	1	0	**8**
	APO10	Gestionar los proveedores	0	1	1	2	1	2	1	0	**8**
	APO11	Gestionar la Calidad	1	2	0	2	1	1	1	0	**8**
	APO12	Gestionar el Riesgo	0	0	2	1	1	1	0	0	**5**
	APO13	Gestionar la Seguridad	0	0	2	1	1	0	0	0	**4**
Construcción, Adquisición e Implementación	**BAI01**	Gestionar los Programas y Proyectos	2	2	1	1	1	0	1	0	**8**
	BAI02	Gestionar la definición de los Requisitos	2	1	0	2	1	1	1	2	**10**
	BAI03	Gestionar la Identificación y Construcción de Soluciones	1	1	0	2	1	0	1	1	**7**
	BAI04	Gestionar la Disponibilidad y la Capacidad	0	1	0	2	1	1	2	0	**7**

Continua

	BAI05	Gestionar la Introducción de Cambios Organizativos	1	1	0	1	2	1	1	1	**8**
	BAI06	Gestionar Cambios	0	1	0	2	1	1	1	1	**7**
	BAI07	Gestionar la Aceptación del Cambio y de la Transición	0	1	0	1	2	1	0	2	**7**
	BAI08	Gestionar el Conocimiento	1	1	0	1	1	2	1	0	**7**
	BAI09	Gestionar los Activos	0	0	2	1	0	1	2	1	**7**
	BAI10	Gestionar la Configuración	0	0	2	1	0	1	2	0	**6**
	DSS01	Gestionar Operaciones	0	1	0	2	1	1	2	0	**7**
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio	0	0	0	2	1	0	0	0	**3**
Entregar, Dar Servicio y Soporte	**DSS03**	Gestionar los Problemas	0	1	0	2	1	1	2	1	**8**
	DSS04	Gestionar la Continuidad	1	1	0	2	1	1	1	1	**8**
	DSS05	Gestionar los Servicios de Seguridad	1	0	0	1	1	0	1	1	**5**
	DSS06	Gestionar los controles de los Procesos de Negocio	0	0	0	2	1	0	1	1	**5**
	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	1	1	1	2	1	1	2	0	**9**
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno	0	0	1	1	1	0	0	0	**3**
Supervisión, Evaluación y Verificación	**MEA03**	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	0	1	0	1	0	0	0	0	**2**

Los procesos resultantes con mayor ponderación que se exponen a continuación en la tabla 16, fueron sometidos a validación, están dirigidos a las autoridades de la institución para determinar su aceptación relacionada con la auditoría de TI de Cocinas Internacionales. Como parte de este

estudio, se tomo los procesos que reunieron un puntaje superior a 9 que se consideraron de alto riesgo para las actividades de la empresa.

Tabla 16

Procesos de TI de Alto Riesgo en Cocinas Internacionales

Dominio	Código	Procesos
Evaluar, Orientar y Supervisar	EDM01	Asegurar el establecimiento y mantenimiento del marco de gobierno
	EDM02	Asegurar la entrega de beneficios
	EDM04	Asegurar la optimización de recursos
Alinear, Planificar y Organizar	APO02	Gestionar la Estrategia
	APO03	Gestionar la Arquitectura
	APO04	Gestionar la Innovación
	APO05	Gestionar el Portafolio
	APO08	Gestionar las Relaciones
Construcción, Adquirían e Implementación	BAI02	Gestionar la definición de requisitos
Supervisión, Evaluación y Verificación	MEA01	Supervisar, Evaluar y Valorar el rendimiento de Conformidad

En acuerdo con el gerente de fábrica de Cocinas Internacionales se hizo la revisión de los procesos resultantes considerados de alto riesgo para la empresa, los mismos que fueron aprobados para ser sometidos en el proceso de auditoría informática enfocada a las seguridades de la información.

De esta manera queda establecido para Cocinas Internacionales los procesos de cada dominio de COBIT 5, serán auditados, para de esta forma conocer si la condición de gestión de sus recursos tecnológicos brinda adecuados niveles de seguridad en la información y brinda un conocimiento de las diferentes alternativas que se puede tomar en cuenta para propender a una mejora continua.

3.6. Plan de Investigación de Campo

Para poder realizar una recolección efectiva de datos e información que sirva como evidencia para respaldar este trabajo se elaboró un plan de auditoría que ha permitido establecer, que proceso está considerado en la evaluación, cuál es la práctica de gestión que se audita, también identifica qué actividad de auditoría se registrará en la misma definiendo las herramientas y/o instrumentos que se utilizará para recolectar la información.

Como información clave también se tendrá la fuente de obtención de datos sea un recurso humano o recurso tecnológico con su respectiva fecha de aplicación. Esta auditoría está relacionada directamente con la evaluación de Seguridades Informáticas tomando como referencia la norma internacional ISO/IEC 27001: 2013, vigente en Ecuador. La información de las empresas debe cumplir con ciertas características que garanticen seguridad, los atributos deseables para la información deberían garantizar no divulgación no autorizada (confidencialidad), no modificación inapropiada (integridad) y disponibilidad conforme sea requerida (disponibilidad)

Estos tres aspectos son fundamentales para establecer seguridad de la información y la norma internacional ISO/IEC 27001:2013 plantea un efectivo establecimiento de sistemas que administren seguridad de la información, los cuales deben estar basados en controles efectivos y adecuados, configurables para adaptación a las necesidades de cada empresa. Como herramienta de ayuda para el auditor se desarrollo el siguiente cuadro que se muestra en la tabla 17, estas actividades son programadas bajo el alineamiento y colaboración de la norma ISO/IEC 27001: 2013.

Tabla 17

Planificación de Auditoría de los Procesos de COBIT 5

PROCESO DE TI COBIT 5	PRÁCTICA DE GESTION	ACTIVIDAD DE AUDITORÍA	HERRAMIENTA INSTRUMENTOS	FUENTES	FECHA DE APLICACIÓN
EDM01 Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	Evaluar el sistema de gobierno.	Evaluar el grado en el que la seguridad de la información cumple con las necesidades de negocio y regulatorias/cumplimiento	Entrevista Cuestionario A Cuestionario B* (según corresponda)	Ing. Jairo Ron	05/01/2016
	Orientar el sistema de gobierno	Obtener el compromiso de la alta dirección con la seguridad de la información y la gestión de riesgos de la información.	Entrevista Cuestionario A Cuestionario C* (según corresponda)	Ing. Jairo Ron	05/01/2016
		Disponer procedimientos jerárquicos de notificación y de escalado de decisiones.	Entrevista Cuestionario A Cuestionario C* (según corresponda)	Ing. Jairo Ron	05/01/2016
	Supervisar el Sistema de Gobierno	Supervisar los mecanismos ordinarios y rutinarios para garantizar que el uso de los sistemas de medida de la seguridad de la información cumple con la legislación y regulación relacionada con la seguridad de la información. Analizar la totalidad de las Implicaciones del cambiante contexto de las amenazas.	Entrevista Cuestionario A	Ing. Jairo Ron	05/01/2016
EDM02: Asegurar la entrega de beneficios	Evaluar la optimización de valor	Identificar y registrar los requisitos de las partes interesadas (tales como accionistas, reguladores, auditores y clientes) para proteger sus intereses y aportar valor a través de la actividad de seguridad de la información. Establecer directrices en consonancia con lo anterior.	Entrevista Cuestionario B*	Ing. Jairo Ron	05/01/2016
	Supervisar la optimización de valor	Seguir los resultados de las iniciativas de seguridad de la información y compararlos con las expectativas para asegurar la entrega de valor frente a los objetivos del negocio.	Entrevista Cuestionario B*	Ing. Jairo Ron	05/01/2016

Continua

EDM04: Asegurar la optimización de Recursos	Evaluar la gestión de recursos	Evaluar la eficacia de los recursos de seguridad de la información en términos de suministro, formación, concienciación y competencias de los recursos necesarios en comparación con las necesidades del negocio.	Entrevista Cuestionario D	Ing. Jairo Ron	06/01/2016
	Supervisar la gestión de recursos	Medir la eficacia, eficiencia y capacidad de los recursos de seguridad de la información respecto a las necesidades del negocio	Entrevista Cuestionario D	Ing. Jairo Ron	06/01/2016
APO02: Gestionar la Estrategia	Realizar un análisis de las deficiencias	Examinar el entorno actual con respecto a las regulaciones y los requisitos de cumplimiento	Cuestionario E Cuestionario F	Ing. Jairo Ron	06/01/2016
APO03 Gestionar la Arquitectura Empresarial	Definir la arquitectura de referencia	Asegurar la inclusión de elementos, políticas y normas de seguridad de la información en el repositorio de arquitectura	Entrevista Cuestionario A Cuestionario B* (según corresponda)	Ing. Jairo Ron	06/01/2016
		Asegurar que la seguridad de la información se encuentra integrada a lo largo de todos los dominios de la arquitectura	Entrevista Cuestionario A Cuestionario B* (según corresponda)	Ing. Jairo Ron	06/01/2016
APO04: Gestionar la Innovación	Evaluar el potencial de las tecnologías	Evaluar el cumplimiento de estos requisitos.	Pruebas de Cumplimiento	3 PCS Aleatorios	07/01/2016 - 21/01/2016
APO05: Gestionar el Portafolio	Evaluar y seleccionar los programas a	Asegurar la existencia de un programa de seguridad de la información.	Pruebas de Cumplimiento	3 PCS Aleatorios	07/01/2016 - 21/01/2016
	Gestionar la consecución de beneficios	Evaluar los cambios en el perfil de riesgo de seguridad de la información, para ilustrar la consecución de beneficios	Pruebas de Cumplimiento	3 PCS Aleatorios	07/01/2016 - 21/01/2016
APO08 Gestionar las Relaciones	Coordinar y comunicar	Establecer los canales de comunicación adecuados entre la función de seguridad de la información y el negocio	Entrevista Cuestionario A Cuestionario C* (según corresponda)	Ing. Jairo Ron	05/01/2016
		Estableces la presentación de informes y métricas sobre seguridad de la información de forma adecuadas	Entrevista Cuestionario A Cuestionario C* (según corresponda)	Ing. Jairo Ron	05/01/2016

Continua

BAI02: Gestionar la Definición de Requisitos	Definir y mantener los requisitos técnicos y	Asegurar que los requisitos de negocio tienen en cuenta las necesidades de protección de seguridad de la información.	Cuestionario G Cuestionario de Riesgo Físico Pruebas de Cumplimiento	Ing. Jairo Ron 3PCS Aleatorios	07/01/2016 - 21/01/2016
MEA01: Supervisar, Evaluar y Valorar el rendimiento y Conformidad	Establecer los objetivos de cumplimiento y rendimiento	Evaluar si los objetivos y las métricas de seguridad de la información son adecuadas, es decir, específicas, medibles, realizables, pertinentes y de duración determinada	Cuestionario de Clasificación de Información Entrevista Cuestionario H*	Ing. Jairo Ron	07/01/2016 - 21/01/2016

La tabla 18, ofrece un detalle más específico de cómo han sido aplicadas las diferentes herramientas para la recolección de información como evidencia de fallos, vulnerabilidades y riesgos que presentan los sistemas de información de Cocinas Internacionales.

Tabla 18

Planificación para Aplicación de Herramientas de Auditoría

Actividad	Herramientas	Fecha	Fuente
Entrevistas, con su respectivo cuestionario, Observación Directa	Cuestionario A Cuestionario B Cuestionario C	05/01/2016	Ing. Jairo Ron
Entrevistas, con su respectivo cuestionario, Observación Directa	Cuestionario D Cuestionario E Cuestionario F Cuestionario G Cuestionario H Cuestionario de Cumplimiento Cuestionario1 Equipo1 Cuestionario2 Equipo1 Cuestionario3 Equipo1 Cuestionario1 Equipo2 Cuestionario2 Equipo2 Cuestionario3 Equipo2	07/12/2016	Ing. Jairo Ron Custodio Equipo 2 Gerencia de Fábrica Sr. Francisco Enríquez Custodio Equipo 1 Diseño 1
Entrevistas, Pruebas y evaluaciones en Sitio, Observación Directa	Cuestionario1 Equipo3 Cuestionario2 Equipo3 Cuestionario3 Equipo3	08/01/2016	Sra. Patricia Córdova Custodio Equipo 3 Asistencia de Gerencia

Continua

Entrevistas, Pruebas y evaluaciones en Sitio	Cuestionario de Respaldos Cuestionario de Sistema de Vigilancia Pruebas en Sitio de verificación de Respaldos Pruebas de Verificación Equipo 1 Pruebas de Verificación Equipo 2 Pruebas de Verificación Equipo 3 Captura de Información Equipo 1 Captura de Información Equipo 2 Captura de Información Equipo 3	13/01/2016	Ing. Jairo Ron Custodio Equipo 2 Gerencia de Fábrica Sr. Francisco Enríquez Custodio Equipo 1 Diseño 1 Sra. Patricia Córdova Custodio Equipo 3 Asistencia de Gerencia
Entrevistas, Pruebas y evaluaciones en Sitio, Observación Directa	Cuestionario Normativa Cuestionario1 Equipo3 Cuestionario2 Equipo3 Cuestionario3 Equipo3 Pruebas de verificación Equipo 4 Captura de Información Equipo 4 Cuestionario de Uso de Aplicaciones Equipo 1	16/01/2016	Sra. Omayra Ruiz Custodio Equipo 4 Contabilidad Sr. Francisco Enríquez Custodio Equipo 1 Diseño 1
Entrevistas, Pruebas y evaluaciones en Sitio, Observación Directa	Cuestionario de Uso de Aplicaciones Equipo 3 Cuestionario de Uso de Aplicaciones Equipo 4	19/01/2016	Sra. Omayra Ruiz Custodio Equipo 4 Contabilidad Sra. Patricia Córdova Custodio Equipo 3 Asistencia de Gerencia
Entrevistas, Pruebas y evaluaciones en Sitio, Observación Directa	Cuestionarios: Riesgos Físicos Clasificación Información Cuestionario de Uso de Aplicaciones Equipo 2	27/01/2016	Sra. Omayra Ruiz Custodio Equipo 4 Contabilidad Ing. Jairo Ron Custodio Equipo 2 Gerencia de Fábrica

3.6.1. Recursos para el Desarrollo del Plan de Investigación de Campo

A continuación se describirán los recursos que fueron necesarios para llevar a cabo el proceso de recopilación de la información como parte de evidencia de la auditoria, algunos de ellos fueron diseñados para ajustarse a la necesidad de la empresa y a la información que se necesitaba obtener, los otros recursos fueron sujetos provistos por parte de la empresa:

Recursos Humanos: Para recolectar y analizar la información se requirió de un Auditor/Evaluador que tenga el conocimiento para llevar a cabo una auditoría bajo el modelo de COBIT 5. Para este proyecto se

manejo un único recurso para la auditoría, la Srta. Ana Lucia Jiménez quien llevo a cabo todo el proceso de auditoría informática.

Recursos de Evidencia: Para hacer posible la planeación de la auditoría se ha partido desde la definición de los procesos más críticos de la empresa, construyendo como resultante la matriz de riesgos, véase tabla 16 y tabla 17. Para ello se requirió de las siguientes herramientas

- **Entrevistas:** Son la herramienta mediante la cual se ha podido obtener una visión general de la empresa, ha permitido definir un pre-diagnóstico, para usar esta herramienta, se recibió el apoyo de la gerencia de fábrica y personal que interactúa con los recursos tecnológicos de la misma.
- **Cuestionarios:** Herramienta mediante la cual se recoge información más detallada para evidencia de las posibles debilidades y vulnerabilidades de la empresa en su entorno tecnológico, que se constituyen en un instrumento de constancia escrita por parte del entrevistado.
- **Pruebas de Cumplimiento:** Esta herramienta nos permitió definir la existencia de controles internos en la organización, a la vez que documentación de verificación para evaluar el nivel o índice de cumplimiento con dichos controles y normas de la organización y externas a ella.
- **Observación Directa:** La observación directa es una herramienta del auditor que permite determinar aspectos generales que se detectan en el tratamiento de la información, como el comportamiento del personal, seguridades físicas implementadas contribuyen con la seguridad de la información y entorno de trabajo tecnológico favorable existente.

Recurso Tecnológico: Se ha trabajado con un computador portátil para la generación de documentos requeridos para el desarrollo de la planificación de la auditoría, así como para el almacenamiento de la

información documentada de la empresa necesario para las actividades programadas. Los programas utilizados para el desarrollo de este proyecto han sido:

- Microsoft Office Word 2007, documentación
- Microsoft Office Excel 2007, matrices y cronogramas

3.6.2. Aplicación de los instrumentos de Investigación

De acuerdo a la planificación establecida para la aplicación de la auditoría con los diferentes instrumentos de investigación se procedió a evaluar el nivel de seguridad de la información en los procesos identificados de alto riesgo, debido a la fuerte relación entre las TI y el Negocio, que apoyan el fortalecimiento y crecimiento.

La mayor parte de entrevistas fueron aplicadas al Gerente de Fábrica de la empresa, debido a que la empresa no tiene una estructura especializada en donde se especifique un área específica para las TI y tampoco se encuentra una especialización para los temas de seguridad de la información, razón por lo que la mayor información de la empresa se obtuvo a través de entrevistas directas con el gerente de fábrica y la auxiliar contable, quien fue delegada por la misma autoridad para proporcionar la información necesaria en la auditoría.

Cabe indicar que durante todo el proceso de auditoría se manejo el instrumento de observación directa lo que permitió tener una idea más general de la condición de la empresa. De la misma manera se ha procedido a la aplicación de cuestionarios que nos permitan capturar la información que los empleados nos pueden brindar como evidencia para la valoración del grado de Seguridad de la Información que manejan y como la empresa ha contribuido en el entrenamiento y conocimiento del personal para esta área.

Además se utilizó la revisión de la información documental existente en la empresa, tanto para verificación del establecimiento de un marco de

gobierno, así como para la verificación de la integración en el marco de negocio a las TI, considerando su interés en la seguridad de la información. También a través de esta documentación se logró realizar la verificación de cumplimiento, obteniendo las evidencias suficientes que permitan realizar la construcción de las recomendaciones necesarias, para mejorar la gestión del negocio en temas de TI y seguridad de la información.

3.7. Análisis de Información

La información obtenida se encuentra contenida en los diferentes cuestionarios en los que se ha capturado la información pertinente como evidencia para conocer la condición de capacidad de cada proceso dentro de la empresa. A continuación en la Tabla 21, se menciona los resultados obtenidos en cada proceso tras la aplicación de los instrumentos de auditoría según el programa planificado

Tabla 19

Resultados de la Auditoría Informática por Procesos

Proceso	Práctica de Gobierno / Gestión	Actividad	Pregunta Principal	Instrumento	Respuesta	Resultado
EDM01	EDM01.01. Evaluar el Sistema de Gobierno	Evaluar la existencia de Sistema de Gestión de Seguridad de la Información	1.- ¿Posee la empresa un sistema de Gestión de Seguridad de la Información?	Entrevista directa Cuestionario A	La dirección ha manifestado que la empresa no dispone de ninguna gestión tecnológica, ni de seguridad de la información	NEGATIVO
EDM01	EDM01.02. Orientar el Sistema de Gobierno	Evaluar que el Sistema de Gestión de seguridad se alinee a la estrategia del negocio	No aplica		La empresa carece de un sistema de gestión de seguridad de la información de manera que la práctica no puede ser evaluada	NEGATIVO

Continua

EDM01	EDM01.03. Supervisar el Sistema de Gobierno	Determinar que se cumple con lo establecido en el Sistema de Gestión de Seguridad de la Información	No aplica		La empresa carece de un sistema de gestión de seguridad de la información de manera que la práctica no puede ser evaluada	NEGATIVO
EDM02	EDM02.01. Evaluar la optimización de valor	Evaluar la Existencia de programas de optimización de valor relacionados a la Seguridad de la Información	2.- ¿La empresa posee programas de optimización de valor relacionadas a la seguridad de la información?	Entrevista directa	La dirección de la empresa ha indicado que no se ha realizado programas para la optimización de valor desde la perspectiva de seguridad de la información	NEGATIVO
EDM02	EDM02.02. Orientar la optimización de Valor	Evaluar los tipos y los criterios de inversión que aporten con iniciativas de seguridad de la información que se han utilizado para los programas de optimización de valor	No aplica		Debido a la ausencia de programas de optimización de valor relacionados a la seguridad de la información la actividad no puede ser evaluada, porque la información no existe	NEGATIVO
EDM02	EDM02.03. Supervisar la optimización de Valor	Verificar que los programas de optimización de valor relacionadas a la seguridad de la información cumplen con las expectativas del negocio	No aplica		Debido a la ausencia de programas de optimización de valor relacionados a la seguridad de la información la actividad no puede ser evaluada, porque la información no existe	NEGATIVO
EDM04	EDM04.01.Evaluar la gestión de recursos	Evaluar la existencia de un plan de asignación de recursos TI que involucren la consideración de aspectos de seguridad de la información	3.- ¿Cuenta la empresa con un plan de asignación de recursos que contemple políticas relacionadas a la seguridad de la información?	Entrevista directa	La empresa no cuenta con planes de asignación de recursos TI	NEGATIVO
EDM04	EDM04.02. Orientar la gestión de Recursos	Evaluar con que grado de eficacia y eficiencia se asignan los recursos de TI considerando el cumplimiento de aspectos de seguridad de la información	No aplica	Entrevista directa Cuestionario D	La ausencia de planes aprobados de asignación de recursos de TI generan como resultado una actividad que no puede ser evaluada	NEGATIVO

Continua

EDM04	EDM04.03. Supervisar la Gestión de Recursos	Evaluar el cumplimiento de los planes de gestión de recursos de TI que respeten los aspectos de seguridad de la información provistos	No aplica		La ausencia de planes aprobados de asignación de recursos de TI generan como resultado una actividad que no puede ser evaluada	NEGATIVO
APO02	APO02.01. Comprender la Dirección de la empresa	Evaluar si el entorno actual de la empresa, sus objetivos y estrategias se encuentran alineadas con las TI	4.- ¿El entorno de la empresa sus objetivos y estrategias integran la participación de las TI considerando un enfoque dirigido a la seguridad de la información?	Entrevista directa Cuestionario E	El plan estratégico de la empresa se encuentra desactualizado desde el año 2008, la gerencia de fábrica informa además que no se ha trabajado en la integración de la seguridad informática al uso de las TI corporativas	NEGATIVO
APO02	APO02.02. Evaluar el entorno, capacidades y rendimiento actuales	Evaluar que el entorno de la empresa presenta la capacidades adecuadas para afrontar los riesgos relativos a la seguridad de la información y que su rendimiento ha sido probado con éxito	5.- ¿Cuenta la empresa con capacidades para mitigar riesgos relacionados a la seguridad de la información?	Entrevista directa Cuestionario E	La ausencia de un gobierno tecnológico impide que la empresa tenga capacidad de reconoces los riesgos vinculados a la seguridad de la información por lo que no existe información que permita a la empresa afrontar riesgos de seguridad de la información	NEGATIVO
APO02	APO02.03. Definir las capacidades objetivo para TI	Verificar la existencia de la definición de capacidades de la seguridad de la empresa	No aplica		La empresa no cuenta con información que permita realizar una evaluación sobre la definición de capacidades objetivo de TI	NEGATIVO
APO02	APO02.03. Definir las capacidades objetivo para TI	Verificar las necesidades de seguridad de la empresa	No aplica		La empresa no cuenta con información que permita realizar verificar las necesidades de seguridad de la información de la empresa	NEGATIVO
APO02	APO02.03. Definir las capacidades objetivo para TI	Verificar la existencia de normas y regulaciones de la seguridad de la información	No aplica		La empresa no cuenta con información que permita realizar la verificación de normas y regulaciones de la seguridad de la información	NEGATIVO

Continua

APO02	APO02.04. Realizar un análisis de las deficiencias	Verificar que la empresa tenga identificadas las carencias detectadas en el entorno de Ti relacionada a la seguridad de la información	6.- ¿Tiene la empresa información que contenga el estudio y análisis de las deficiencias que presenta la empresa relacionadas a la seguridad de la información	Entrevista directa Cuestionario E	la empresa no posee ninguna información que evidencie las deficiencias encontradas en el ámbito de TI, ni de la seguridad informática	NEGATIVO
APO02	APO02.05. Definir el plan estratégico o la hoja de ruta	Verificar que el plan estratégico de seguridad de la información se encuentre alineado tanto a las estrategias de TI como a las estrategias del Negocio	No aplica		La empresa no cuenta con estrategias para la seguridad de la información	NEGATIVO
APO02	APO02.06. Comunicar la estrategia y la dirección de TI	Verificar que los temas referentes a seguridad de la información he hayan comunicado a todas las partes interesadas y que esta información sea completa para capacitar a todas las partes involucradas	7.- ¿Se ha comunicado en la empresa temas relativos a la seguridad de la información?	Entrevista directa Cuestionario C	La empresa no ha comunicado a su organización e interesados ningún tema vinculado a la seguridad de la información del ambiente de TI	NEGATIVO
APO03	APO03.01. Desarrollar la visión de la arquitectura de la empresa	Verificar que la empresa cuente con una arquitectura empresarial definida que muestra las capacidades de permiten cumplir con las estrategias del negocio	8.- ¿Se encuentra definida formalmente la arquitectura de la empresa?	Entrevista directa	La empresa no tiene definida de manera formal una arquitectura empresarial	NEGATIVO
APO03	APO03.02. Definir la arquitectura de referencia	Verificar que la arquitectura empresarial refleje la situación actual y objetivo de la empresa	No aplica		La empresa no ha entregado información sobre la arquitectura empresarial por lo que no se puede realizar la evaluación	NEGATIVO

Continua

APO03	APO03.03. Seleccionar las oportunidades y soluciones	Analizar la capacidad de oportunidades detectadas por parte de la empresa junto con su programa de inversiones para los temas de seguridad de la información y valorar sus esquemas planteados para afrontar las soluciones	9.- ¿Se ha realizado inversiones relacionadas a la provisión y mejoramiento de seguridad de la información de la empresa en base a las oportunidades detectadas y/o las soluciones requeridas?	Entrevista Directa	La empresa no cuenta con programas de inversión orientados a las TI y a la seguridad de la información, la evaluación de la capacidad no puede ser valorada	NEGATIVO
APO03	APO03.04. Definir la implementación de la arquitectura	Verificar que la implementación de la arquitectura empresarial se encuentre debidamente planificada y alineada a la estrategia del negocio	10.- ¿Existe la planificación para la implementación de una arquitectura empresarial?	Entrevista Directa	La empresa no ha entregado información sobre la arquitectura empresarial por lo que no se puede realizar la evaluación	NEGATIVO
APO03	APO03.05. Proveer los servicios de arquitectura empresarial	Verificar que los servicios de la arquitectura empresarial se cumplan bajo el cumplimiento de las maneras de trabajar	No aplica		La empresa no ha entregado información sobre la arquitectura empresarial por lo que no se puede realizar la evaluación	NEGATIVO
APO04	APO04.01. Crear un entorno favorable para la innovación	Verificar la existencia de planes de innovación orientados a la seguridad de la información	11.- ¿Maneja la empresa planes para la innovación tecnológica, enfocada a la seguridad de la información?	entrevista Directa	La empresa no maneja información para el manejo de planes de innovación tecnológica orientada a temas de seguridad de la información	NEGATIVO
APO04	APO04.02. Mantener un entendimiento del entorno de la empresa	Verificar que los planes de innovación que involucran la seguridad de la información contribuyan al cumplimiento de las estrategias del negocio y de las TI	No aplica		La empresa no maneja información para el manejo de planes de innovación tecnológica orientada a temas de seguridad de la información	NEGATIVO

Continua

APO04	APO04.03. Supervisar y explorar el entorno tecnológico	Verificar que la empresa considere el entorno de negocio para el apoyo de los planes de innovación	No aplica		No existen unidades o funciones que estudien las oportunidades de innovación de TI en la empresa ni de sus seguridades	NEGATIVO
APO04	APO04.04. Analizar el potencial de las tecnologías emergentes y las ideas innovadoras	Verificar el interés de la empresa por los temas de innovación tecnológica que involucran la seguridad de la información	No aplica		No existen unidades o funciones que estudien las oportunidades de innovación de TI en la empresa ni de sus seguridades	NEGATIVO
APO04	APO04.05. Recomendar Iniciativas apropiadas adicionales	Evaluar los resultados de las pruebas, para la experimentación de la innovación tecnológica relacionada a los temas de seguridad de la información	No aplica		No existen unidades o funciones que estudien las oportunidades de innovación de TI en la empresa ni de sus seguridades	NEGATIVO
APO04	APO04.06. Supervisar la implementación y el uso de la innovación	Verificar que las soluciones de innovación adquiridas sean debidamente implementadas y utilizadas garantizando que cumplen con los niveles aceptables de riesgos	No aplica		No existen unidades o funciones que estudien las oportunidades de innovación de TI en la empresa ni de sus seguridades	NEGATIVO
APO05	APO05.01. Establecer la combinación deseada de inversiones	Verificar que exista un plan de inversiones para los temas relacionados a la seguridad de la información	12.- ¿Existe un plan de inversiones relacionado a los temas de seguridad de la información?	entrevista Directa	La empresa no maneja planes de inversión para las TI y la seguridad de la información	NEGATIVO
APO05	APO05.02. Determinar la disponibilidad y las fuentes de fondos	Verificar que exista la disponibilidad de recursos para cumplir con el plan de inversiones previsto a los temas relacionados a seguridad de la información	No aplica		La empresa no maneja planes de inversión para las TI y la seguridad de la información	NEGATIVO

Continua

APO05	APO05.03. Evaluar y seleccionar los programas a financiar	Verificar la existencia de un programa de seguridad de la información	13.- ¿Existe algún programa en la empresa para la seguridad de la información?	entrevista Directa Cuestionario de Cumplimiento de Activos Informáticos	No poseen programas para la seguridad de la información que considere las aplicaciones a financiar	NEGATIVO
APO05	APO05.04. Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversión	Verificar que el programa de seguridad de la información sea supervisado, optimizado y entregue un resultado de rendimiento a la inversión	No aplica		No poseen programas para la seguridad de la información	NEGATIVO
APO05	APO05.05. Mantener los portafolios	Verificar que la empresa mantenga en operación el portafolio de programas de seguridad de la información	No aplica	entrevista Directa	No poseen programas para la seguridad de la información , existen aplicaciones que consideran la seguridad de la información pero no se encuentran registrados dentro del portafolio de aplicaciones de la empresa	NEGATIVO
APO05	APO05.06. Gestionar la consecución de beneficios	Verificar que el portafolio de seguridad proporcione y mantenga los beneficios y capacidades de TI apropiadas	No aplica		No poseen programas para la seguridad de la información	NEGATIVO
APO08	APO08.01. Entender las expectativas del negocio	Verificar la compresión de los problemas relacionados a seguridad de la información para cumplir con las estrategia de TI y del Negocio	14.- ¿Tiene la empresa conocimiento de los problemas que se presentan en el tema de seguridad de la información y como esta afecta la consecución de las estrategias de TI y del negocio?	entrevista Directa	La empresa no posee información de los problemas de seguridad que presenta el sistema informático que impide la consecución de metas del negocio	NEGATIVO

Continua

APO08	APO08.02. Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio	Verificar las consideraciones que posee el plan de innovación de las TI enfocada a las seguridades de la información, considerando las oportunidades, riesgos y limitaciones para la mejora del negocio	15.- ¿Considera el plan de innovación de TI enfocada a la seguridad aspectos como: oportunidades, riesgos y limitaciones?	entrevista Directa	La empresa no tiene información acerca de la identificación de las oportunidades, riesgos y limitaciones de TI para mejorar el negocio desde el enfoque de seguridad de la información.	NEGATIVO
APO08	APO08.03. Gestionar las relaciones con el negocio	Verificar la existencia de informes que señalen el rendimiento de las TI implementadas en relación a la seguridad de la información	16.- ¿Maneja la empresa informes que permitan la medición del rendimiento de las soluciones tecnológicas adoptadas en relación a la seguridad de la información?	entrevista Directa	No existe información sobre el desarrollo de informes que indiquen el rendimiento de las TI desde la perspectiva de seguridad de la información	NEGATIVO
APO08	APO08.04. Coordinar y comunicar	Verificar que se cuenta con un plan de comunicación que involucre a todas las partes interesadas relacionada a la seguridad de la información	17.- ¿Cuenta la empresa con un plan de comunicaciones para el manejo de los temas de seguridad de la información?	entrevista Directa Cuestionario C	No se encuentra establecido ningún plan de comunicaciones relacionados a la seguridad de la información	NEGATIVO
APO08	APO08.05. Proveer los datos de entrada para la mejora continua de los servicios	Verificar informes que indiquen la mejora de la capacidad de la seguridad de la información	18. ¿Se puede verificar la capacidad de rendimiento de seguridad de la información que involucren el proceso de una mejora continua?	entrevista Directa	No existen informes para la retroalimentación de procesos de mejora continua relacionados a la seguridad de la información	NEGATIVO
BAI02	BAI02.01. Definir y mantener los requisitos técnicos y funcionales del negocio	Verificar la existencia de la documentación de los requerimientos para la seguridad de la información	19.- ¿Existe documentación de registro de los requerimientos de seguridad de la información?	entrevista Directa	No se ha verificado ninguna documentación respecto a los requisitos de seguridad de la información	NEGATIVO

Continua

BAI02	BAI02.02. Realizar un estudios de viabilidad y proponer las soluciones alternativas	Verificar la existencia de los diferentes estudios de viabilidad en la implementación de las soluciones de TI	20.- Existen estudios que contengan información sobre la viabilidad de los temas de Seguridad de la información y rasgos de las posibles alternativas de solución.	entrevista Directa	No existe información que permita la retroalimentación de temas de viabilidad para la implementación de soluciones de TI relacionadas a la seguridad de la información	NEGATIVO
BAI02	BAI02.03. Gestionar los riesgos de los requerimientos	Verificar la existencia e identificación de riesgos de seguridad en los requerimientos de seguridad	No aplica		No existe información relacionada	NEGATIVO
BAI02	BAI02.04. Obtener la aprobación de los requerimientos y las soluciones	Verificar las revisiones de los requisitos de seguridad y soluciones	No aplica		No existe información relacionada	NEGATIVO
MEA01	MEA01.01. Establecer un enfoque de la supervisión	Verificar la existencia de un procedimiento que permita la supervisión de la seguridad de la información	21.- ¿Cuenta la empresa con un programa que cumpla con medios que permitan garantizar la supervisión de la seguridad de la información?	entrevista Directa	No existe información que respalde la existencia de un procedimiento de supervisión para la seguridad de la información	NEGATIVO
MEA01	MEA01.02. Establecer los objetivos de cumplimiento y rendimiento	Verificar los planes, objetivos y métricas para evaluar el rendimiento	No aplica		No existe un programa de supervisión para la seguridad de la información	NEGATIVO
MEA01	MEA01.03. Recopilar y procesar los datos de cumplimiento y rendimiento	Verificar la recolección de información correspondientes a la evaluación de rendimiento y cumplimiento	No aplica		No existe un programa de supervisión para la seguridad de la información	NEGATIVO

Continua

MEA01	MEA01.04. Analizar e informar sobre el rendimiento	Verificar informe de revisiones sobre resultados de evaluación a programas de rendimiento de la seguridad de la información	No aplica		No existe un programa de supervisión para la seguridad de la información	NEGATIVO
MEA01	MEA01.05. Asegurar la implantación de medidas correctivas	Verificar la implementación de medidas correctivas relacionadas con la seguridad de la información	22.- ¿Se han aplicado medidas correctivas relacionadas al entorno de la seguridad de la información?	entrevista Directa	No se ha detectado ninguna información del establecimiento de medidas correctivas relacionadas a los temas de Seguridad de la Información	NEGATIVO

De acuerdo con los resultados obtenidos en la auditoría de los procesos relacionados a la seguridad de la información, se observa que los procesos no han sido implementados y tampoco se han ejecutado acciones para integrar herramientas de información necesaria para la ejecución de las garantías de seguridad de la información. Las respuestas negativas de los procesos responden a un nivel de capacidad 0 identificado en Cobit 5 Procesos Catalizadores, como un proceso no implementado o no existente, en el caso de la empresa Cocinas Internacionales los procesos no existen para seguridad de la información.

Se procede a continuación con la elaboración del Primer Informe de la Auditoría, que se llevó a cabo en la empresa, este informe será sujeto de lectura, revisión, entrega de observaciones y finalmente se procederá con la entrega del Informe Final de la Auditoría Informática realizada la empresa enfocada a los temas relacionados con seguridades de la información.

CAPÍTULO 4

INFORME TÉCNICO DE AUDITORÍA

4.1. Introducción

La empresa Cocinas Internacionales es una PYME, dedicada a la manufactura la cual produce e instala los más modernos y elegantes modulares diseñados a través del uso de tableros aglomerados y tableros de Fibraplac o MDF y en ciertas ocasiones también a través de la utilización de madera sólida, que apoyada de elementos tecnológicos producen los más agradables diseños de muebles para diferentes ambientes.

Cocinas Internacionales maneja como visión de su negocio el convertirse en una empresa líder tanto en la producción como en la instalación de muebles modulares, buscando siempre ofrecer productos de buena calidad, asumiendo la actitud de reto y compromiso, llegando a ser reconocidos en el ámbito regional y nacional por el valor agregado, los costes competitivos, los estándares de tiempo y la excelencia en el servicio que ofrecen a sus distinguidos clientes.

Su visión en el negocio de Cocinas Internacionales, es que a través de su actividad comercial puedan entregar productos que se adapten a las necesidades de sus clientes de manera permanente, es decir, que exista una continua evolución que permita cumplir con estas necesidades cambiantes sin reducir el alto nivel de calidad, consiguiendo siempre un beneficio mutuo.

Cocinas Internacionales al momento no gestiona ninguna arquitectura de TI en la empresa, su arquitectura no se encuentra formalmente definida dado que aunque maneja fuertemente un recurso tecnológico para apoyo de las actividades del negocio, el mismo no posee una estructura formal documentada que indique la composición de las estructuras de TI.

El propósito de esta auditoría fue enfocarse en la evaluación de los controles que permiten garantizar seguridad de la información en el Sistema de Información de la empresa Cocinas Internacionales, orientado para aquellos procesos críticos que se reveló tras la utilización de la cascada de metas de COBIT 5 alineada a las metas corporativas tanto del negocio como de TI propias de la empresa auditada. Evaluar si sus mecanismos de control son eficaces y eficientes para garantizar seguridad en su información y revelar las posibles deficiencias a fin de que sean cubiertas para una mayor garantía en su sistema de información.

Es sujeto de auditoría el Sistema de Información de la empresa Cocinas Internacionales, enfocando a los respectivos productos de COBIT 5 como lo son Seguridad de la Información y Aseguramiento, utilizando como marco de referencia la verificación de existencia y cumplimiento de controles efectivos para garantizar la seguridad de la información.

4.2. Resumen Ejecutivo

La empresa Cocinas Internacionales preocupada por conocer la eficiencia de su Sistema de información fue sometida a un proceso minucioso y cuidadoso de Auditoría Informática enfocada a la Evaluación de la Seguridad de la información al sistema de información que actualmente opera en la empresa.

Como parte de la actividad de la auditoría se obtuvo la suficiente información que ha servido para entender el contexto de operación de la misma a fin de conocer sus principales necesidades y la forma de apoyar estas necesidades. Esta información se obtuvo a través de la documentación facilitada de la empresa y de la entrevista directa con el gerente de fábrica quien ha participado activamente en esta actividad de auditoría.

Para la realización de esta auditoría informática a las seguridades de la información, se utilizó COBIT 5 como referencia, el cual consiste en un marco de negocio de lo más completo para gobierno y la gestión de las TI y

el Negocio, que ofrece la ventaja de aplicación a empresas de todo tamaño y de todo ámbito, teniendo como objetivo alinear las TI al negocio de tal manera que brinde mayor beneficio a la empresa. Cobit 5 nos ha permitido de esta manera alinear las metas del negocio y las de TI con las propias metas de la empresa.

Junto con la dirección se trabajo en la definición y el establecimiento de las metas de la empresa utilizando el modelo de cascada de metas de COBIT 5. Una vez realizada la cascada de metas se construyo la matriz de riesgos, donde se selecciono en acuerdo con la dirección de la empresa los procesos más críticos de la empresa para ser sometidos a las evaluaciones enfocadas al producto de Cobit 5 para la Seguridad de la Información.

La selección de los procesos de mayor riesgo permitió la elaboración de los diferentes instrumentos para la planificación y recolección de evidencia que apoya al informe final de auditoría, en el cual se ha logrado plasmar un conjunto de recomendaciones que permitirán a la empresa fortalecer el ámbito de seguridad de la información que se requiere para garantizar la operación segura de su valioso activo como es la información del negocio.

4.3. Alcance de la Auditoría

De conformidad con la carta de auspicio para servicios de auditoría, se realizó la auditoría informática dirigida al sistema de información de la empresa Cocinas Internacionales, enfocado en seguridades de la información, la auditoría se desarrolló en las fechas: del 19 de Octubre del 2015 al 04 de febrero del 2016. El alcance de esta auditoría consistió en la evaluación de controles a los procesos seleccionados mediante un análisis de riesgo, que permitan revelar la condición de seguridad de la información del sistema de información de la empresa.

Esta evaluación de controles a los procesos seleccionados y aprobados por la dirección de la empresa, se llevó a cabo en las

instalaciones localizadas en Quito y Cumbayá, cubriendo los departamentos de gerencia de general, gerencia de ventas, gerencia de fábrica, contabilidad, recursos humanos, diseño, asistencia de gerencia, asistencia de contabilidad, recepción y producción.

La auditoría se realizó con el apoyo de los estándares de Auditoría y Aseguramiento de los Sistemas de Información y las directrices de auditoría y aseguramiento provistas por ISACA, además se alineó a estos estándares y guías junto con la norma internacional ISO/IEC 27001:2013 vigente en las normas del Ecuador para temas de Seguridad de la Información. Estos estándares han requerido que se lleve una planificación de la auditoría que permita obtener la suficiente, pertinente y válida evidencia que permita proporcionar una base razonable para la respectiva declaración de conclusiones, opiniones y hallazgos de la auditoría.

Es pertinente aclarar que el ámbito de la aplicación de la auditoría se encuentra limitada al examen de los controles en los procesos seleccionados y todos los elementos catalizadores exclusivamente en relación con los temas de seguridad de la información que se establece en los procesos identificados de alto riesgo de la empresa. Este análisis se determinó en acuerdo con la dirección de la empresa Cocinas Internacionales. La auditoría a los procesos identificados se desarrollo en base al Producto de ISACA, Cobit 5 para la Seguridad de la Información, que es una extensión especializada de línea de productos de COBIT 5.

4.4. Objetivos de la Auditoría

El objetivo principal de esta auditoría fue evaluar la condición actual del Sistema de Información de la empresa Cocinas Internacionales a través del marco metodológico de gestión de las TI y el Negocio, COBIT V5, para conocer las debilidades y riesgos a los que se encontraría expuesta la información corporativa.

Para cumplir el objetivo principal de esta auditoría ha sido necesario establecer los objetivos específicos que nos permitan alcanzar lo requerido, dentro de lo cual se ha determinando que para ello se debe iniciar con la realización de una selección previa de los procesos prioritarios a ser evaluados según la base de conocimiento de COBIT V5, a través de la utilización de la Cascada de metas que establece el Marco Metodológico de COBIT V5, el mismo que ha sido trabajado y evaluado con la contribución del personal de la empresa de Cocinas Internacionales.

Otro de los objetivos específicos de esta auditoría fue la respectiva elaboración del plan de investigación de campo, que permita al auditor llegar a un conocimiento y comprensión de la empresa, para de esta forma permitir el desarrollo de la auditoría mediante la respectiva recolección de información relevante.

Es objetivo de esta auditoría la respectiva elaboración de los instrumentos de investigación de campo que se ajusten a la obtención de los resultados deseados en el proceso de auditoría, sin que se presten a ser ambiguos. El análisis de resultados obtenidos mediante la correcta aplicación de los instrumentos de recolección de la información que se incluyan al enfoque requerido en la auditoría.

Como un objetivo final de esta auditoría es la elaboración, presentación y lectura del respectivo informe al personal interno de la empresa Cocinas Internacionales para su respectivo análisis, corrección y observaciones finales que contribuyan al apoyo del mejoramiento de su sistema de información en términos de seguridad de la información.

4.5. Metodología de la Auditoría

La metodología empleada para este trabajo se baso en la auditoría basada en riesgos (ABR), que ha consistido en las etapas que se procederá a describir a continuación:

4.5.1. Primera Fase

Contacto con el interesado en la empresa, en este caso práctico fue el Ingeniero Jairo Ron, Gerente de fábrica de la empresa Cocinas Internacionales, con quien se mantuvo una reunión, en la cual se indicó el trabajo que se desarrollaría en la empresa, que consistía en la Auditoría Informática al Sistema de Información de la empresa, enfocado a la seguridad de la Información, de la misma manera se formalizó los objetivos y el alcance de este trabajo.

En entrevistas posteriores se procedió a realizar una definición general del entorno que se involucraría en la auditoría, en esta etapa se recopiló la información a través de entrevistas y documentación formalmente emitida por la empresa para comprensión de su contexto y actividades de negocio, toda la información permitió comprender de una mejor manera las actividades de la empresa, su entorno de negocio, su estructura, además de su filosofía corporativa, esta se constituyó en la información de partida para iniciar el trabajo con el marco de gobierno y gestión de las tecnologías de la información y el negocio de COBIT 5.

La información de la empresa se alineó a las condiciones de adaptación de COBIT 5. Utilizando la cascada de metas que permitió la construcción de las diferentes matrices que entregaron el conocimiento de los diferentes procesos críticos identificados en cada dominio de Cobit 5 para la empresa Cocinas Internacionales. Estos procesos fueron revisados, verificados y aceptados por la Gerencia de Fábrica.

Una vez aceptados los procesos que se auditarían en la empresa, se trabajo en el diseño de una planificación de auditoría donde se identificó las prácticas de gestión a evaluar de acuerdo a las guías de Cobit 5, que ofrece en su producto de Seguridad de la información.

4.5.2. Segunda Fase

Se presentó a la Gerencia de Fábrica de Cocinas Internacionales una planificación para el cumplimiento del programa de auditoría a los procesos más críticos de la empresa en relación a la seguridad de la información, el cual contenía la definición de las herramientas a utilizar para la respectiva recopilación que serviría como evidencia de los resultados obtenidos de la auditoría, este programa fue revisado y autorizado sin modificación por la Gerencia de Fábrica de Cocinas Internacionales.

Se construyó cada instrumento a utilizar en la recolección de información para la auditoría en la evaluación de los diferentes procesos de Cobit 5 en la empresa. Se consideró que los principales instrumentos de recolección de información para esta actividad fueron: la entrevista, el cuestionario, la observación directa, las pruebas de cumplimiento y la revisión documental.

Una vez establecido y autorizado el programa de auditoría con sus respectivos instrumentos de recolección de información se procedió a cumplir con el calendario establecido en el programa para la recolección de la información requerida en la evaluación de la seguridad de la información. Los instrumentos para la recolección de la información se relacionaron a la existencia y verificación de la existencia de un sistema de gestión de seguridad de la información, de acuerdo a como se establece en la Norma Internacional ISO/IEC 27001:2013 para el diseño de un Sistema de Gestión de Seguridad de la Información y conforme a las orientaciones que se establece en la guía de Cobit 5 para la Seguridad de la Información.

4.5.3. Tercera Fase

La siguiente etapa de esta auditoría dio lugar al análisis de la información obtenida de cada proceso, donde se hizo referencia a la evaluación de la capacidad del proceso enfocado a las seguridades de la

información para determinar el grado de cumplimiento de los propósitos de cada uno.

Con la información analizada se procedió a la construcción del informe que contiene el detalle de los hallazgos y evidencias detectadas en la empresa, para lo cual se detalla por cada hallazgo, un criterio que se apoya y respalda en la base de conocimiento de ISACA en las publicaciones realizadas de COBIT 5 para la seguridad de la información, también se determina la condición en la que se encontró el hallazgo, la causa de su condición y se entrega las recomendaciones para mejorar e integrar las soluciones previstas para la empresa a fin de fortalecer la seguridad de la información en su sistema de información por cada proceso.

4.6. Resultados o Hallazgos de la Auditoría

En el siguiente apartado se procederá a explicar de una manera detallada los resultados de la auditoría realizada a la empresa Cocinas Internacionales, en conformidad con cada uno de los procesos resultantes de COBIT V5 para la empresa, definidos como procesos críticos en base a la seguridad de la información.

4.6.1. EDM01: Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno

Hallazgo 1: No existe evidencia de un marco de referencia de gobierno de seguridad de la información.

Criterio: “EDM01.01 Evaluar el sistema de gobierno. Identificar y comprometerse continuamente con las partes interesadas de la empresa, documentar la comprensión de los requerimientos y realizar una estimación del actual y futuro diseño del gobierno de Tecnologías de la Información (TI) de la empresa.

EDM01.02 Orientar el sistema de gobierno. Informar a los líderes y obtener su apoyo, su aceptación y su compromiso. Guiar las estructuras,

procesos y prácticas para el gobierno de TI en línea con los principios, modelos para la toma de decisiones y niveles de autoridad diseñados para el gobierno. Definir la información necesaria para una toma de decisiones informadas.

EDM01.03 Supervisar el sistema de gobierno. Supervisar la ejecución y efectividad del gobierno de TI de la empresa. Analizar si el sistema de gobierno y los mecanismos implementados (incluyendo estructuras, principios y procesos) están operando de forma efectiva y proporcionan una supervisión apropiada de TI."[3]

Condición: La empresa no cuenta con un Sistema de Gestión para la Seguridad de la Información (SGSI), evidencia: respuesta del Gerente de Fábrica a la pregunta nro. 2 del cuestionario A.

Causa:

- La empresa posee un plan estratégico de negocio al que no se ha dado seguimiento desde el año 2008, esta documentación es el principal habilitador para el desarrollo de instrumentos que permiten una adecuada gestión del negocio, en consecuencia la empresa no cuenta con información que le permita definir un plan, para el gobierno de la seguridad de la información, además, el plan antes mencionado no cuenta con estrategias relacionadas al gobierno y/o gestión de tecnología de la información.
- La empresa no cuenta con los elementos necesarios de información que se requieren, tales como: planes, estrategias, informes, entre otros, los cuales permitan trabajar sobre la planificación de un gobierno de TI y de Seguridad de la Información.
- No existe ninguna evidencia de una gestión estratégica de la TI y de la seguridad de la información

[3] Cobit 5 an ISACA Framework, ISACA, *COBIT 5 para la Seguridad de la Información*, Rolling Meadows, IL 60008 EE.UU., 2012, p.71.

Efecto:

- La seguridad de la información no se considera como una capacidad estratégica de TI y del Negocio de la empresa
- Riesgo de alto impacto, no puede garantizar la efectividad de controles internos y externos, que mantengan niveles aceptables de riesgos relacionados con la seguridad de la información, tales como: fraudes, fuga de información, pérdida total de información ante la materialización de desastres, control de cumplimiento legal y regulatorio para el uso de programas software, acceso no autorizado a la información, entre otros.
- Inversiones y esfuerzos requieren mayores recursos económicos para mitigar las amenazas que se presenten
- Implementación de soluciones no planificadas afectan el presupuesto general de la empresa.

Recomendaciones:

En base al resultado obtenido de la auditoría al proceso EDM01. Asegurar el Establecimiento y Mantenimiento de un Marco de Gobierno enfocado a las Seguridad de la Información, se recomienda a la dirección de la empresa, considerar de manera inmediata, la responsabilidad de delegar el encargo para la realización de las siguientes actividades a los recursos humanos idóneos:

- Realizar la actualización de la información estratégica de la empresa, en donde se debe prever la incorporación de las estrategias de TI y sus objetivos de manera que puedan ser medidos y evaluados para garantizar el cumplimiento de metas.
- Incorporar el diseño, la implementación y mantenimiento de un Sistema de Gestión de las TI, para lo cual se recomienda tomar como referencia la guía que ofrece COBIT 5 para la gestión de las tecnologías de la información y el negocio, este marco metodológico

posee una gran capacidad de adaptación a empresas de todo tamaño y de todo ámbito para una gestión tecnología alineada a las estrategias del negocio.

- Desarrollar el diseño para la implementación de un sistema de gestión para la seguridad de la información (SGSI), orientado y supervisado, para lo cual se recomienda tomar en cuenta las directrices que establece COBIT 5 para la Seguridad de la Información, considerando además el modelo de diseño para un Sistema de Gestión de la Seguridad de la Información establecido en la norma internacional ISO/IEC 27001:2013, que indica los aspectos claves que se deben definir para la planeación e implementación de un efectivo sistema de gestión para la seguridad de la información.
- Se recomienda a la empresa que para realizar un diseño de gobierno de las TI y de la Seguridad de la información se considere la contratación de un servicio externo para que pueda apoyar este proceso con el conocimiento y experiencia requerido, debido a que involucrar personal especializado en la nómina del personal de la empresa supondría un gasto más elevado y permanente, que la contratación del servicio de consultoría que es temporal. Lo recomendable seria contratar personal especializado en los temas de Seguridad de la Información separado del tema de TI

Toda la información que se genere para el diseño, implementación y supervisión de las TI y la seguridad de la información, debe estar debidamente documentada y disponible para el personal que se requiera, sujeta a evaluación, actualización y mejora.

4.6.2. EDM02: Asegurar la entrega de Beneficios

Hallazgo 2: No existe evidencia de programas para la optimización de valor orientados a la Seguridad de la Información.

Criterio: "EDM02.01 Evaluar la optimización de valor. Evaluar continuamente las inversiones, servicios y activos del portafolio de TI para determinar la probabilidad de alcanzar los objetivos de la empresa y aportar valor a un coste razonable. Identificar y juzgar cualquier cambio de directrices que necesite ser comunicado a la dirección ejecutiva para optimizar la creación de valor.

EDM02.02 Orientar la optimización del valor. Orientar los principios y las prácticas de gestión de valor para posibilitar la materialización del valor óptimo de las inversiones habilitadas por TI a lo largo de todo su ciclo de vida económico.

EDM02.03 Supervisar la optimización de valor. Supervisar los indicadores clave y sus métricas para determinar el grado en que el negocio está obteniendo el valor y los beneficios esperados de los servicios e inversiones habilitadas por TI. Identificar los problemas significativos y considerar las acciones correctivas. "[4]

Condición: De acuerdo a entrevista realizada al gerente de fábrica Ing. Jairo Ron, se detectó que la empresa no tiene evidencia de programas o planes que manejen el tema de inversiones enfocadas a las TI, ni de seguridad de la información. No existe ningún programa que gestione la optimización de valor.

Se detectó que la empresa solo tiene adquiridas licencias de las siguientes aplicaciones: JoseNet, Sistema de Corte y Kitchen Draw, el resto de aplicaciones no tiene respaldo de adquisición, además los equipos de la empresa tienen instalados los programas antivirus sin licencia y se encuentran infectados con software malicioso (virus), evidencia obtenida según la pregunta 6 del cuestionario de Evaluación de Cumplimiento para Equipos Informáticos.

---

[4] Cobit 5 an ISACA Framework, ISACA, *COBIT 5 para la Seguridad de la Información*, Rolling Meadows, IL 60008 EE.UU., 2012, p.73.

El respaldo manual que se lleva a cabo no es controlado, ni supervisado y tampoco tiene un criterio definido que sea adecuado en la clasificación de información, el empleado respalda lo que cree conveniente pero no tiene un modelo que establezca el patrón de respaldo a seguir, según lo confirma cuestionario de Verificación de Dispositivos y mecanismos de respaldo, de la pregunta 8 a la 13, contestadas por el Ing. Jairo Ron.

No existe ningún contrato en la empresa para el soporte de TI, existen programas instalados en los equipos de los cuales el usuario desconoce su propósito, esta evidencia se obtiene del documento de Captura de Información de los Equipos 1 y Equipo 4. La gestión tecnológica y de seguridad se hace de forma empírica y no posee ninguna evidencia de planificación.

Causa:

- No existe la información de apoyo que permita desarrollar un sistema para la gestión de las TI en la empresa, la gestión de la seguridad de la información.
- No existen programas o planes que permitan la gestión de riesgos.
- No se tiene definido los mecanismos de control que permitan verificar el software instalado en los equipos.
- No existe la definición formal de roles y actividades de los empleados.

Efecto:

- Gestión tecnológica se hace de forma empírica y no en base a una planificación, se observa que el recurso tecnológico no trabaja en función de apoyo a las estrategias del negocio de una manera eficiente y eficaz.
- Seguridad de la información resulta costoso, no es considerado para que trabaje con la finalidad de retornar una inversión adecuada a la empresa (en términos de ofrecer integridad, confidencialidad y disponibilidad de la información a costos óptimos), sino que más bien

representa un alto gasto que se exterioriza de forma imprevista, esto ha provocado que la empresa pierda beneficios en la optimización de valor relacionados al tema de TI y seguridad de la información.

- Exposición a riesgos altos en la operación de procesos de negocio, esto le representa un valor alto a la empresa que debe asumirse afectando el presupuesto general.
- Subutilización de los recursos TI y presencia de riesgos potenciales de seguridad
- La empresa no puede experimentar y conocer la forma en que las TI y la seguridad de la información pueden contribuir con el cuidado y el incremento de su cartera de inversiones.
- No existen parámetros que les permitan realizar una medición de eventos o incidentes relacionados con la seguridad de la información no deseada
- Solución de incidentes de seguridad de la información en la empresa no se hace de manera óptima, por lo que no es detectado y tratado, lo que se traduce en un escenario de riesgo de seguridad de la información ignorado.
- No se desarrolla planes que soporten la gestión de riesgos e incidentes de seguridad que permitan a la empresa conocer donde deben aplicar un mayor esfuerzo para mitigar la criticidad de riesgos de seguridad de la información, impidiendo que de esta manera sus esfuerzos y recursos sean orientados efectivamente en el ámbito de las inversiones.
- La empresa no considera la desventaja competitiva
- La empresa no tiene manera de garantizar la continuidad de las operaciones de negocio, tanto normales como críticas, ante la materialización de desastres naturales o incidentes de seguridad como: fuga, divulgación, pérdida de información, accesos no autorizados o indisponibilidad del sistema de información de la empresa, son problemas que se pueden presentar y la falta de

controles y mecanismos o programas de protección a los diferentes sistemas que conservan la información de la empresa como: diseños de productos, costos, facturación, contabilidad, nomina, inventario, etc. no preservan la seguridad de la información en los procesos diarios que el negocio efectúa.

- No posee programas de inversión en seguridad de la información
- Presenta problemas de incumplimiento con las leyes y regulaciones externas debido a que posee programas ilegales en los equipos que contribuyen con la actividad económica
- Ausencia de herramientas que colaboren y contribuyan a garantizar seguridad de la información: como firewalls, antivirus con funcionalidad completa, programas anti-spam, etc.,
- Falta de herramientas que mejoren el rendimiento de los equipos o protección de la información, razón por la que se encuentran varios equipos infectados con código malicioso, o reflejan problemas con el rendimiento no optimizado de los equipos.
- Omisión de políticas y supervisión en la administración de la red para acceso a la red, se requiere herramientas que permitan el monitoreo del tráfico de red de la empresa, que les ayude a determinar que la red mantiene un nivel manejable de riesgo contra ataques cibernéticos y mal uso del recurso interno, destinado a las actividades que no son de orden laboral.
- Privación de inversión en soluciones óptimas de respaldo hace que se ejecuten procesos manuales de alto riesgo para la conservación de su información, ante la materialización de desastres y pérdida total de la información, donde la empresa no tendría manera de recuperar la información completa del negocio, que es necesaria para restablecer sus actividades con normalidad.
- La condición actual representa una amenaza no controlada en la empresa, que es considerada de alto impacto porque tiene la capacidad de afectar las operaciones del negocio hasta dejarlo

inoperativo y puede llegar a comprometer fuertes cantidades económicas para el restablecimiento de las funciones y operaciones de negocio, además de verse involucrado en temas de orden legal.

Recomendación:

En base al resultado de la auditoría del proceso EDM02 Asegurar la Entrega de Beneficios enfocado a la Seguridad de la Información, se recomienda a la dirección de la empresa, trabajar en el desarrollo de un plan de inversiones tanto para el negocio, como para las TI y las Seguridades de la información. Cobit 5 tiene guías específicas en el proceso indicado para el trabajo de desarrollo del plan de inversiones de la empresa enfocadas tanto al negocio como de las TI que pueden ser adaptadas a las necesidades de la empresa.

Para el diseño para un plan de inversiones enfocado a la seguridad de la información se debe considerar las directrices de Cobit 5 para la Seguridad de la información, que debe contener al menos la siguiente información:

- Comprensión del contexto de la empresa, todas sus actividades y los requisitos de la dirección de la empresa
- Definición de manera formal los roles, funciones y actividades de los empleados que permitan fijar de una manera más organizada y efectiva, la asignación de recursos tecnológicos conforme a las necesidades que se requiera en cada rol, que dé lugar a la segregación de funciones, a fin de garantizar seguridad en la información.
- Definición de métodos adecuados que les permitan conocer o demostrar los valores de beneficio, es necesario crear metas y métricas del proceso, estas pueden ser adaptadas desde las metas y métricas del proceso EDM02 genéricas de acuerdo a lo que específica Cobit 5 para la seguridad de la información.

- Establecer los valores de beneficio, tanto económicos como no económicos, esta información debe considerar ser apoyada con la norma internacional ISO/IEC 27001:2013, ítem 6.1, Generalidades para la toma de acciones que permitan el tratamiento de riesgos y oportunidades en un sistema planificado para la gestión de la seguridad de la información.
- Disponer períodos de tiempo en donde los resultados y la obtención de beneficios sean informados apropiadamente a la dirección de la empresa, estos deben ser revisados, analizados, mantenidos, actualizados y mejorados, según sea considerado, para las necesidades de la empresa, tal como lo recomienda la norma internacional ISO/IEC 27001:2013, ítem 9.3 sobre Revisión de la Dirección.

Toda la información que se genere para la materia de inversiones enfocadas a la seguridad de la información, debe ser debidamente documentada y estar disponible para el personal que lo requiera, sujeta a evaluación, actualización y mejora.

4.6.3. EDM04: Asegurar la optimización de recursos

Hallazgo 03: No existe evidencia de que los recursos sean optimizados.

Criterio: “EDM04.01 Evaluar la gestión de recursos. Examinar y evaluar continuamente la necesidad actual y futura de los recursos relacionados con TI, las opciones para la asignación de recursos (incluyendo estrategias de aprovisionamiento) y los principios de asignación y gestión para cumplir de manera óptima con las necesidades de la empresa.

EDM04.02 Orientar la gestión de recursos. Asegurar la adopción de principios de gestión de recursos para permitir un uso óptimo de los recursos de TI a lo largo de su completo ciclo de vida económica

EDM04.03 Supervisar la gestión de recursos. Supervisar los objetivos y métricas clave de los procesos de gestión de recursos y establecer cómo serán identificados, seguidos e informados para su resolución las desviaciones o los problemas.**"**[5]

Condición: No se encontró ninguna evidencia que indique que los recursos tecnológicos son optimizados, no existe evidencia de la existencia de planes de recursos aprobados que estén relacionados con la seguridad de la información, no hay evidencia de que existan estudios sobre las deficiencias de la empresa. En entrevista con el Gerente de Fábrica de la empresa, expresó que no tienen información sobre planes de optimización de recursos relacionados a la seguridad de la información, por lo que se evidencia que los recursos tecnológicos y de seguridad de la información operan de forma empírica y no planificada. Los usuarios/empleados de la empresa tienen libre acceso a las configuraciones de los equipos, esta evidencia se confirma a través del cuestionario: Pruebas de Cumplimiento para equipos informáticos en los equipos de gerencia de fábrica, contabilidad, asistencia a gerencia y diseño 1, pruebas que fueron contestadas por cada usuario de equipo, en la pregunta 2 de la sección de controles técnicos indicaron no tener ninguna restricción de acceso al equipo teniendo perfiles de administrador.

No existe evidencia de controles que permita deshabilitar a los usuarios no autorizados en la manipulación a las configuraciones de los equipos, tampoco existe la evidencia de controles que limiten la instalación de aplicaciones potencialmente peligrosas, que son descargadas directamente a través de internet.

Causa:

- Plan estratégico desactualizado

[5] Cobit 5 an ISACA Framework, ISACA, *COBIT 5 para la Seguridad de la Información*, Rolling Meadows, IL 60008 EE.UU., 2012, p.77.

- No existe ninguna planificación para la gestión y optimización de recursos tanto de TI como de seguridad de la información.
- No existen estudios donde se determinen las deficiencias de la empresa en cuanto a retorno de beneficios.

Efecto:

- La empresa no obtiene el máximo provecho de sus recursos debido a que no conoce la capacidad de los recursos que usa.
- Presenta evidentes inconvenientes de subutilización de recursos (aplicaciones, equipos, configuraciones de equipos, configuración de red) como se evidencia, un ejemplo se detecta en el sistema contable, en el cual existen varios módulos que no son utilizados, se desconoce si esta condición se debe a que los módulos no son aplicables al entorno o no se ajustan a los requerimientos de la empresa, esto supone un desperdicio para la empresa, ya que paga por la funcionalidad completa de la aplicación y no la aprovecha al máximo, perdiendo valor en la optimización del sistema.
- Procesos como la adquisición de los recursos únicamente está pensada para la solución de problemas de orden administrativo eventual y es debido a esto que no se ha concebido que actualmente la información y su adecuada gestión para la seguridad de la información deben estar integradas en todos los ámbitos de la empresa, esta práctica no es suficiente para optimizar sus recursos.
- La optimización actualmente no es posible en la empresa, una de estas razones es que la empresa no tiene definido los perfiles y roles específicos del personal, lo que dificulta la asignación de recursos adecuados que estén acorde a las funciones de cada uno.
- Desconocimiento de características que debe poseer determinado recurso para ajustarse a la necesidad de rol del empleado a fin de no caer en la subutilización de recursos.

- El rendimiento de los equipos no es el óptimo, una de las razones se debe a que el libre acceso a la red permite a los usuarios descargar archivos o aplicaciones, que pueden afectar seriamente el recurso tecnológico y debido a ello se tiene equipos informáticos infectados, pese a contar con un antivirus, este a su vez no funciona completamente o se encuentra desactivado lo que contribuye a ignorar las advertencias de seguridad.
- Ausencia de controles internos para el manejo del recurso informático
- No existe el manejo de perfiles de usuarios y como consecuencia se entrega privilegios de uso global en los equipos, lo que ha provocado el uso de recursos sin ningún compromiso de responsabilidad, los usuarios tiene la capacidad de desactivar fácilmente los programas como antivirus o el mismo firewall que tienen como propósito proteger la información de la empresa que se encuentra en los equipos y la información que circula por las redes internas y externas de ataques, esto perjudica el negocio afectando el rendimiento de los equipos.
- Exposición de alto impacto, debido a que pierde valor en la percepción de beneficios, presencia de códigos maliciosos tanto en equipos como en los dispositivos previstos eventualmente para almacenamiento de respaldos, que al ser conectados a equipos infectados de virus atacan directamente la información ocultándola y provocando daños permanentes, que no sean susceptibles de recuperación y que dejan expuesta a un peligro potencial la información ante una materialización de desastres, la empresa sería afectada al perder la capacidad de recuperación de información clave para reactivar el funcionamiento de la misma.

Recomendación:

En base al resultado de la auditoría del proceso EDM04 Asegurar la Optimización de Recursos enfocado a la Seguridad de la Información, se recomienda a la dirección de la empresa, trabajar en el desarrollo de planes

que permitan la optimización de recursos conforme a la guía que ofrece Cobit 5 para la seguridad de la información, para ello es recomendable implementar la participación de los siguientes elementos:

- Elaboración de Inventarios de Equipos (Hardware) y Programas (Software) instalado en la empresa
- Realizar la formalización de roles y funciones para asignación de recursos TI adecuados a la función requerida, evaluando las capacidades de equipo y paquetes de software requerido
- Elaborar estudios de deficiencias de la infraestructura empresarial en el entorno de seguridad de la información
- Diseñar programas que permitan la evaluación de la seguridad de la información, en cuanto a suministros, formación, concienciación y competencias de los recursos
- Elaborar planes de diseño para la optimización de recurso que posean métricas, que permitan a la dirección medir la eficacia, eficiencia y capacidad relacionada a la Seguridad de la Información, se puede tomar como referencia, las métricas planteadas de manera genérica por Cobit 5 para la seguridad de la información o utilizar las mismas como una referencia o modelo para plantear las métricas apropiadas de la empresa.

Toda la información que se genere en el entorno de optimización de recursos tanto de TI como para la seguridad de la información, deberá estar debidamente documentada, revisada, aprobada y disponible para quien lo solicite.

4.6.4. APO02: Gestionar la Estrategia

Hallazgo 04: No existe evidencia de que se esté gestionando la Estrategia enfocada a la Seguridad de la Información.

Criterio: "APO02.01 Comprender la dirección de la empresa. Considerar el entorno actual y los procesos de negocio de la empresa, así

como la estrategia y los objetivos futuros de la compañía. Tomar también en cuenta el entorno externo a ella (catalizadores de la industria, regulaciones relevantes, bases para la competencia).

APO02.02 Evaluar el entorno, capacidades y rendimiento actuales. Evaluar el rendimiento de las actuales capacidades internas de negocio y de TI, así como el de los servicios externos de TI; y desarrollar una perspectiva de la arquitectura empresarial en relación a TI. Identificar los problemas que se están experimentando y generar recomendaciones en las áreas que pueden beneficiarse de estas mejoras. Considerar los aspectos diferenciadores y las opciones de los proveedores de servicios, y el impacto financiero, los costes y beneficios potenciales de utilizar servicios externos.

APO02.03 Definir las capacidades objetivo para TI. Definir las capacidades objetivo para el negocio y para TI y los servicios de TI necesarios. Esto debería estar basado en el entendimiento del entorno empresarial y sus necesidades; en la evaluación de los actuales procesos de negocio, el entorno de TI y los problemas presentados; considerando los estándares de referencia, las mejores prácticas y las tecnologías emergentes validadas o propuestas de innovación.

APO02.04 Realizar un análisis de las deficiencias. Identificar las diferencias entre el entorno actual y el deseado y considerar el alineamiento de activos (las capacidades que soportan los servicios) con los resultados del negocio para optimizar la inversión, y la utilización de la base de activos internos y externos. Considerar los factores críticos de éxito que apoyan la ejecución de la estrategia.

APO02.05 Definir el plan estratégico y la hoja de ruta. Crear un plan estratégico que defina, en cooperación con las partes interesadas relevantes, cómo los objetivos de TI contribuirán a los objetivos estratégicos de la empresa. Incluyendo cómo TI apoyará el programa aprobado de inversiones, los procesos de negocio, los servicios y los activos de TI.

Orientar las tecnologías para definir las iniciativas que se requieren para cubrir las diferencias, la estrategia de abastecimiento y las medidas que se utilizarán para supervisar el logro de los objetivos, para dar prioridad a las iniciativas y combinarlas en una hoja de ruta a alto nivel."[6]

Condición: La empresa ha presentado la evidencia documental de la existencia de un plan de mejoramiento estratégico para la empresa con vigencia del año 2005 al 2008, no existe ninguna documentación adicional, y según el gerente de fábrica, la empresa no cuenta con ninguna otra documentación que soporte el apoyo de TI en la empresa ni de la seguridad de la información. La empresa no tiene los instrumentos necesarios que le permitan afrontar los temas de seguridad de la información de manera que se encuentre establecido entre las estrategias del negocio involucrando a las TI y por consiguiente la Seguridad de la Información.

Causa:

- Instrumentos de apoyo para la generación de planes, modelos, estrategias, entre otros, no se encuentra actualizados, así como tampoco se tiene sustento de que se le ha dado seguimiento hasta el año 2008.

Efecto:

- Desconocimiento de las necesidades de integridad, confidencialidad y disponibilidad de la información.
- Ejecución de actividades diarias sin garantía de seguridad.
- Deficiencia en la estrategia de comunicación para orientar a los empleados sobre una cultura que tenga conciencia en la generación, uso, almacenamiento y eliminación de la información responsable.
- Desconocimiento del valor real de la información en el negocio, la empresa que conoce el valor de su información invierte esfuerzos en

[6] Cobit 5 an ISACA Framework, ISACA, *COBIT 5 para la Seguridad de la Información*, Rolling Meadows, IL 60008 EE.UU., 2012, p.87.

protegerla porque reconoce que es el recurso que le brinda ventaja competitiva, no así Cocinas Internacionales evidencia la falta de esfuerzos en la protección de información debido al desconocimiento de su valor.

- Desconoce la información que requiere protección
- Desconoce el valor de inversión en la protección de la información, razón que deriva a que no se establezca las acciones y recursos necesarios (tecnológicos y humanos) que tengan el propósito de generar los instrumentos, herramientas, mecanismos, controles y personal, necesarios para el cumplimiento y supervisión que contribuya al mejoramiento continuo, que se convierta en una ventaja competitiva, que retorne beneficios a todas las partes interesadas del negocio, tanto internas(empleados, gerentes, administradores) como externas(clientes, proveedores)
- La carencia de la gestión estrategia de la seguridad de la información impide la definición de varios elementos que provean garantía de seguridad de la información como el establecimiento de normas, políticas, personal de supervisión, etc.
- No garantiza integridad en la información debido a que no existen controles, normas, principios, ni personal que supervise el cumplimiento de las normativas de integridad, la empresa no maneja ningún sistema de encriptación para la generación, envió y publicación de información a terceros, la misma puede ser modificada por el personal o software malicioso sin que las autoridades pertinentes tengan conocimiento.
- El libre acceso a los equipos informáticos sin asignación de usuarios y perfiles hace que cualquier usuario tenga acceso a todos los recursos de los equipos donde la información es almacenada y generada lo que provoca que la misma sea fácilmente, extraída, modificada y hasta eliminada, sin un adecuado control y asignación formal de responsables en la custodia de información.

- La empresa no realiza ninguna clasificación de información según el impacto que puede representar para el negocio, la pérdida de la misma.
- No se tiene identificada que información debe ser considerada confidencial y cual no, logrando en este punto dejar toda información de manejo público, que tiene el riesgo de ser fácilmente divulgada sin establecer sanciones y responsables de la custodia de la información.
- La disponibilidad de la información se maneja bajo un concepto que implica alto riesgo en la empresa, debido a que se tiene la percepción de que esta debe estar disponible en todo momento para todos, lo cierto es que el criterio de disponibilidad difiere un poco debido a que esta debe estar disponible según sea requerido y autorizado en el momento oportuno.
- El personal está en contacto con toda la información de toda la empresa o de la gran parte de estaciones de trabajo lo que implica un alto riesgo, porque esta disponibilidad de información sin perfiles y responsabilidades, provoca que la información pueda ser sustraída, modificada, eliminada y divulgada a terceros no autorizados. Como un ejemplo se puede mencionar que el contador de la empresa fácilmente accede al computador de la auxiliar de contabilidad que también tiene funciones de recursos humanos en la empresa, el mismo equipo almacena información sensible de las dos áreas, al contador solo le interesa acceder a los recursos e información explicitas a su rol, pero por el contrario tiene acceso a la información sensible de Recursos Humanos, que pueden ser afectados.
- Todo el personal puede usar el equipo que conserva los diseños de los productos que no tienen ninguna protección o aplicación especial de lectura, estos pueden ser fácilmente leídos y sustraídos, lo que puede incurrir en la entrega de información de diseños nuevos a otras instituciones dedicadas a la misma actividad generándole a la empresa pérdida, debido a una competencia desleal.

- Esta vulnerabilidad expone a la empresa a un nivel de riesgo alto, ya que afecta seriamente la supervivencia del negocio.

Recomendación: En base al resultado obtenido de la auditoría al proceso APO02 Gestionar la Estrategia enfocado a la Seguridad de la Información, se recomienda a la dirección de la empresa desarrollar el plan estratégico de seguridad de la información ya que este proveerá la visión de lo que la empresa requiere para lograr con el cumplimiento de las metas de seguridad, las cuales deberán estar alineadas a las metas estratégicas de TI y del Negocio. Este plan estratégico de seguridad puede ser construido en base a las guías y orientaciones que provee COBIT 5 para la seguridad de la información, el cual se puede adaptar a las necesidades de la empresa, se recomienda establecer en el desarrollo de esta planificación estratégica la siguiente información:

- Comprensión y definición de cómo la seguridad de la información afecta las operaciones del negocio y su importancia en la empresa
- Disponer de forma obligatoria, el cumplimiento de normativa legal externa como: Protección de Datos, propiedad Intelectual y comercio electrónico, entre otros relacionados a la seguridad de la información
- Se recomienda fijar calendarios de evaluación de la estrategia, para verificar cumplimiento y eficiencia de las metas, métricas y resultados del proceso que deben estar bajo el conocimiento de la dirección.

Este proceso es apoyado con otros elementos que se debe considerar, para ello se recomienda lo siguiente:

- Definir la arquitectura empresarial para determinar su alineación a la estrategia de seguridad de la información
- Desarrollar del plan de gestión de riesgos de TI y relacionados a la seguridad de la información de manera que se pueda establecer la necesidad de gestionar el Riesgo relacionado a la seguridad de la información

- Previo establecimiento de políticas de seguridad de la información, se deberá realizar la definición de controles eficientes que se ajusten a la realidad de la empresa mitigando el riesgo en caso de materialización o ante entornos que brinden poca confianza para la seguridad de la información. La empresa debe apoyarse de la norma internacional ISO/IEC 27001:2013, Ítem 5.2 sobre políticas, que permitirán apoyar la gestión estrategia de la empresa en términos de seguridad de la información.
- Considerar las técnicas adecuadas para la construcción de sistemas de gestión para la seguridad de la información con sus requisitos, basados en la norma ISO/IEC 27001:2013

Toda la información que se genere para el proceso debe estar debidamente documentada, disponible y actualizada para quien lo requiera, para efectos de información, evaluación y retroalimentación para mejora continua del proceso. Se recomienda tomar en cuenta la recomendación para la divulgación de la información de seguridad de la información de la empresa a las personas autorizadas y hacerlo de forma segura y completa tal como recomienda la misma norma ISO/IEC 27001:2013, Ítem 7.4 sobre Comunicación.

4.6.5. APO03: Gestionar la Arquitectura Empresarial

Hallazgo 05: No existe evidencia de que la empresa tenga una arquitectura empresarial.

Criterio: "APO03.01 Desarrollar la visión de la arquitectura de empresa. La visión de la arquitectura proporciona una primera descripción de alto nivel de las arquitecturas de partida y objetivo, cubriendo los dominios de negocio, información, datos, aplicaciones y tecnología. La visión de la arquitectura proporciona al promotor la herramienta clave para vender los beneficios de la capacidad propuesta a las partes interesadas de la empresa. La visión de la arquitectura describe cómo las nuevas capacidades

permitirán alcanzar las metas de la empresa y los objetivos estratégicos y considera las preocupaciones de las partes interesadas en su implementación.

APO03.02 Definir la arquitectura de referencia. La arquitectura de referencia describe la situación actual y el objetivo de la arquitectura para los dominios negocio, información, datos, aplicaciones y tecnología

APO03.03 Seleccionar las oportunidades y las soluciones. Racionalizar las desviaciones entre las arquitecturas de referencia y objetivo, considerando tanto la perspectiva técnica como la del negocio y agrupándolas en paquetes de trabajo de proyecto. Integrar el proyecto con todos los programas de inversiones relacionados con TI para asegurar que las iniciativas relacionadas con la arquitectura estén alineadas y que, estas iniciativas, sean parte del cambio general en la empresa. Hacer de ello un esfuerzo en colaboración con las partes interesadas clave de la empresa y en TI para evaluar el grado de preparación de la empresa para su transformación e identificar oportunidades, soluciones y todas las restricciones de la implementación.

APO03.04 Definir la implementación de la arquitectura. Crear un plan de implementación y de migración viable, acorde con la cartera de proyectos y programas. Asegurar que el plan está estrechamente coordinado para asegurar que se aporta valor y se disponen de los recursos necesarios para finalizar los trabajos.

APO03.05 Proveer los servicios de arquitectura empresarial. La provisión de los servicios de arquitectura de empresa incluye la guía y supervisión de los proyectos a implementar, la formalización de las maneras de trabajar mediante los contratos de arquitectura, la medición y

comunicación del valor añadido por la arquitectura y la supervisión del cumplimiento."[7]

Condición: La empresa no ha presentado evidencia que indique la arquitectura de la empresa. La arquitectura de la empresa se ha establecido de forma empírica y se desconoce su composición y distribución.

Causa:

- No existe un sistema de gobierno TI que gestione los recursos tecnológicos relacionados a seguridad de la información.

Efecto:

- Impedimento para la realización de inversiones programadas que beneficien al negocio en cuanto a los recursos tecnológicos y la seguridad de la información.
- Arquitectura formal no establecida, lo que lleva a las tecnologías a trabajar sin funciones, ni propósitos específicos.
- Las tecnologías no soportan y no contribuyen con el cumplimiento y alcance de las iniciativas del negocio de una manera eficaz, eficiente y aun coste óptimo.
- Desconocimiento del impacto que se tiene tras cada estrategia de negocio que se implemente, en la que intervienen los recursos de TI, ya que no considera que las TI y la seguridad de la información se deben acoplar al negocio según las estrategias.
- Presenta un problema de orden competitivo en los mercados. Actualmente las empresas deben adaptar las nuevas tecnologías a las necesidades de la empresa para fortalecer y proteger sus negocios, sin embargo, Cocinas Internacionales actualmente se encuentra con una gran desventaja, ya que presentaría serios problemas al momento de acoplarse a un entorno cambiante

[7] Cobit 5 an ISACA Framework, ISACA, *COBIT 5 para la Seguridad de la Información*, Rolling Meadows, IL 60008 EE.UU., 2012, p.91.

tecnológico, que busca cada día generar mejores oportunidades para el retorno de inversiones a través de beneficios que incrementen su cadena de valor a productos y servicios.

- La empresa no está preparada en este contexto para afrontar temas de innovación tecnología que le permitan mantenerse a la vanguardia de soluciones tecnológicas que se adapten a un entorno tan cambiante como lo es el entorno de los negocios e intervención de procesos de producción.
- La empresa ahora mismo no está en capacidad de afrontar proyectos de Innovación Organizacional, reestructuración tanto administrativa o la de gestión de negocios.
- Limitación del potencial de la empresa, no entrega una visión integrada y coherente de sus TI, revelando falencias de seguridad de alto riesgo sobre las que no se dedican esfuerzos para mitigar su efecto.
- Impedimento para la realización de la optimización de recursos ya que se desconoce como explotar el potencial de los recursos adquiridos a fin de brindar mejores y mayores beneficios.
- No existe ninguna garantía de funcionalidad, por lo que se considera de alto impacto debido a que está expuesta que en cualquier momento fallen estaciones de trabajo como: el servidor de internet, el equipo destinado a gerencia, el equipo destinado de diseño de modulares, el equipo de contabilidad entre otros, los cual exponen a la empresa a escenarios de grandes pérdidas económicas, sin tomar en cuenta que las operaciones de negocio podrían quedar inoperativas
- Búsqueda de soluciones temporales, lo cual le cuesta más a la empresa, debido a que no podría considerar soluciones definitivas porque no puede prever que sean óptimas para la arquitectura empírica que actualmente manejan.

Recomendaciones:

En base al resultado obtenido de la auditoría del proceso APO03 Gestionar la Arquitectura empresarial enfocado a la Seguridad de la Información se recomienda a la dirección de la empresa Contratar el servicio de asesoría de TI externo que permita establecer de manera formal la arquitectura empresarial que sostiene TI en el empresa, considerando lo recomendado en COBIT 5 para el proceso de la arquitectura empresarial. Este diseño de arquitectura empresarial, debe contar con:

- Definición de las metas, métricas y procedimientos de evaluación
- Información sobre las buenas prácticas tomadas como referencia para la construcción de la arquitectura TI de la empresa
- Más detalles sobre el diseño y construcción de la definición de la arquitectura empresarial, estos detalles pueden ser estudiados desde Cobit 5 en el proceso de la gestión de la arquitectura empresarial y adaptarlo a su entorno según sea necesario.

Además se recomienda la contratación de un servicio de asesoría para la seguridad de la información con fines de gestión de la arquitectura empresarial definida con el enfoque de seguridad de la información. Es recomendable que la gestión de la arquitectura empresarial con enfoque a las seguridades de la información sea estructurada en base a las guías que ofrece COBIT 5 para la seguridad de la información, el diseño de esta arquitectura empresarial enfocada a la seguridad de la información debe contar con:

- Definición de la visión de la arquitectura de la empresa: objetivos, requisitos, propuesta de valor
- Generar información que involucre las carencias y oportunidades de soluciones, tomando en cuenta la valoración de riesgo que debe encontrarse a un nivel manejable para los temas que intervengan en la seguridad de la información.

- Elaborar planes de inversión de soluciones y optimización de recursos que mantengan una relación directa al diseño de una arquitectura empresarial contribuyendo a la mejora continua de la operación de sus servicios.
- Generar informes periódicamente, que reporten la entrega de beneficios requeridos sobre las soluciones adquiridas en la arquitectura empresarial, dirigidas al conocimiento de la dirección de la empresa

Toda la información que se genere del proceso, debe estar debidamente documentada, revisada, aprobada, actualizada y disponible para el personal que lo requiera con fines de información, verificación y supervisión.

4.6.6. APO04: Gestionar la innovación

Hallazgo 06: No existe evidencia de que la empresa gestione la innovación orientada a la seguridad de la información.

Criterio: "APO04.01 Crear un entorno favorable para la innovación. Crear un entorno que sea propicio para la innovación, considerando la cultura, la gratificación, la colaboración, los foros tecnológicos y los mecanismos para promover y captar ideas de los empleados.

APO04.02 Mantener un entendimiento del entorno de la empresa. Trabajar junto a las partes interesadas relevantes para entender sus retos. Mantener un entendimiento adecuado de la estrategia corporativa y del entorno competitivo, así como de otras restricciones de modo que las oportunidades habilitadas por las nuevas tecnologías puedan ser identificadas.

APO04.03 Supervisar y explorar el entorno tecnológico. Realizar una supervisión sistemática y una exploración del entorno externo a la

empresa para identificar tecnologías emergentes que tengan el potencial de crear valor (por ejemplo, materializando la estrategia corporativa, optimizando costes, evitando la obsolescencia y habilitando de una mejor manera los procesos corporativos y de TI). Supervisar el mercado, la competencia, sectores industriales y tendencias legales y regulatorias para poder analizar tecnologías emergentes o ideas innovadoras en el contexto empresarial

APO04.04 Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras. Analizar las tecnologías emergentes identificadas y/u otras sugerencias de innovación TI. Trabajar con las partes interesadas para validar los supuestos sobre el potencial de las nuevas tecnologías y la innovación.

APO04.05 Recomendar iniciativas apropiadas adicionales. Evaluar y supervisar los resultados de las pruebas de concepto y, si son favorables, generar recomendaciones para más iniciativas y obtener el soporte de las partes interesadas.

APO04.06 Supervisar la implementación y el uso de la innovación. Supervisar la implementación y el uso de las tecnologías emergentes durante la integración, adopción y durante todo el ciclo de vida económico para garantizar que se producen los beneficios prometidos y para identificar las lecciones aprendidas."[8]

Condición: Según entrevista con el gerente de la empresa, no se tiene un programa de innovación tecnológica que contribuya a la seguridad de la información. También se pudo determinar en base a observación directa y revisión de programas en 4 equipos aleatorios de la empresa que el personal no está capacitado de la manera correcta para proteger sus equipos, encontrando como evidencias, antivirus desactualizados y gratuitos, lo que implica que no poseen una funcionalidad completa de

[8] Cobit 5 an ISACA Framework, ISACA, *COBIT 5 para la Seguridad de la Información*, Rolling Meadows, IL 60008 EE.UU., 2012, p.93.

protección, y en casos específicos desactivados durante las jornadas laborales debido a configuraciones incorrectas de funcionamiento, adicional se detectó igualmente que el firewall del equipo no se encuentra activo, siendo esta una herramienta software predeterminada del sistema operativo Windows, diseñada igualmente para protección y seguridad de la información frente al tráfico de red. No existe una cultura orientada a la seguridad de la información, tampoco existen capacitaciones que orienten sobre el tema al personal

Causa:

- No existen planes que soporten una arquitectura empresarial
- No existen planes para la inversión orientadas a la seguridad de la información.
- No existe información sobre el presupuesto asignado a TI y Seguridad de la información

Efecto:

- Pérdida de beneficios que están inmersos en el ámbito económico debido a la falta de inversión en temas de innovación tecnológica por cuestiones de seguridad de la información
- No existe procesos de innovación, no es posible la mejora continua, en un mundo tan cambiante en el tema tecnológico, la innovación permite ampliar el margen de beneficios que percibe tanto la empresa como sus clientes.
- No tiene capacidad de competencia a través de la mejora continua y la innovación, esto resta la capacidad de agregar valor a los productos y servicios que ofertan.
- Pérdida de la funcionalidad en las herramientas tecnológicas utilizadas, no reciben el suficiente soporte de respuesta frente a riesgos de seguridad existentes y cada día afectan la seguridad de la información, violando las seguridades debido a tecnologías obsoletas.

- No hay lugar para la optimización de recursos sin innovación tecnológica. Un beneficio importante para toda organización es la optimización de riesgos que permita mitigar el impacto en caso de materialización.
- Cocinas Internacionales no tiene planes de innovación orientada a la seguridad de la información, lo que es un indicador de que la empresa está expuesta a riesgos de alto impacto, ya que no existen soluciones a través de la incorporación de opciones de innovación que ayuden a controlar estos problemas presentes en la empresa.
- Exposición a nivel alto de impacto debido a que cada día las empresas se enfrentan a nuevos retos en términos de seguridad y Cocinas internacionales no es una excepción, sin embargo, en caso de materialización de riesgos la implicación de seguridad puede afectar la operación de los procesos de la empresa dejándola inactiva o ser objeto de prejuicios de orden legal que afecten la imagen de la misma.

Recomendaciones: En base al resultado obtenido de la auditoría al proceso APO04 Gestionar la Innovación enfocado a la Seguridad de la Información, se recomienda a la dirección de la empresa trabajar en el desarrollo de planes de inversión enfocados a la seguridad de la información conforme lo considera Cobit 5 para la seguridad de la información, es importante indicar que los planes de inversión que se desarrollen en la empresa, deben estar relacionados directamente con la optimización de recursos y la entrega de beneficios procedentes de la gestión del portafolio.

El desarrollo de un plan para las inversiones debe considerar la participación del responsable de la gestión de TI de la empresa, el responsable de la gestión de Seguridad de la Información y el responsable del área financiera para los estudios de factibilidad económica, además de contar con la aprobación de la dirección de la empresa para la implementación de los planes de innovación.

Cabe recomendar que en el diseño de un plan de innovación enfocado a la seguridad de la información, se deberá tomar en cuenta los siguientes aspectos claves que se recomienda no dejar por fuera y que sean claramente definidos y especificados:

- Establecer un ambiente favorable para la inversión, a través de la inclusión de políticas y principios que respalden la innovación con el fin de gestionar el riesgo de la seguridad de la información.
- Definir cómo afecta la innovación relacionada a la seguridad de la información en la empresa, cuáles son sus oportunidades y cuáles son sus limitaciones.
- Realizar un análisis previo y posterior a la implementación de las soluciones tecnológicas que permitan conocer el impacto que tiene las mismas sobre la empresa, su capacidad de resultados, el equilibrio con el coste de adquisición justificado y los beneficios que persigue tras la implementación de un proceso coordinado de innovación enfocado a la seguridad de la información.
- Desarrollar estudios de factibilidad, identificando las tecnologías emergentes más apropiadas para el entorno del negocio y los beneficios que se espera retornar.
- Implementar actividades de seguimiento a los planes de inversión que permitan la retroalimentación del proceso para dar lugar a la mejora continua del proceso.
- Fijar las métricas que permitan evaluar que los planes y procesos de innovación, brinden un grado aceptable de satisfacción a la dirección de la empresa, para crear el interés adecuado a las partes interesadas.

Toda la información que se genere para el proceso de gestión de la innovación orientado a la seguridad de la información, deberá estar documentado, revisado, aplicado y actualizado, de manera que permita la verificación y supervisión de cumplimiento, disponible para quien lo solicite.

4.6.7. APO05: Gestionar el Portafolio

Hallazgo 07: No existe evidencia de que la empresa tenga un programa de gestión de portafolio orientado a la seguridad de la información.

Criterio: "**APO05.01 Establecer la combinación deseada de inversiones.** Revisar y garantizar la claridad de las estrategias y servicios actuales corporativos y de TI. Definir una adecuada combinación de inversiones, basada en los costes, la alineación con la estrategia y medidas financieras, tales como coste y retorno esperado de la inversión a lo largo de todo el ciclo de vida económico, grado de riesgo y tipo de beneficio para los programas del portafolio. Ajustar las estrategias corporativas y de TI cuando sea necesario.

APO05.02 Determinar la disponibilidad y las fuentes de fondos. Determinar las fuentes potenciales de fondos, las diferentes opciones de financiación y las implicaciones de las fuentes de financiación sobre las expectativas de retorno de la inversión.

APO05.03 Evaluar y seleccionar los programas a financiar. A partir de los requisitos de la combinación de inversiones del portafolio general, evaluar y priorizar casos de negocio de programas y decidir sobre las propuestas de inversión. Asignar fondos e iniciar los programas.

APO05.04 Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversión. Periódicamente, supervisar y optimizar, el rendimiento del portafolio de inversiones y de los programas individuales, a lo largo de todo el ciclo de vida de dichas inversiones.

APO05.05 Mantener los portafolios. Mantener los portafolios de programas y proyectos de inversión, servicios de TI y activos de TI.

APO05.06 Gestionar la consecución de beneficios. Supervisar los beneficios de proporcionar y mantener servicios y capacidades TI apropiadas, sobre la base del caso de negocio acordado en vigor. ”[9]

Condición: La empresa no cuenta con un portafolio orientado a la seguridad de la información.

Causa:

- Privación de programas de gestión de inversiones
- Ausencia de programas de gestión de la innovación hace que la empresa no pueda tener actualmente una gestión del portafolio
- Carencia de información que indique la combinación de inversiones, innovación y portafolio para asegurar la información

Efecto:

- Estaciones de trabajo poseen aplicaciones que no tiene ningún propósito laboral y hasta es desconocido el propósito por el usuario que lo maneja.
- Falta de control en el uso y manejo de aplicaciones que no tienen relación con las actividades de trabajo, son instaladas sin ninguna supervisión y autorización
- Contenido alto de programas potencialmente peligrosos para la operación del sistema de la estación y de la empresa
- Incumplimiento de normativa regulatoria por posesión de software ilegal, que no posee su respectivo respaldo de adquisición y uso, lo que implica un delito de propiedad intelectual y derechos de autor.
- Estaciones de trabajo tienen instalados programas de protección que no son completamente funcionales, debido a las restricciones que poseen las aplicaciones estás son descargadas o provistos desde páginas que ofertan programas gratuitos, sin garantía de

[9] Cobit 5 an ISACA Framework, ISACA, *COBIT 5 para la Seguridad de la Información*, Rolling Meadows, IL 60008 EE.UU., 2012, p.95.

funcionamiento que es lo que se requiere para el resguardo de la seguridad de la información de la empresa.

- La implementación de las TI y de la seguridad de la información no tienen un criterio basado en el análisis de las necesidades de la empresa, lo que provoca que se adquiera TI y de seguridad de la información sin ningún soporte definido para apoyar el entorno del negocio.
- La adquisición del portafolio tanto de TI como de Seguridad informática, no está inmerso en una actividad estratégica del negocio, esto genera que la empresa corra un alto riesgo de pérdida de la inversión
- No se cuenta con un inventario de aplicaciones de la empresa, por lo que se desconoce si las aplicaciones actualmente obtenidas en la empresa son suficientes para cumplir con el funcionamiento y protección de información de la empresa.
- No existe ningún informe que indique las evaluaciones de rendimiento de las aplicaciones ni de su propósito y condición.
- No se mide las necesidades tecnológicas de la empresa, por lo que se genera un desconocimiento, al saber si la tecnología actual usada es lo suficientemente robusta y completa para afrontar los retos del negocio.

Recomendaciones: En base al resultado obtenido de la auditoría al proceso APO05 Gestionar el Portafolio enfocado a la Seguridad de la Información, se recomienda a la dirección de la empresa seguir las orientaciones que brinda la guía de COBIT 5 para la seguridad de la información. Previa esta recomendación se invita a la dirección de la empresa a la realización de las siguientes actividades, que permitirán la obtención de los elementos de apoyo para la implementación adecuada del proceso:

- Realizar el inventario técnico del equipo informático y asignación de custodios de equipo e información contenida
- Realizar inventario de los programas contenidos en cada equipo y propósito de uso
- Realizar un estudio y análisis sobre los programas encontrados, evaluando su uso y propósito
- Definir con el estudio anterior los programas necesarios para suplir los roles del usuario para su actividad laboral
- Definición de perfiles de programas en los equipos que se asignan al personal
- Verificar la condición legal del portafolio de aplicaciones empresariales
- Establecer un plan estratégico de Inversiones combinadas con las necesidades del portafolio empresarial, considerando las oportunidades y riesgos
- Revisar la disponibilidad de fondos para la inversión en el portafolio de aplicaciones de la empresa, proyectar la regularización de licencias de aplicaciones de uso comercial y aplicaciones de protección de información, así como de monitoreo de red para una adecuada gestión.
- Disponer un programa enfocado de seguridad de la información
- Crear las métricas necesarias que permitan valorar el rendimiento y vigilancia de las garantías de seguridad de la información, teniendo en cuenta métricas que permitan valorar integridad, confidencialidad y disponibilidad de la información.

Toda la información que se genere del proceso debe quedar como constancia debidamente documentado, revisado, aprobado, actualizado y disponible para el personal que lo requiera con fines de información, verificación y supervisión.

4.6.8. APO08: Gestionar las Relaciones

Hallazgo 08: No existe evidencia de que la gestión de relaciones este formalizado ni orientado para el tema de seguridad de la información de la empresa

Criterio: "**APO08.01 Entender las expectativas del negocio.** Entender los problemas y objetivos actuales del negocio y sus expectativas para TI. Asegurar que los requisitos son entendidos, gestionados y comunicados, y su estado acordado y aprobado.

APO08.02 Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio. Identificar oportunidades potenciales para que TI sea catalizadora de un mejor rendimiento empresarial.

APO08.03 Gestionar las relaciones con el negocio. Gestionar la relación con los clientes (representantes del negocio). Asegurar que los roles y responsabilidades de la relación están definidos, asignados y que se facilita la comunicación.

APO08.04 Coordinar y comunicar. Trabajar con las partes interesadas y coordinar, de extremo a extremo, la entrega de los servicios de TI y las soluciones proporcionadas al negocio

APO08.05 Proveer datos de entrada para la mejora continua de los servicios. Mejorar y evolucionar continuamente los servicios basados en TI y la entrega del servicio a la empresa, para alinearlos con unos cambiantes requisitos de empresa y tecnológicos."[10]

Condición: La gerencia de la fábrica mediante entrevista manifestó que no se tiene ninguna estructura de relaciones para el manejo de los temas concernientes a seguridad de la información y se observó que el personal en general, no está familiarizado con la importancia y el

[10] Cobit 5 an ISACA Framework, ISACA, *COBIT 5 para la Seguridad de la Información*, Rolling Meadows, IL 60008 EE.UU., 2012, p.103.

cumplimiento de aspectos que determinan seguridad de la información, los problemas no son comunicados a la dirección ni a ningún encargado por desconocimiento, de manera que no se aplica ningún correctivo.

Causa:

- Gestión estrategia de la empresa se encuentra desactualizada, e incompleta en los aspectos que cubren la parte de TI, en el plan estratégico no se determina la importancia y relevancia de la seguridad de la información.
- No se tiene personal capacitado en los temas de seguridad
- No se tiene definición de roles para afrontar los temas de seguridad de la información
- No se brinda una capacitación al personal de la empresa en temas de seguridad de la información
- No se tiene un registro de incidentes relacionados con las TI y la seguridad de la información
- No se comunica y no se combaten los incidentes existentes de seguridad de la información

Efecto:

- La ausencia de registro de incidentes impide a la empresa el escalado de incidentes para su respectivo tratamiento
- El personal no tiene una visión clara en temas relacionados a la seguridad de información
- No se cuenta con información que respalde la inversión necesaria para la asignación de recursos tanto tecnológicos como humanos que estén capacitados para llevar a cabo una gestión de seguridad y las relaciones efectivas para el tema de seguridad de la información
- La falta de comunicación y herramientas de información para afrontar temas de seguridad de la información, provoca una desorientación en

el personal para cumplir con sus funciones preservando la seguridad de la información.

- No existen estructuras y funciones encargadas de recoger la información de incidentes de seguridad de la información, para entregarlas a las autoridades pertinentes de la empresa, constituyéndose en una herramienta útil para la toma de decisiones de la empresa.
- No se puede recopilar información que le acerque a la realidad de la exposición de riesgos en temas de seguridad, esto debido a que no se pueden gestionar por responsables de los temas en materia a fin de proveer soluciones que permitan mitigar riesgos y mejorar continuamente el negocio a través de unas TI que brinden seguridad de la información.
- No se controla los pequeños incidentes de seguridad que provocan pérdidas a la empresa
- No se puede implementar soluciones definitivas debido a que la falta de información a través de la comunicación entre los empleados no considera aspectos claves de influencia como lo es el tema de seguridad de la información.

Recomendaciones: En base al resultado obtenido de la auditoría del proceso APO08 Gestionar las Relaciones enfocado a la Seguridad de la Información, se recomienda a la dirección de la empresa seguir las orientaciones que brinda la guía de COBIT 5 para la seguridad de la información de este proceso. Previa esta recomendación se invita a la dirección de la empresa la realización de las siguientes actividades que permitirán la obtención de los elementos de información de apoyo para la gestión adecuada del proceso:

- Disponer una definición clara sobre los objetivos que busca alcanzar la seguridad de la información en la empresa, definiendo como esta afecta y habilita las estrategias del negocio

- Definir las estructuras organizativas con funciones específicas de seguridad de la información que puedan identificar e informar sobre las oportunidades, riesgos y limitaciones de las iniciativas de seguridad de la información para la empresa
- Fijar las relaciones clave en la empresa, para influir de manera positiva en la comunicación y el establecimiento de una cultura orientada a la seguridad de la información en las operaciones diarias de la empresa, como un principio rector y comunicar esta información dentro de toda la organización.
- Se recomienda construir las funciones y estructuras organizativas siguiendo la guía que ofrece la norma internacional ISO/IEC 27001: 2013, Anexo A.6 .1 sobre la Organización Interna.
- Se recomienda realizar charlas de capacitación al personal sobre los temas inherentes a la seguridad de la información y su contribución, para adaptar a la empresa las políticas que garanticen integridad, confidencialidad y disponibilidad de la información.
- Establecer períodos de entrega de informes, sobre los resultados obtenidos en las métricas de las evaluaciones obtenidas en los procesos, a la dirección de la empresa para contar con elementos que apoyen la toma de decisiones informada.
- Estructurar los mecanismos y herramientas de evaluación que permitan generar resultados de la evaluación del proceso, tomando en consideración las métricas propuestas en la guía de Cobit 5 para la seguridad de la información de este proceso.

Toda la información que se genere relacionada a este proceso debe ser debidamente documentada, revisada, aprobada, actualizada, evaluada y debe estar disponible para el personal que lo requiera para información o sujeto de supervisión.

4.6.9. BAI02: Gestionar la definición de requisitos

Hallazgo 09: No existe evidencia de que la empresa tenga registradas las definiciones de requisitos orientados a la seguridad de la información.

Criterio:"BAI02.1 Definir y mantener los requisitos técnicos y funcionales de negocio. Basado en los casos de negocio, identificar, priorizar, especificar y aceptar la información del negocio, funcional, técnica y los requerimientos de control que cubre el ámbito/ comprensión de todas las iniciativas de requerimientos para mejora de la entrega de los propósitos de TI – soluciones de negocio habilitadoras

BAI02.02 Realizar un estudio de viabilidad y proponer soluciones alternativas. Realizar un estudio de viabilidad de las potenciales soluciones alternativas, evaluando su viabilidad y seleccionando la opción preferida. Si se considera, implementar la opción seleccionada como un piloto para determinar posibles mejoras.

BAI02.03 Gestionar los riesgos de los requerimientos. Identificar, documentar, priorizar y mitigar los riesgos funcionales y técnicos relativos al procesamiento de la información y asociados con los requerimientos de la empresa y solución propuesta.

BAI02.04 Obtener la aprobación de los requerimientos y soluciones. Coordinar la realimentación de las partes interesadas afectadas y, en las fases clave predeterminadas, obtener la aprobación y la firma del patrocinador o propietario del producto y cierre de los requerimientos técnicos y funcionales, de los estudios de viabilidad, de los análisis de riesgos y de las soluciones recomendadas"[11]

Condición: La empresa no dispone de evidencia que indique el establecimiento de los requerimientos de seguridad deseables para la

[11] Cobit 5 an ISACA Framework, ISACA, *COBIT 5 para la Seguridad de la Información*, Rolling Meadows, IL 60008 EE.UU., 2012, p.121.

efectiva operación de las funciones de la empresa. Se evidencia la falta de los requisitos en la omisión de controles para el cumplimiento de requisitos legales y contractuales en la empresa, los equipos poseen software de propiedad intelectual sin el debido respaldo de adquisición del mismo, ningún empleado maneja un sistema de acceso controlado por usuarios y contraseñas para impedir accesos no autorizados, cualquier empleado puede fácilmente acceder a cualquier ordenador y extraer, alterar y eliminar información sin autorización.

Excepto el equipo de gerencia de fábrica, que posee un control de tipo físico que impide su libre acceso. No se usa ningún control criptográfico para el manejo de la información, no existe ninguna revisión a la seguridad de información de la empresa, debido a la ausencia de normas y políticas de seguridad, no se realiza ninguna evaluación de cumplimiento tanto de procesamiento y procedimiento, así como técnicos para la evaluación directa a los sistemas de información.

Causa:

- Perspectiva ausente de la seguridad de la información y de las TI en el plan estratégico de la empresa
- Plan estratégico no actualizado
- Falta de seguimiento al plan estratégico
- Privación de una arquitectura empresarial formalizada,
- Carencia de informes sobre riesgos de seguridad de la información presentes en los procesos de negocio de la empresa.

Efecto:

- Incumplimiento de requisitos legales
- Deficiencia de requisitos contractuales con servicios de terceros
- Incumplimiento con las revisiones de seguridad de la información, compromete el prestigio de la empresa, compromete su capacidad de

proteger la información, compromete sus finanzas y la operación normal del negocio.

- Sistemas no se encuentran debidamente documentados y actualizados, lo que implica que existe un alto grado de desinformación de las obligaciones legales, estatutarias de reglamentación y contractuales relacionadas a la seguridad de la información.
- Presencia de inconvenientes legales al violar derechos de autor por posesión y uso de software ilegal en las operaciones del negocio, lo que puede generar implicaciones penales
- Ausencia de controles y de comunicación para procedimientos en el manejo de la información al personal.
- No garantiza privacidad y protección de información de datos personales, los equipos son accedidos sin ninguna restricción por todos los empleados de la organización e inclusive por terceros.
- No manejan ningún mecanismo de control criptográfico la información puede ser fácilmente obtenida y no está protegida ni contra lectura, ni contra escritura.
- Estas deficiencias exponen a la empresa a un nivel de alto riesgo, ya que pueden tener hasta consecuencias de orden penal o dejar inoperativa la empresa.

Recomendaciones: En base al resultado obtenido de la auditoría al proceso BAI02 Definición de los Requisitos enfocado a la Seguridad de la Información, se recomienda a la dirección de la empresa desarrollar la información de apoyo necesaria para este proceso como lo es: la definición formal de la arquitectura empresarial TI y el plan de Gestión de Riesgos de TI, estos instrumentos son esenciales para realizar la definición de requisitos enfocados a la seguridad de la información, que se debe establecer siguiendo las recomendación de Cobit 5 para la seguridad de la información del proceso.

Se recomienda a la dirección de la empresa junto con el especialista de seguridad de la información tener en cuenta la siguiente información para generar la definición de requisitos enfocados a la seguridad de la información:

- Realizar una investigación para la definición de controles que cumplan con los requisitos requeridos por la empresa, los cuales pueden ser obtenidos como parte de apoyo desde la norma internacional ISO/IEC 27001:2013, Anexo A.18 de Cumplimiento, los cuales pueden ser aceptados como requisitos de seguridad de la información para la empresa que incluyen temas de propiedad intelectual, protección de datos y comercio electrónico entre otros.
- Establecimiento de un estudio de factibilidad de los requisitos de seguridad de la información que deben ser revisados y aprobados por la dirección de la empresa para su cumplimiento.
- Realizar el estudio de impacto de las soluciones en temas relacionados a la seguridad de la información y relación correspondiente con niveles de riesgo, para ello se deberá contar previo con el plan de gestión de riesgos.
- Establecer el compromiso de respaldo por parte de la dirección tanto en los temas de factibilidad como en el de la gestión de riesgos para la definición de los requisitos de seguridad.

Toda la información que se genere del proceso deberá ser debidamente documentada, revisada, aprobada, actualizada y estar disponible para el personal que lo requiera con fines de información, supervisión y evaluación.

4.6.10. MEA01: Supervisar, evaluar y valorar el rendimiento y conformidad

Hallazgo 10: No existe evidencia de que la empresa cuente con un sistema de gestión del rendimiento de la compañía que integre los objetivos, alcance y métodos de medición en las soluciones del negocio.

Criterio: "MEA01.01 Establecer un enfoque de la supervisión. Involucrar a las partes interesadas en el establecimiento y mantenimiento de un enfoque de supervisión que defina los objetivos, alcance y método de medición de las soluciones de negocio, la entrega del servicio y la contribución a los objetivos de negocio. Integrar este enfoque con el sistema de gestión del rendimiento de la compañía.

MEA01.02 Establecer los objetivos de cumplimiento y rendimiento. Colaborar con las partes interesadas en la definición, revisión periódica, actualización y aprobación de los objetivos de rendimiento y cumplimiento enmarcados dentro del sistema de medida del rendimiento.

MEA01.03 Recopilar y procesar los datos de cumplimiento y rendimiento. Recopilar y procesar datos oportunos y precisos de acuerdo con los enfoques del negocio

MEA01.04 Analizar e informar sobre el rendimiento. Revisar e informar de forma periódica sobre el desempeño respecto de los objetivos, utilizando métodos que proporcionen una visión completa y precisa del rendimiento de las TI y encaje con el sistema corporativo de supervisión.

MEA01.05 Asegurar la implantación de medidas correctivas. Apoyar a las partes interesadas en la identificación, inicio y seguimiento de las acciones correctivas para solventar anomalías**."**[12]

Condición: La empresa no presenta evidencia de contar con un enfoque de supervisión a la seguridad de la información de la empresa. La empresa desde su constitución no ha manejado ningún enfoque de seguridad de la información.

[12] Cobit 5 an ISACA Framework, ISACA, *COBIT 5 para la Seguridad de la Información*, Rolling Meadows, IL 60008 EE.UU., 2012, p.161.

Causa:

- La empresa carece de la gestión de políticas de la seguridad de la información
- No posee requerimientos formal e informalmente establecidos en la empresa para la seguridad de la información.
- La empresa no cuenta con la información que apoye este proceso como lo son estándares y otras regulaciones relacionadas a la seguridad de la información.

Efecto:

- No existe la definición de acciones que impliquen la recolección, validación y evaluación de incidentes relacionados a la seguridad que les permitan de esta manera gestionar los riesgos que implica la seguridad de la información de la empresa.
- La empresa desconoce cómo mejorar el rendimiento de la seguridad de la información tomando encuentra que esta afecta a todo el ámbito del negocio.
- No guarda información de los incidentes sufridos ni de la repetición de los mismos
- No existe el control de personal con el conocimiento necesario, que trabaje en la reducción de riesgos de seguridad que afectan las áreas más vulnerables de la empresa.
- Este se considera un riesgo de alto impacto para la empresa ya que al no tener un sistema para la gestión de la seguridad la empresa no tiene que evaluar, esto supone la falta de control para brindar un entorno seguro a sus empleados y al manejo y gestión de su información a través del uso de los recursos informáticos.
- Esta falta de supervisión hace que la empresa no esté en condición de determinar que tan óptimo en temas de seguridad es la gestión de sus actividades y cuáles son sus vulnerabilidades o debilidades sobre

las que se tiene que involucrar un mayor esfuerzo para cumplir de una manera eficiente, eficaz y segura sus procesos de negocio.

- Se generan accesos a la información de la empresa desde el exterior de la misma, sin control o autorización de la información y personale correspondiente pertinente, lo cual puede desembocar en la substracción de información valiosa para la empresa exponiéndola a la divulgación a terceros no autorizada como un ejemplo de lo que se evidencia en las actividades diarias de la misma.
- La empresa está expuesta de esta manera a todo tipo de ataque ya que no existen medidas que les ayuden a gestionar los riesgos de seguridad de la información
- No se ha realizado ninguna evaluación del riesgo que les permita gestionar adecuadamente su seguridad para ser mejora conforme el entorno y las necesidades del negocio lo requieran.
- La empresa no tiene ninguna protección relacionada a temas de seguridad de la información por lo que la evaluación no es procedente debido a que no ha sido establecido ningún mecanismo de control que sea sujeto de evaluación.

Recomendaciones: En base al resultado obtenido de la auditoría al proceso MEA01 Supervisar, evaluar y valorar el rendimiento y la conformidad enfocado a la Seguridad de la Información, se recomienda a la dirección de la empresa tomar en cuenta las recomendaciones para el diseño e implementación de programas que contribuyan a generar resultados de valoración para el proceso de acuerdo a las Guías señaladas a través de Cobit 5 para la seguridad de la información.

Es recomendable considerar el desarrollo de todos los elementos de apoyo como: el plan estratégico del negocio, el plan estratégico de TI y el plan estratégico para la seguridad de la información, junto con el apoyo de los diferentes planes como lo son de riesgos, inversiones, arquitectura empresarial, sistema de gobierno para la seguridad de la información, planes

para la optimización de valor y entrega de beneficios desde la perspectiva empresarial, tecnológica y de seguridad de la información. Considerar las siguientes actividades para un efectivo diseño e implementación del proceso:

- Generar la información en cada proceso, debe estar documentada, revisada, aprobada y disponible con el fin de ser sujeta de verificación y de evidencia por parte de la empresa
- Se recomienda la contratación de un servicio de asesoría externa que permita a la empresa tener las guías de respaldo para la implementación de un sistema formal para la gestión de TI y la gestión de la seguridad de la información
- Desarrollar registros de incidencias y valoración de resultados de cada proceso, según los elementos de apoyo que se deberá establecer de manera programada, para la respectiva evaluación de rendimiento y análisis de resultados de los que deberá tener conocimiento la dirección de la empresa para su respectiva revisión y aprobación.
- Crear programas de capacitación sobre la seguridad de la información y gestión de las TI al personal, para la integración de seguridad de la información en las capacidades de los empleados sin que sean funciones específicas del los roles de seguridad de la información
- Establecer programas de evaluación de desempeño relacionados con los temas de seguridad de la información, a fin de que la empresa pueda receptar la retroalimentación clave para la mejora de los procesos relacionados a la seguridad de la información
- Implementar un programa específico que permita evaluar las seguridades de la información y dar paso a procesos de mejora continua

Toda la información que se genere del proceso deberá ser debidamente documentada, revisada, aprobada, actualizada y estar disponible para el personal que lo requiera con fines de información, supervisión y evaluación

4.7. Conclusiones y Recomendaciones

Esta auditoría es presentada con la finalidad de indicar a la dirección de la empresa las vulnerabilidades y debilidades que la empresa posee en la gestión de Seguridad de la Información, a la vez en que se constituye en una herramienta clave para la toma de decisiones, lo que permitirá a la empresa el empleo de soluciones basadas en una planificación estratégica de sus tecnologías con el fin de brindar garantía en la seguridad de la información que actualmente gestiona la empresa.

Los resultados obtenidos en el proceso de auditoría se constituyen en una importante oportunidad de mejora de manera que la misma pueda percibir los mejores beneficios para el negocio con una alineación estratégica de las TI a las estrategias corporativas garantizando además la seguridad en su información en términos de integridad, confidencialidad y disponibilidad.

Cobit 5 para la seguridad de la información aprovisionó un conocimiento amplio que pudo ser ajustado a las necesidades del negocio para su correspondiente auditoría. Cobit 5 para la seguridad de la información es un producto de ISACA, que se constituye como una base de conocimiento, brindando a las empresas como Cocinas Internacionales la garantía de una gestión segura de la información que se alinee a las metas de TI y las metas corporativas.

En cada proceso seleccionado para el ámbito de la auditoría se puede hacer las siguientes recomendaciones a nivel general en esta sección del documento. Es necesario actualizar la documentación que contiene la información estratégica del negocio, esta es la plataforma que permitirá a la empresa construir un gobierno de TI y del negocio, y en consecución a esta actividad desarrollar un gobierno tecnológico enfocado a las seguridades de la información de la organización, apoyándose para la construcción de un SGSI basado en la norma internacional ISO/IEC: 27001:2013. Esta es la

recomendación base para implementar un gobierno tecnológico orientado a la seguridad de la información que se alineé a las estrategias del negocio como lo propone el proceso EDM01. Establecimiento y mantenimiento de un gobierno enfocado a la Seguridad de la información.

En cuanto al proceso EDM02. Entrega de Beneficios relacionada a Seguridad de la Información. Es necesaria la elaboración de los planes de inversión que permitan definir el retorno de la inversión adecuada a la empresa, tanto en el ámbito económico como no económico. Esto puede ser desarrollado una vez que la empresa tenga claramente definidos los beneficios que aspiran obtener en el ámbito de seguridad de la información a través de la planificación estratégica del negocio donde deberá estar integrada la información relacionada con los temas de seguridad de la información.

EDM04. Optimización de Recursos. Para formar un criterio de optimización de recursos es necesario que se tenga conocimiento de todo el recurso tecnológico disponible en la empresa, por lo que se debe hacer un reconocimiento técnico de los equipos de la empresa, reconocer su propósito, el manejo adecuado de aplicaciones que permitan a los empleados cumplir con sus respectivas actividades laborales. Para ello es necesario que la empresa cuente con la definición de perfiles de los empleados y realizar el respectivo análisis de el conjunto de aplicaciones que se deben utilizar según el perfil del empleado y su rol, esto permitirá identificar a la empresa la idoneidad de los recursos y sus posibles oportunidades de optimización frente a costos.

APO02. Gestionar la Estrategia. Es fundamental que exista una estrategia organizacional actualizada, vigente e implementada, se recomienda que para la actualización de la estrategia se estudie la inclusión de objetivos que involucren el ámbito de TI, considerando además la definición de metas que impliquen la garantía de seguridad de la información. Esto permitirá elaborar elementos de apoyo para que un

gobierno de TI y de seguridad de la información este estrechamente relacionado con las metas del negocio, conservando congruencia y sustento para la toma de decisiones informada.

APO03. Gestionar la Arquitectura Empresarial, para poder realizar una adecuada gestión de la arquitectura es necesario que esta se encuentre definida en la empresa, por ello se debe estudiar y definir la arquitectura que actualmente soporta las actividades del negocio, esto permitirá determinar las deficiencias de la arquitectura y las oportunidades de mejora continua, además que le proveerán a la empresa una visión global de cómo sostiene la empresa sus procesos de negocio. Esto permitirá que la empresa pueda planear la optimización efectiva de sus recursos, además de combinarlos con una adecuada inversión en el portafolio de sus soluciones. Permitirá realizar una planificación estratégica orientada en la información, que sea efectiva acorde a las necesidades tecnológicas del negocio y su seguridad de la información, que le permitirá estar a la empresa en la capacidad de adaptarse a cambios profundos o superficiales conociendo el impacto en el entorno del negocio.

APO04. Gestionar la Innovación. Es recomendable que la empresa cuente con el apoyo de elementos como la planeación estratégica, la especificación de roles y funciones que permitan obtener las oportunidades de mejora a través de la innovación, con el uso de herramientas que promuevan la optimización de recursos y realizar una adecuada combinación de inversiones que retornen los beneficios deseados para la empresa. Una vez con los elementos de apoyo se debe hacer los estudios necesarios para proveer un entorno adecuado en la empresa que brinde un ambiente positivo para la innovación.

APO05. Gestionar el portafolio. Es necesario que se realice la formalización de roles y funciones de los empleados y la asignación de equipos que permitan asignar el portafolio de aplicaciones requerido y necesario para cumplir con las funciones del encargo del empleado, además

de establecer y determinar la condición de uso legal que garanticen a la empresa su cumplimiento regulatorio externo como lo es el de Propiedad intelectual de aplicaciones consideradas para el uso comercial. Que permitan combinar adecuadamente los fondos que se vinculen a seguridad de la información.

APO08. Gestionar las Relaciones. Es importante formalizar la estructura organizacional considerando los roles de la función de seguridad de la información para todos los empleados sin la necesidad de un conocimiento específico. Debe ser constituida y comunicada a todo el personal que tenga responsabilidad de supervisión para la mejora continua del proceso en base a la retroalimentación del comportamiento y cultura de los empleados.

BAI02. Gestionar la definición de Requisitos. Para apoyar y sustentar este proceso es necesario que se disponga de la arquitectura de la empresa en relación a la seguridad de la información, este elemento permitirá estructurar los requisitos que serán necesarios para cubrir estas posibles deficiencias al sistema de seguridad de la información. Con la colaboración de elementos como la planificación estratégica, análisis de riesgos, programas de optimización de recursos, gestión de la innovación entre otros.

MEA01. Supervisar, evaluar y valorar el rendimiento y la conformidad. Es necesario que la empresa tenga la información habilitante básica actualizada y disponible para el desarrollo de planes que promuevan el mejoramiento continuo. La planificación estratégica de la organización debe tener un seguimiento continuo, ya que el cumplimiento de las metas estratégicas contribuirá a la empresa una dirección de lo que requiere lograr. Además que se constituirá en el instrumento que permita la evaluación del cumplimiento de la dirección especificada.

Las aplicaciones de las recomendaciones señaladas en este trabajo le permitirán a la empresa adaptarse de manera segura a un entorno tecnológico cambiante. Estableciendo un gobierno tecnológico soportado en

la seguridad de la información, lo que facilitará desarrollar una planificación organizada y efectiva tanto para sus inversiones, portafolios y optimización adecuada de los recursos para aprovechar su máximo potencial.

Es recomendable en este punto, indicar que la empresa requiere de personal capacitado tanto en el área de TI como de seguridad de la información, el coste de inversión por contratación de personal de planta puede superar la capacidad de inversión de la empresa y puede resultar no tan beneficioso por la línea de negocio de la empresa y su rentabilidad, sin embargo, toda empresa debe contar con la adecuada gestión de sus TI por lo que se recomienda tener como alternativa la contratación de un servicio de asesoría tecnológica y de seguridad de la información que les pueda aportar con las mejores orientaciones para la implementación de las recomendaciones realizadas en este informe.

CAPITULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

5.1.1. Conclusiones Técnicas de COBIT 5

- Los procesos de auditoría informática o evaluaciones técnicas en la actualidad son muy necesarios en las empresas, independientemente de su tamaño o entorno de negocio, esto permite que una empresa tenga un conocimiento de la condición y de cómo las Tecnologías de Información apoyan y fortalecen los procesos de negocio brindándoles grandes beneficios a costos de operación óptimos.
- Cobit 5 es un marco metodológico para el gobierno y gestión de las tecnologías de la Información y el negocio, provee un conocimiento amplio, gracias a que reúne la experiencia de varios profesionales de todo el mundo en las diferentes áreas en las que las tecnologías de la información se encuentran involucradas, brindando un soporte consiste que puede ser aplicado a las organizaciones de todo tipo de entorno y de todo tamaño.
- Cobit 5 es un marco metodológico muy versátil, que logra adaptarse a las necesidades y expectativas de las organizaciones, sus guías y recomendaciones cubren por completo, brindando las pautas que pueden escoger las organizaciones para adaptar un gobierno tecnológico eficientemente gestionado
- La gestión tecnología de una empresa no solo debe estar basada en la disponibilidad de los recursos, sino que además debe garantizar seguridad de la información en todos los procesos de la empresa en los que se encuentre implícito el uso de recursos tecnológico que deben garantizar la seguridad de la información en aspectos de integridad, confidencialidad y disponibilidad.
- Todo trabajo de auditoría y/o evaluación técnica se constituye una valiosa herramienta de apoyo para la toma de decisiones informada

que permitan a las empresas y a sus autoridades implementar las medidas necesarias que beneficien la operación del negocio y que además les brinden una ventaja competitiva en un entorno en el que las tecnologías de la información y la información se han vuelto el activo más preciado para posicionar y consolidar los negocios.

- La Auditoría Basada en Riegos que propone Cobit 5 partiendo de la utilización de la cascada de metas es lo suficientemente consistente para establecer una relación directa e indirecta entre las metas de negocio con las Tecnologías de la información, tanto genéricas como propias de la empresa.
- Cada catalizador es importante y tiene una participación igual de importante en cada proceso, se constituyen en los elementos de apoyo en donde individualmente no tiene gran peso, pero en conjunto pueden generar el éxito en el cumplimiento del propósito de un proceso o su fracaso.
- Cobit 5 puede ser implementado siguiendo sus guías por personal con conocimientos en Tecnologías de la Información sin mayor dificultad apoyándose de los productos que ISACA tiene como elementos de conocimiento y experiencias en implementación del marco de referencia para un gobierno de TI y de negocio integrados.

5.1.2. Conclusiones del Proyecto

- La auditoría informática aplicada a la Empresa Cocinas Internacionales, permitió detectar que la empresa no posee controles para garantizar la seguridad de la información debido a la falta de un gobierno de las TI, que se deriva de la falta de seguimiento al plan estratégico institucional que se encuentra desactualizado.
- La empresa es una PYME y en su característica organizacional no posee un área específica dedicada a las TI, ni a la seguridad de la información, por esta razón el tema de TI ha sido descuidado y poco atendido, provocando una gestión poco eficiente de los recursos relacionados a las TI del negocio.

- La falta de un gobierno tecnológico en la actualidad en las empresas sean medianas o grandes, representa una gran desventaja para los negocios, cada día son más las empresas que dependen del activo de TI para generar soluciones de alta rentabilidad, que buscan la optimización de costos y la capacidad de mantener niveles de riesgo en condiciones adecuadas donde su impacto no afecte de forma crítica las operaciones del negocio.
- La auditoria informática realizada tuvo un alcance orientado a los procesos de mayor riesgo, para los cuales se elaboro un informe que involucra recomendaciones que deben ser tomadas en cuenta para poder diseñar un Sistema de Gestión de la Seguridad de la Información adecuado que brinde los beneficios más útiles para la empresa.

5.2. Recomendaciones

5.2.1. Recomendaciones Técnicas de COBIT 5

- Es recomendable que las empresas integren como una estrategia institucional la gestión de las tecnologías de la información considerando las evaluaciones periódicas a sus sistemas de control a fin de que les permitan evaluar la eficacia y la eficiencia de los controles implementados en la gestión de las Tecnologías de la Información.
- Es recomendable el uso de Cobit 5 para la implementación de un gobierno y gestión tecnológico su experiencia brinda un amplio soporte para todas las áreas. Esta versión consolida 5 características que permiten una gestión y gobierno integral, sin necesidad de que se haya implementado antes otros marcos de gobierno, esta metodología puede ser independiente aun de versiones anteriores y no requiere obligatoriamente la existencia de un marco metodológico de gestión antecesor.

- Es recomendable que para implementar Cobit 5 como marco de gobierno y gestión de las tecnologías de información de las empresas, se definan una configuración específica y personalizada que logre adaptar las necesidades y entorno del negocio de una manera guiada, se debe considerar que toda la información de Cobit 5 es un conjunto genérico de sugerencias que no son obligatorias para todas las empresas.
- Se recomienda considerar que seguridad de la información debe cubrir todos los extremos de la empresa para no dejar brechas de seguridad descuidadas, Cobit posee un conjunto definido de procesos que permiten garantizar seguridad, sin embargo, seguridad de la información debe ser considerada en todos los procesos, por ello es necesario establecer seguridad de la información desde las guías provistas en el Producto de Cobit 5 para la Seguridad de la información que provee una visión de cobertura general a todos los procesos que garanticen el cumplimiento de las características de seguridad de la información que son: integridad, confidencialidad y disponibilidad de la información.
- Se recomienda considerar que las auditorías internas y/o evaluaciones técnicas deben ser parte del ciclo de vida dentro de los procesos de las empresas, esto permitirá a las empresas evaluar la eficacia de los controles y soluciones implementadas y obtener una retroalimentación para un proceso de mejora continua.
- Se recomienda manejar matrices de riesgos personalizadas que reflejen las necesidades reales de la empresa y los procesos que realmente represente un alto riesgo para el funcionamiento normal de las operaciones del negocio, estableciendo de acuerdo al criterio de las autoridades si las ponderaciones establecidas por COBIT V5 son precisas en su peso o si es necesario personalizar el peso de las mismas que refleje al final el resultado más cercano a la realidad de la empresa.

- Se recomienda utilizar la guía de implementación de Catalizadores de Cobit 5, el cual ofrece una amplia visión de cómo se componen y como deben ser integrados en el ámbito de gobierno y gestión de las tecnologías de la información y el negocio, a fin de lograr un conjunto de elementos que apoyen y contribuyan con el cumplimiento de las prácticas de gestión de cada proceso.
- Es recomendable que se cuente con los elementos de información clave al momento de implementar un Marco de Referencia para el Gobierno de las TI y el Negocio de Cobit 5, además se debe contar con el personal idóneo que tenga conocimientos básicos de tecnologías de la Información a fin de que esté familiarizado con la información contenida en las guías de orientación para la implementación de los modelos de gobierno y gestión.

5.2.2. Recomendaciones del Proyecto

- La recomendación a la empresa cocinas internacionales para poder experimentar lo beneficios de un gobierno y gestión de la tecnología es actualizar la información estratégica de la institución en la cual se involucre de manera determinante la influencia tecnológica y la importancia de su gestión para el cumplimiento de las metas estratégicas institucionales incorporando también la importancia que representa la empresa una adecuada gestión de la seguridad de su información.
- Es recomendable que la empresa Cocinas Internacionales considere la contratación de un servicio de consultoría que les permita diseñar un sistema de gobierno de TI que se adapte a las expectativas de la organización, Cobit 5 es un marco metodológico recomendado ya que posee los atributos que le permite adaptarse a las necesidades de todo tipo de organización, por otro lado no se recomienda a la empresa contratar personal de nómina para establecer una unidad encargada específicamente de las funciones de TI, debido a que se debe considerar que es un gasto elevado y poco rentable por la

actividad económica de la empresa donde estaría sujeta a una inversión a largo plazo.

- Se recomienda a la empresa apoyarse en la elaboración y análisis de planes para la gestión de riesgos inherentes al ámbito de TI, que les permita centrar y orientar esfuerzos en los procesos adecuados de una manera guiada e informada para dar apoyo a los procesos que más lo requieran.
- El informe generado como resultado de la presente auditoria entrega una serie de recomendaciones que deben ser tomadas en cuenta para crear un entorno de Seguridad de la Información, sin embargo, se recomienda a la empresa, no tomar únicamente estas recomendaciones sino que implementar un sistema de Gobierno y Gestión Tecnológico en Base a las guías de Cobit 5, y posterior usar las guías para implementar un diseño para el gobierno de Seguridad de la información de la misma familia de Productos de Cobit 5, que brindara mayores beneficios permitiendo implementar todos los procesos y no únicamente los más críticos como los que fueron objeto de evaluación en esta auditoría.

Referencias Bibliográficas

Actualidad Técnologica. (s.f.). Recuperado el 07 16, 2015, de http://tecno-actualidad.blogspot.com/2010/02/auditoria-de-sistemas-interna-externa.html#

Auditoria Informatica. (s.f.). Recuperado el 07 16, 2015, de http://muziek-film-kunst.blogspot.com/2010/11/121-auditoria-interna-y-externa.html

Buges, M. J. (18, 06 2015). *Slideshare.* Recuperado el 01 27, 2016, de http://es.slideshare.net/mariajosebuigues3/iso-27001-actualizacin-versin-2013

Calderón, J., & Ocaña, D. (2014, 04 01). *Repositorio Digital ESPE.* Recuperado el 29 07, 2015, de http://repositorio.espe.edu.ec/handle/21000/9032

Cocinas Internacionales. (2005). *Plan de Mejoramiento Estratégico.* Quito.

Fernández, N. (2008, 11 27). *Entérate en Línea*. Recuperado el 07 17, 2015, de http://www.enterate.unam.mx/Articulos/2005/octubre/auditoria.htm

Hernández, E. H. (1997). *Auditoria Informática: Un Enfoque Metodológico y Práctico.* México: CECSA.

ISACA. (2012). COBIT 5 para la Seguridad de la Información. Rolling Meadows, Rolling Meadows, EE.UU.

ISACA. (2012). Cobit 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. Estados Unidos, Rolling Meadows, Rolling Meadows.

ISACA. (s.f.). COBIT 5 para el Aseguramiento.

Kuna, H. D. (2014, 09 22). *researchgate.* Recuperado el 07 17, 2015, de http://www.researchgate.net/profile/Horacio_Kuna/publication/26519345_Asistente_para_la_Realizacin_de_Auditoras_de_Sistemas_en_Organismos_Pblicos_o_Privados/links/54203f6a0cf241a65a1beafb.pdf

Meryk, J. T. (2014, 10 06). *Scribd.* Recuperado el 01 28, 2016, de https://www.scribd.com/doc/244315158/MAPEO-DE-COBIT-5-con-ISO-27001-2013-pdf

Moreno, J. (2012, 09 30). *slideshare.* Recuperado el 07 16, 2015, de http://es.slideshare.net/j_moreno/auditoria-informatica-y-de-sistemas-de-informacion

Naveda, A. (2012, 03 01). *Repositorio Digital ESPE.* Recuperado el 29 07, 2015, de http://repositorio.espe.edu.ec/handle/21000/9032

Proyectos fin de carrera. (s.f.). Recuperado el 07 15, 2015, de http://www.proyectosfindecarrera.com/auditoria-interna-externa.htm

Ramírez, G. (2009, 12 17). *e-archivo.uc3m.es.* Recuperado el 07 17, 2015, de http://e-archivo.uc3m.es/bitstream/handle/10016/6136/PFC_German_Ramirez_Rodriguez.pdf?sequence=1

Tejada, E. (2015). *Auditoría de Seguridad Informática. IFCT0109.* Málaga: IC Editorial.