ÍNDICE

CONTENIDO **PAG.**

Gráficos **PAG.**

TABLAS **PAG.**

1. INFORMACIÓN GENERAL

Título del Proyecto:

Auditoría informática aplicando la metodología COBIT 4.1 en el departamento de sistemas perteneciente al GRUPO KFC.

Tipo de Proyecto:

Investigación Evaluativa: Evaluar los procesos que se llevan a cabo dentro de cada área del Departamento de Sistemas.

Investigación Tecnológica: Por el motivo en el que se va analizar cómo se lleva a cabo los procesos tecnológicos que se realizan en cada área del Departamento de Sistemas.

Propósito:

- Obtener información para plantear soluciones a los inconvenientes analizados en base a la auditoría informática que se realizará.

La auditoría informática que se realizará tiene como propósito el obtener información de cómo se lleva a cabo los procesos, cuáles son los inconvenientes, de qué manera se trabaja, entre otros, para poder solucionar los problemas que se encuentren mediante el análisis de resultados una vez concluida la auditoria.

Fecha de inicio: Noviembre/2015

Fecha de finalización: Julio/2016

Lugar de ejecución:

Amazonas y Corea- Quito – Pichincha – Sierra - Grupo KFC

Unidad Académica que auspicia

Universidad Técnica de Cotopaxi

Carrera que auspicia:

Ingeniería en Informática y Sistemas Computacionales.

Línea de investigación: Tecnología de la información y comunicación.

Sublíneas de Investigación de las Carrera: Auditoria Informática

Equipo de Trabajo

Tutor:

DATOS PERSONALES

Nombre: Gustavo Rodríguez Bárcenas

Nacionalidad: Cubana

Fecha de nacimiento: 03 de Diciembre 1972

Estado Civil: Casado

Residencia: Los Arupos, San Felipe, Latacunga, Cotopaxi, Ecuador.

E-mail: gustavo.rodriguez@utc.edu.ec

Teléfonos: 0987658959

TÍTULOS OBTENIDOS

- Tecnólogo en Informática, Escuela Politécnica "Mateo Sánchez", Mayarí, Holguín, Cuba, 1995.
- Ingeniero Mecánico, Instituto Superior Minero Metalúrgico de Moa (ISMMM), 2003.
- Magister Sistemas Informáticos para la Educación. ISMMM, 2007.
- Magister en Bibliotecología y Ciencia de la Información. Universidad de la Habana, 2011.
- Diploma de Estudios Avanzados (DEA) en Documentación e Información Científica. Universidad de Granada, España, 2011.
- Doctor (PhD) en Ciencias de la Información. Calificación Sobresaliente *CUM LAUDE*, Universidad de Granada, España, 2013.

Coordinador del Proyecto

DATOS PERSONALES

Nombre: Henry Daniel Ortiz Colaguazo

C.I: 172020840-2

Dirección: San Bartolo Huamboya y Buenavista S15-107 - Quito

Teléfonos: 0999786485-022672815

Correo electrónico: Daniel.ortiz974@gmail.com-daniel.ortiz@kfc.com.ec

Educación Primaria

- ESCUELA FISCAL MIXTA “ESTADOS UNIDOS DE NORTE AMÉRICA”

1996-2002 INSTRUCCIÓN PRIMARIA

Educación Secundaria

- INSTITUTO TECNOLÓGICO SUPERIOR “SUCRE”

2002-2008 BACHILLER TÉCNICO INDUSTRIAL ESPECIALIDAD ELECTRÓNICA

2. RESUMEN DEL PROYECTO

La presente auditoría establece una metodología a seguir para el análisis detallado de los procesos que se realizan. Se ha tomado como caso particular la empresa (organización) Grupo KFC-Quito, disponiendo de una cadena de restaurantes de comida alimenticia, el cual cuenta con un Departamento de Sistemas en el que se realizan procesos vinculados a cada una de las áreas que cumplen con los objetivos propuestos.

Grupo KFC-Departamento de Sistemas necesita realizar una auditoria informática completa utilizando y aplicando la Metodología COBIT 4.1 el cual se enfoca en que los procesos informáticos se ejecuten y se administren de manera correcta, ya que en la actualidad existe dificultades en las actividades que se realizan en cada área del Departamento de Sistemas, esto se da por la inexistencia de políticas de seguridad de la información o no existen controles que evidencien los procesos realizados.

Es por este motivo que se llevó a cabo la auditoria Informática aplicando la Metodología y utilizando varios instrumentos y técnicas para la recolección de información y a la vez la creación de las políticas de Seguridad para el Departamento de Sistemas, obteniendo los resultados favorables y concluyendo en que los procesos y objetivos que se proponen cada área se cumple a cabalidad pero no existe la documentación necesaria para evidenciar los procesos, es por esto que beneficia la creación de políticas y una planificación para controlar el manejo de información.

3. JUSTIFICACIÓN DEL PROYECTO

En el Departamento de Sistemas perteneciente al GRUPO KFC existen diferentes áreas que se encargan de brindar servicio al cliente como son; áreas de Business Intelligence, Infraestructura, Soporte, Soporte CAR y Planta, Desarrollo y Proyectos, ERP (Planificación de Recursos Empresariales). Se puede evidenciar que cada área cumple con todos los objetivos propuestos enfocándose en el cumplimiento de cada proceso, pero con la gran dificultad de que no se documenta ni se evidencia los procesos correspondientes, lo cual contrae grandes dificultades para los usuarios, auditores externos, es por esto que la auditoría es importante realizarla ya que no existe políticas de seguridad o estrategias los cuales controlen cómo se lleva a cabo los procesos o funciones correspondientes.

Tradicionalmente, las áreas informáticas han tenido un amplio reconocimiento técnico; sin embargo no han sido tomadas en cuenta en las grandes decisiones, de ahí que el personal administrativo y empleados del Departamento de Sistemas (IT) están convencidos que los recursos informáticos deben ser evaluados, protegidos y administrados, por lo que se considera de suma importancia el control y aprovechamiento adecuado de los recursos tecnológicos de informática.

En vista de que en el Departamento de Sistemas (IT) no se ha realizado una Auditoría Informática, se ha desarrollado una Guía basada en la Metodología COBIT 4.1, para la realización de la misma, con el objeto de dar cumplimiento a lo dispuesto por los organismos de control a los que se encuentra sujeto el Departamento de Sistemas (IT).

Se eligió la Metodología COBIT 4.1 tomando en cuenta las necesidades institucionales y la orientación que ésta tiene, la misma que permite realizar un análisis por procesos, partiendo de los objetivos del Departamento de Sistemas (IT) y de cada uno de sus áreas.

4. BENEFICIARIOS DEL PROYECTO

Los beneficiaros directos del proyecto son alrededor de 50 personas que trabajan en el Departamento de Sistemas el cual cumplen con varias funciones dentro de cada área y los beneficiaros indirectos son los auditores externos quienes cumplen con la función de revisar los procesos que se llevan a cabo en el Departamento de Sistema.

El Departamento de Sistemas del Grupo KFC, cuenta en los actuales momentos con las siguientes áreas:

1.- Área de ERP: Coordinador, Carla Chiriboga

2.- Área de Soporte: Coordinador, Luis Vásquez

3.- Área de Desarrollo y Proyectos: Coordinador, Ana Jacho

4.- Área de Infraestructura: Coordinador, Alex Ponce

5.- Área de Soporte CAR y Planta: Coordinador, Mario Molina

6.- Área de Business Intelligence: Coordinador, Amarilis Loor

5. EL PROBLEMA DE INVESTIGACIÓN:

Ineficiencia en los procesos llevados a cabo por las áreas del departamento de sistemas del GRUPO KFC, provocados por la falta de políticas y estrategias que evidencien la documentación asociada a las actividades que se desempeñan.

6. OBJETIVOS:

Objetivo General.

Desarrollar una auditoría informática, aplicando la metodología COBIT 4.1 en el departamento de sistemas, para establecer políticas y estrategias eficientes para solucionar los inconvenientes enfocados a la Tecnología de la información (TI).

Objetivos Específicos.

- Elaborar un plan de auditoría informática, utilizando la metodología COBIT 4.1 en el área de sistemas, para solucionar los inconvenientes enfocados a la documentación de los procesos de cada área del Departamento de Sistemas.
- Determinar los KPI (Indicador clave de rendimiento) de cada área del Departamento de Sistemas, mediante encuestas y entrevistas con las personas que trabajan en cada área, para determinar los procesos importantes en los cuales se maneja información confidencial de la empresa.

- Realizar una evaluación al Departamento de Sistemas, utilizando la aplicación MSAT, para determinar los riesgos y defensas de la información, aplicaciones, conexiones de red e inalámbricas, servicios,
- Verificar el cumplimiento de los procesos, Utilizando un Checklist "Información de Gestión de la Seguridad BS ISO IEC 17799: 2005 SANS", para analizar el cumplimiento de cada proceso y poder realizar un plan de acción para cada área.
- Redactar Políticas de seguridad de la información, teniendo como referencia las políticas de la organización mundial SANS, para aplicar en cada área del Departamento de Sistemas y a la vez proteger mediante estrategias los procesos e información con la que se trabaja.

7. OBJETIVOS ESPECÍFICOS, ACTIVIDADES Y METODOLOGÍA

1. Elaborar un plan de auditoría informática, utilizando la metodología COBIT 4.1 en el área de sistemas, para solucionar los inconvenientes enfocados a la documentación de los procesos de cada área del Departamento de Sistemas.

   Actividad: Elaborar un plan de control de actividades

   Resultado: Cronograma para realizar la auditoria informática

   Metodología: Investigación Descriptiva

2. Determinar los KPI (Indicador clave de rendimiento) de cada área del Departamento de Sistemas, mediante encuestas y entrevistas con las personas que trabajan en cada área, para determinar los procesos importantes en los cuales se maneja información confidencial de la empresa.

   Actividad: Determinar las principales actividades de cada área.

   Resultado: Obtener información.

   Metodología: Investigación Descriptiva

3. Realizar una evaluación al Departamento de Sistemas, utilizando la aplicación MSAT, para determinar los riesgos y defensas de la información, aplicaciones, conexiones de red e inalámbricas, servicios, etc.
   Actividad: Realizar la evaluación con la aplicación MSAT.

Resultado: Resultados de la evaluación con la aplicación MSAT (Graficas, porcentajes)

Metodología: Investigación Descriptiva

4. Verificar el cumplimiento de los procesos, Utilizando un Checklist "Información de Gestión de la Seguridad BS ISO IEC 17799: 2005 SANS", para analizar el cumplimiento de cada proceso y poder realizar un plan de acción para cada área.
   Actividad: Verificar el cumplimiento de cada proceso enfocado a cada área.

   Resultado: Resultados del CheckList

   Metodología: Método Inductivo

5. Redactar Políticas de seguridad de la información, teniendo como referencia las políticas de la organización mundial SANS, para aplicar en cada área del Departamento de Sistemas y a la vez proteger mediante estrategias los procesos e información con la que se trabaja.
   Actividad: Redactar las políticas de seguridad para cada área y para el Departamento de Sistemas.

   Resultado: Políticas de Seguridad

   Metodología: Investigación Descriptiva

8. FUNDAMENTACIÓN CIENTÍFICO TÉCNICA

8.1 Fundamentos de la auditoría informática

Considerando que el objetivo de la investigación es la planificación y la realización de una **AUDITORÍA INFORMÁTICA,** a continuación se cita conceptos y definiciones sobre la misma:

Buades. B. (1985), plantea que la Auditoria Informática es el conjunto de técnicas, actividades y procedimientos, destinados a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control, eficacia, seguridad y adecuación del servicio informático en la empresa, por lo que comprende un examen metódico, puntual y discontinuo del servicio informático, con vistas a mejorar en: rentabilidad, seguridad y eficacia.

Monografías (2015), sobre la auditoria informática indica que el concepto de Auditoría es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una sección, un organismo, una entidad.

Eduardo L. (2000), menciona que Auditoria Informática es el conjunto de procedimientos y técnicas para evaluar y controlar un sistema informático con el fin de constatar si sus actividades son correctas y de acuerdo a las normativas informáticas y generales prefijadas en la organización.

8.2 Objetivos generales de una auditoría informática

Entre los objetivos que se pretende alcanzar con la aplicación de la Auditoría Informática, según la página Monografías (2008), detallan:

- Buscar una mejor relación beneficio - costo de los sistemas automáticos o computarizados.
- Incrementar la satisfacción de los usuarios de los sistemas computarizados
- Asegurar una mayor integridad, confidencialidad y confiabilidad de la información mediante la recomendación de seguridades y controles.
- Conocer la situación actual del área informática y las actividades y esfuerzos necesarios para lograr los objetivos propuestos.
- Seguridad del personal, datos, hardware, software e instalaciones.
- Apoyo de función informática a las metas y objetivos de la organización.
- Seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático.
- Minimizar existencias de riesgos en el uso de Tecnología de información.
- Decisiones de inversión y gastos innecesarios.
- Capacitación y educación sobre controles en los Sistemas de Información.

8.3 Características de la auditoría informática

Rocío L. (2005). Sobre las características de Auditoría es la información de la empresa y para la empresa, siempre importante, se ha convertido en un Activo Real de la misma, con sus Stocks o materias primas si las hay. Por ende, han de realizarse inversiones informáticas, materia de la que se ocupa la Auditoria de Inversión Informática.

Del mismo modo, los Sistemas Informáticos o Tecnológicos han de protegerse de modo global y particular: a ello se debe la existencia de la Auditoria de Seguridad Informática en general, o a la auditoria de Seguridad de alguna de sus áreas, como pudieran ser Desarrollo o Técnica de Sistemas.

Cuando se producen cambios estructurales en la Informática, se reorganiza de alguna forma su función, está en el campo de la Auditoria de Organización Informática o Tecnológica.

Estos tres tipos de auditorías engloban a las actividades auditoras que se realizan en una auditoria parcial. De otra manera, cuando se realiza una auditoria del área de Desarrollo de Proyectos de la Informática de una empresa, es porque en ese desarrollo existen, además de ineficiencias, debilidades de organización, o de inversiones, o de seguridad, o alguna mezcla de ellas

Rocío L. (2016). Sobre las Características auditoria informática menciona:

"Las empresas acuden a las auditorías externas cuando existen síntomas bien perceptibles de debilidad. Estos síntomas pueden agruparse en clases:

1. **Síntomas de necesidad de una auditoria informática:**

- Síntomas de descoordinación y desorganización.
- No coinciden los objetivos de la Informática y de la Compañía.
- Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente.

2. **Síntomas de mala imagen e insatisfacción de los usuarios.-** Tenemos los siguientes:

- No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de Software en los terminales de usuario, refrescamiento de paneles, variación de los ficheros que deben ponerse diariamente a su disposición, etc.
- No se reparan las averías de Hardware ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.
- No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de Aplicaciones críticas y sensibles.

3. Síntomas de Debilidades Económico-Financiero:

- Incremento desmesurado de costes.
- Necesidad de justificación de Inversiones Informáticas (la empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).
- Desviaciones Presupuestarias significativas.
- Costes y plazos de nuevas inversiones.
- Síntomas de inseguridad: evaluación de nivel de riesgos.

4. Síntomas de Inseguridad.- Evaluación de riesgos:

- Seguridad lógica.
- Seguridad física.
- Confidencialidad: Los datos son propiedad inicialmente de la organización que los genera. Los datos de personal son especialmente confidenciales.
- Continuidad del servicio: Es un concepto aún más importante que la seguridad. Establece las estrategias de continuidad entre fallos, mediante planes de contingencia totales y locales.
- Centro de Proceso de Datos fuera de control. Si tal situación llegara a percibirse, sería prácticamente inútil la auditoria. Esa es la razón por la cual, en este caso, el síntoma debe ser sustituido por el mínimo indicio".

8.4 Estándares de auditoría

COBIT (control de objetivos para la tecnología y la información)

En Control de Objetivos para la Tecnología y la Información (COBIT) ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnología de Información (TI).

COBIT se fundamenta en los Objetivos de Control existentes de la Information Systems Audit and Control Foundation (ISACF), mejorados a partir de estándares internacionales técnicos, profesionales, regulatorios y específicos para la industria, tanto existentes como en

surgimiento. Los Objetivos de Control resultantes han sido desarrollados para su aplicación en sistemas de información en toda la empresa. El término "generalmente aplicable y aceptado" es utilizado explícitamente en el mismo sentido que los Principios de Contabilidad Generalmente Aceptados (PCGA o GAAP por sus siglas en inglés). Para propósitos del proyecto, "buenas prácticas" significa consenso por parte de los expertos.

Este estándar es relativamente pequeño en tamaño, con el fin de ser práctico y responder, en la medida de lo posible, a las necesidades de negocio, manteniendo al mismo tiempo una independencia con respecto a las plataformas técnicas de Tecnologías de Información (TI) adoptadas en una organización. El proporcionar indicadores de desempeño (normas, reglas, etc.), ha sido identificado como prioridad para las mejoras futuras que se realizarán al marco referencial.

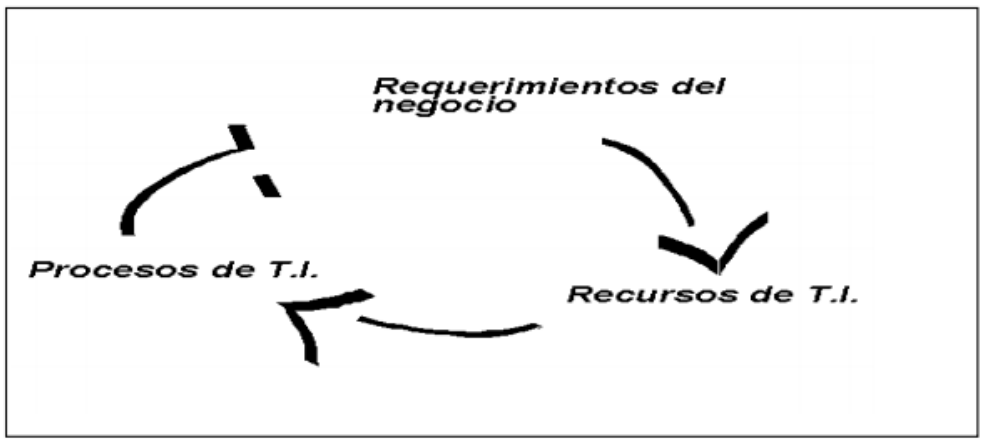
Mario L. (2010). Sobre COBIT plantea que el desarrollo del Control de Objetivos para la Tecnología y la información (COBIT) ha traído como resultado la publicación del Marco Referencial general y de los Objetivos de Control detallados, y le seguirán actividades educativas. Estas actividades asegurarán el uso general de los resultados del Proyecto de Investigación COBIT.

El concepto fundamental del marco referencial de la metodología COBIT, se refiere a:

El enfoque de control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio.

La Información es el resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información, que deben ser administrados por procesos TI.

Gráfico 1: Principios del marco de trabajo



Fuente: http://www.rociolopez.8m.com/

Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que COBIT hace referencia como requerimientos de negocio para la información. Al establecer la lista de requerimientos, COBIT combina principios contenidos en modelos referenciales existentes y conocidos:

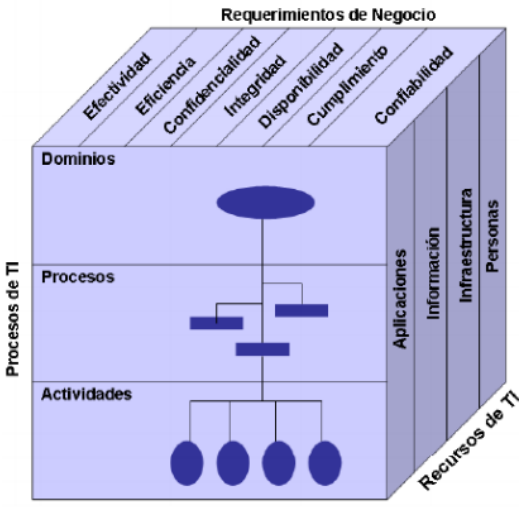
1. **Requerimiento de Calidad:**

- Calidad.
- Costo.
- Entrega de servicio.

2. **Requerimientos de Seguridad:**

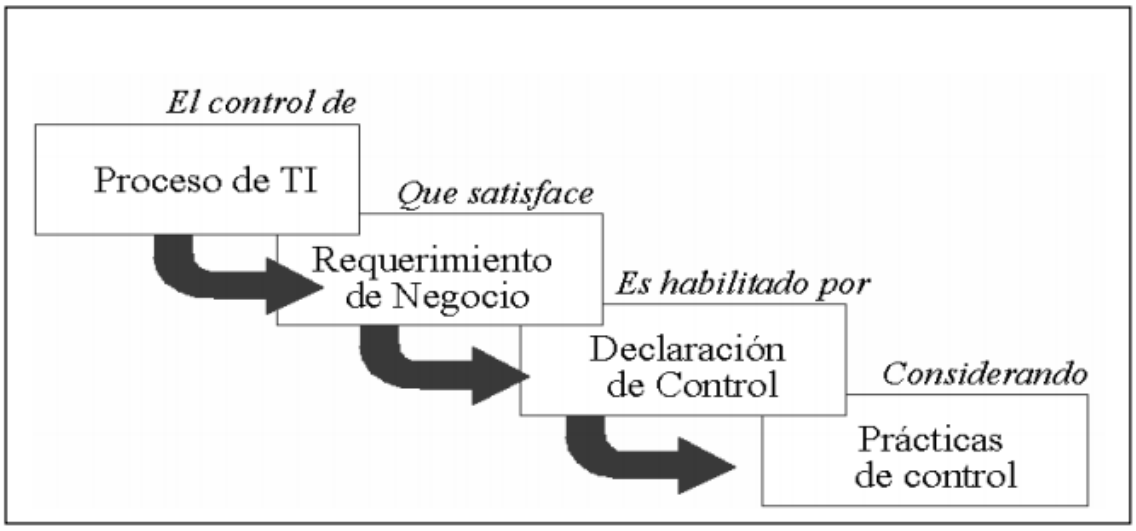
- Confidencialidad.
- Integridad.
- Disponibilidad.

Gráfico 2: Criterios de información



Fuente: http://www.rociolopez.8m.com/

Gráfico 3: Estructura de COBIT



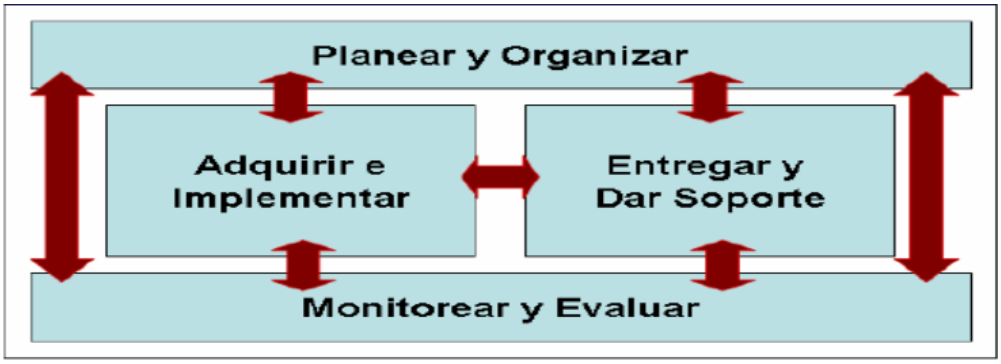
Fuente: http://www.rociolopez.8m.com/

Misión de COBIT

Galeón R. (2015). Sobre la COBIT misión. Consultado 10/02/2016, Disponible: **http://aabbccddee.galeon.com/Método.htm.** "la misión de COBIT es investigar, desarrollar, publicar y promover un conjunto internacional, autorizado y actual de objetivos de control en tecnología de información generalmente aceptados para uso cotidiano de gerentes de empresa y auditores".

8.5 Metodología de COBIT

Gráfico 4: Dominios de COBIT



Fuente: http://redyseguridad.fi-p.unam.mx/proyectos/cobit/seccion_informativa/4_monitorear_evaluar/seccion_informativa_me.html

Dominio: (PO) Planificación y Organización

A través de este dominio se comprende las decisiones estratégicas y tácticas que definen la manera en que la Tecnología de Información (TI) ayuda de mejor forma al logro de los objetivos de la institución.

Dominio: (AI) Adquisición e Implementación

Con este dominio se identifica soluciones de Tecnologías Informáticas (TI) adquiridas o desarrolladas, y por supuesto hacerlas operativas, integrándolas como procedimientos del día a día, lo que permite ser mejores y tener una continuidad operativa.

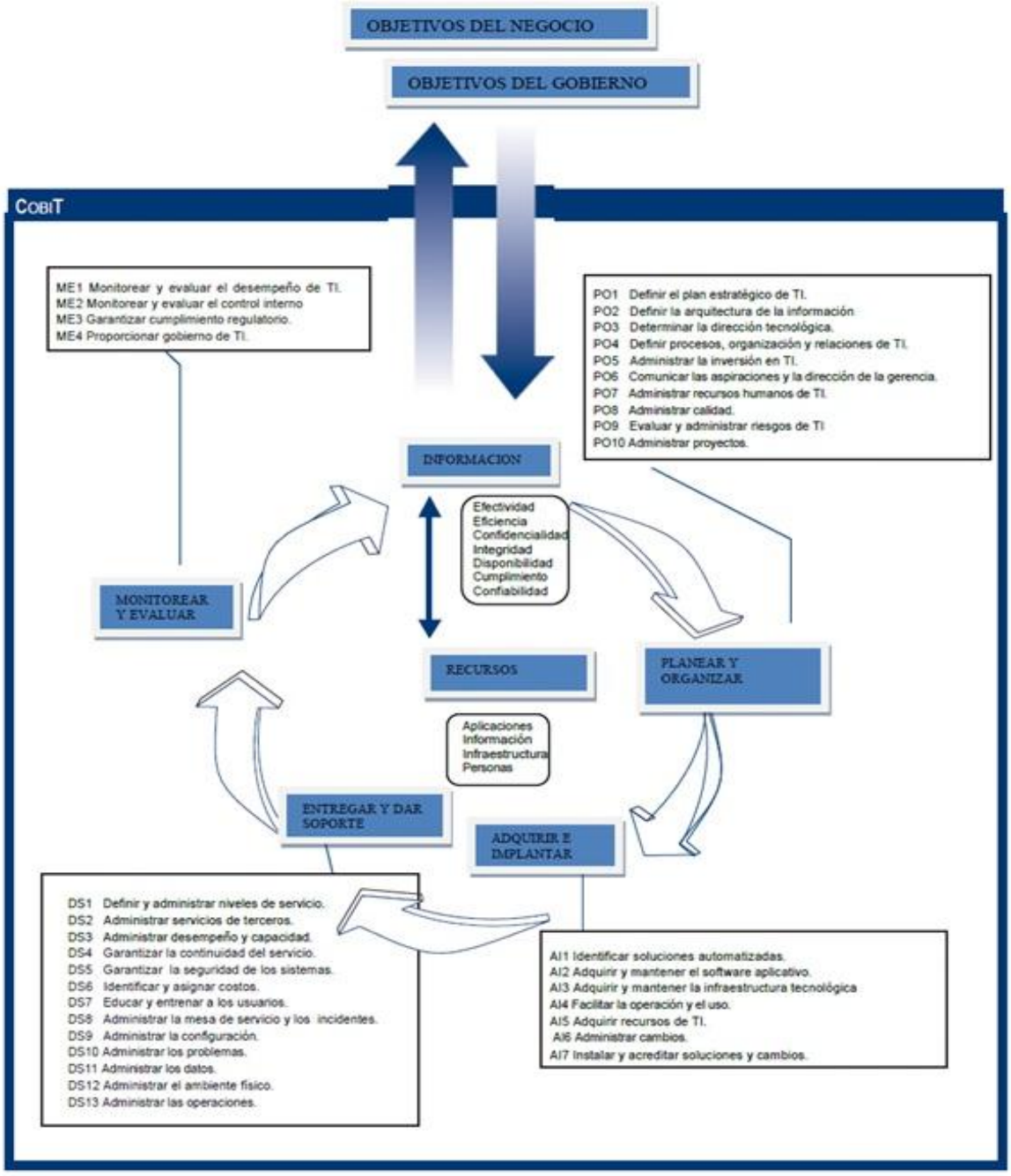
Dominio: (ES) Entrega y Soporte

Mediante este dominio se llega a comprender las actividades de soporte a los sistemas en producción. En esta área se incluye el procesamiento de los datos por sistemas de aplicación.

Dominio: (M) Monitoreo

Mediante este dominio todos los procesos de TI deben ser evaluados regularmente, tanto en cuanto a su calidad, como al cumplimiento de los requerimientos de control.

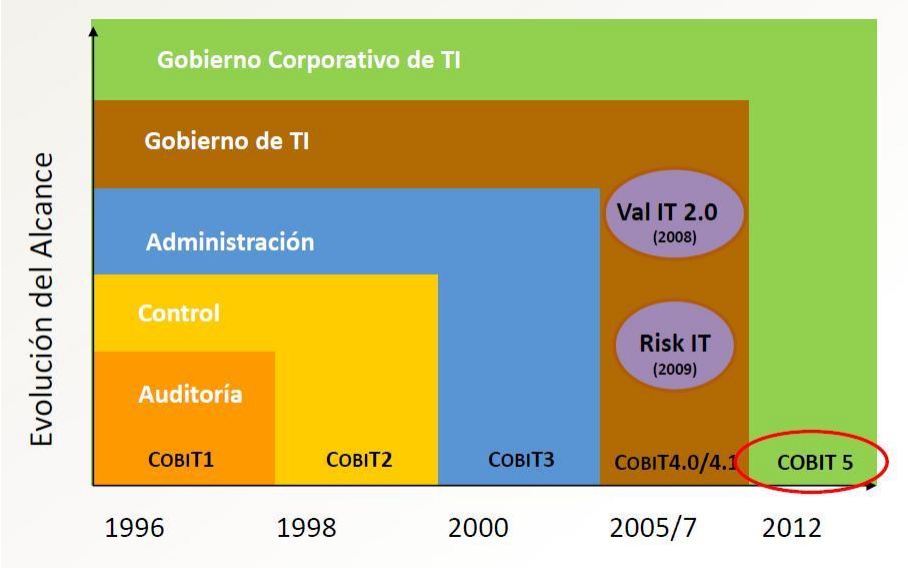
Gráfico 5: Metodología COBIT



Fuente:https://www.google.com.ec/search?q=cobit&espv=2&biw=1600&bih=799&source=lnms&tbm=isch&sa=X&ei=qJSRVa79MsO_sAX627yABg&ved=0CAYQ_AUoAQ#tbm=isch&q=cobit+FORMA+DE+TRABAJO&imgrc=psAM8Imyol6A3M%3ª

8.6 Procesos para el desarrollo de COBIT 4.1

Grafico 6: COBIT 4.1



Fuente: www.Isaca.com

Ruther R. (2012). Plantea que COBIT 4.1 está orientado a la creación del Gobierno de TI, tomando en consideración los objetivos primordiales que se debe tomar en cuenta en cada dominio, pero el principal objetivo de esta etapa es aplicar el tercer y cuarto dominio el cual está enfocado en entregar y dar soporte y el monitoreo.

Los Recursos de IT necesitan ser administrados por un conjunto de procesos agrupados en forma natural, con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos.

Resulta claro que las medidas de control no satisfarán necesariamente los diferentes requerimientos de información del negocio en la misma medida.

Por esa razón los procesos en COBIT satisfacen uno o varios criterios de la información de la siguiente manera:

(P) Primario.- es el grado al cual el objetivo de control definido impacta directamente el requerimiento de información de interés.

(S) Secundario es el grado al cual el objetivo de control definido satisface únicamente de forma indirecta o en menor medida el requerimiento de información de interés.

Blanco (vacío) podría aplicarse; sin embargo, los requerimientos son satisfechos más apropiadamente por otro criterio en este proceso y/o por otro proceso.

Procesos COBIT 4.1

Tabla 1: Proceso COBIT 4.1

Procesos y Objetivos de Control COBIT 4.1	
PLANIFICACION Y ORGANIZACIÓN	
PO1	Definen un Plan de TI Estratégico
PO2	Definen la Información Arquitectura
PO3	Determinan Dirección Tecnológica
PO4	Definen los Procesos de TI, Organización y Relaciones
PO5	Manejan la Inversión TI
PO6	Comunican Objetivos de Dirección y Dirección
PO7	Manejan Recursos TI Humanos
PO8	Manejan Calidad
PO9	Evalúan y Manejan Riesgos de TI
P10	Manejan Proyectos
ADQUISICION	
AI1	Identifican Soluciones Automatizadas
AI2	Adquieren y Mantienen Software De aplicación
AI3	Adquieren y Mantienen Infraestructura de Tecnología
AI4	Permiten Operación y Usan AI5 Procuran Recursos TI
AI6	Manejan Cambios
AI7	Instalan y Acreditan Soluciones y Cambios
ENTREGAR Y DAR SOPORTE	
DS1	Definición y administración de los niveles de servicio
DS2	Administración de los servicios de terceros.
DS3	Administración del desempeño y capacidad de TI
DS4	Garantías en la continuidad del servicio
DS5	Garantías en la seguridad de los sistemas.
DS6	Identificación y asignación de costos de TI.
DS7	Educación y entrenamiento a los usuarios
DS8	Administración de la mesa de servicios de TI y los incidentes.

DS9	Administración de la configuración de TI.
DS10	Administración de los problemas con TI.
DS11	Administración de los datos.
DS12	Administración del ambiente físico
DS13	Administración de las operaciones de TI.
MONITOREAR Y EVALUAR	
ME1	Monitoreo y evaluación del desempeño de TI.
ME2	Monitoreo y evaluación el control interno.
ME3	Garantías en el cumplimiento regulatorio
ME4	Proporciona gobierno de TI

Fuente: www.ISACA.com

8.7 Grupo KFC

La empresa **GRUPO KFC** se encuentra ubicada en la Av. Corea y amazonas edificio Belmonte, siendo sede central donde se realizan los manejos de datos y demás acciones pertenecientes a la cadena de restaurantes más grande en el Ecuador.

Función

Su función principal es la comercialización y venta de productos de comida rápida, la cual maneja alrededor de 11 empresas

Sistema Organizacional.

La organización de la empresa es de manera ordenada ya que existen varios procesos que conlleva el trabajo para beneficio de la empresa, dichos trabajos se efectúan en cada piso del edificio perteneciente a la empresa, teniendo en cuenta que existen varias áreas de trabajo como el de sistemas, contabilidad, políticas y leyes, diseño gráfico, artes, eléctrica, entre otras áreas de trabajo.

Área de sistemas

El área de sistemas es de vital importancia para una empresa, es el departamento encargado de incorporar las nuevas tecnologías, optimizar los procesos e implementar soluciones innovadoras para las organizaciones, por lo que contar con un equipo bien preparado es imprescindible.

Departamento de Sistemas Grupo KFC

Gran parte de la actividad que se desarrolla en el Área de Sistemas (Departamento de IT) del GRUPO KFC corresponde a la administración, configuración, instalación, y al soporte a los usuarios el cual utilizan un medio electrónico ya sea en las oficinas o en los locales de comida pertenecientes al GRUPO KFC en los cuales se labora, con los objetivos de garantizar, mejorar, optimizar e integrar los procesos que se llevan a cabo en cada área perteneciente al área o en los locales en los que se brinda un correcto servicio al cliente, como también facilitar su utilización a todos los sectores de la comunidad de la Empresa.

Esta labor se desarrolla en tareas como éstas:

- Mantenimiento de los equipos, detección y resolución de averías.
- Sintonía del sistema operativo y optimización del rendimiento.
- Gestión de cuentas de usuario y asignación de recursos a las mismas.
- Preservación de la seguridad de los sistemas y de la privacidad de los datos de usuario, incluyendo copias de seguridad periódicas.
- Evaluación de necesidades de recursos (memoria, discos, unidad central) y provisión de los mismos en su caso.
- Instalación y actualización de utilidades de software.
- Atención a usuarios (consultas, preguntas frecuentes, información general, resolución de problemas, asesoramiento, etc.).
- Organización de otros servicios como copia de ficheros en cinta, impresión desde otros ordenadores en impresoras dependientes de estos equipos.

DESCRIPCIÓN DE LAS ÁREAS: El Departamento de Sistemas del Grupo KFC, cuenta en los actuales momentos con las siguientes áreas:

1.- Área de ERP: Tiene a cargo las siguientes funciones.

- Desarrollar soluciones mediante programación.
- Mejorar los requerimientos en el sistema informático.
- Planificación de actividades para el mejoramiento continuo del ERP.
- Resolver inconvenientes que no pueden ser resueltos internamente con la ayuda del proveedor.

- Desarrollo de interfaces para integrar los procesos que se manejan internamente.
- Soluciones en inconvenientes de procesos internos y de calidad de desarrollo de nuevos o cambios de requerimientos.

2.- Área de Soporte: Tiene a cargo las siguientes funciones.

- Solución de inconvenientes en el manejo de sistema de call center ELASTIXS (llamadas entrantes, salientes, tiempos de descanso, tiempos de espera, tiempos de servicio).
- Solución de inconvenientes en el manejo del sistema ARANDA (registro cliente)
- Solución de inconvenientes a usuarios de locales en operaciones de implementación o adecuación de servicios informáticos.
- Resolver problemas de Hardware en locales Y oficinas del CAR.
- Revisión de Problemas de Ofimática de Usuarios

3.- Área de Desarrollo y Proyectos: Tiene a cargo las siguientes funciones.

- Análisis de requerimientos de proyectos, el cual debe cumplirse en el tiempo estimado, teniendo en cuenta la interfaz y la codificación del programa.
- Seguridad de bases de datos de sistemas y aplicaciones
- Mejora de procesos e innovaciones de Sistema Gerente –Domicilio – Autoimpresores
- Soporte necesario a los niveles de servicio.
- Solución para restaurar un servicio de TI (Nómina, Línea de producción, Facturación).
- Documentación de requerimientos de procesos del negocio para automatizarlos de forma precisa.

4.- Área de Infraestructura: Tiene a cargo las siguientes funciones.

- Solución de inconvenientes en la estructura física de la red (cableado, equipos de red, WIFI, etc.)
- Solución a inconvenientes en los Servicios de: Correo Electrónico Institucional, Servidores Web, Servicio DNS, entre otros
- Mejorar continuamente la implementación/instalación de la infraestructura de la red con el objetivo de incrementar la confiabilidad de la Red
- Solución de inconvenientes de Hardware y Software que prestan servicio.
- Solución de inconvenientes sobre la Instalación y Operación de los puntos de Red.

5.- Área de Soporte CAR y Planta: Tiene a cargo las siguientes funciones.

- Instalación de laptops y desktops bajo parámetros establecidos por la empresa sobre software.
- Mantenimiento y ensamblaje de equipos
- Backup de Información (Respaldo y recuperación de archivos)
- Configuración de impresoras en RED y MATRICIALES (Solución de inconvenientes).
- Solución de inconvenientes a usuarios en operaciones de implementación o adecuación de servicios informáticos.
- Realización y control de copias de seguridad de la información sensible de la empresa.
- Revisión de Problemas de Ofimática de Usuarios

6.- Área de Business Intelligence: Tiene a cargo las siguientes funciones

- Definición de Metodologías para la correcta administración de procesos de desarrollo de Inteligencia de Negocios.
- Estrategias para la implementación de soluciones BI
- Administración del desarrollo de proyectos de inteligencia de negocios que permitan mantener actualizada la plataforma de información de la empresa.
- Administración del correcto funcionamiento del Data Ware House
- Implementación y mantenimiento continúo a las soluciones BI.
- Desarrollo de estrategias para el mejoramiento de calidad de datos de las diferentes líneas de negocio de la compañía, tanto como la información existente como la información que se ingrese en un futuro.

9. PREGUNTAS CIENTÍFICAS O HIPÓTESIS:

9.1 Hipótesis.

La aplicación de una Auditoría Informática utilizando la metodología COBIT 4.1, permitirá comprobar el manejo de la información y el control de procesos con el que trabajan las determinadas áreas pertenecientes al Departamento de Sistemas".

9.1.1 Variable Independiente

Aplicación de una Auditoría Informática utilizando la metodología COBIT 4.1.

9.1.2 Variable Dependiente

Comprobar el manejo de la información y el control de procesos con el que trabajan las determinadas áreas pertenecientes al Departamento de Sistemas.

10. METODOLOGÍAS Y DISEÑO EXPERIMENTAL

10.1 Población y muestra

A continuación se presentan las personas pertenecientes al Departamento de Sistemas que han sido tomadas en cuenta para que contribuyan en la Investigación planteada y que de esta manera la información recopilada sea de personas confiables por ende sea considerado como información verídica.

INVOLUCRADOS DEPARTAMENTO SISTEMAS GRUPO KFC	**CANTIDAD**
Coordinadores de cada área	6
Gerente General	1
Subgerente	1
Personal que labora en cada área	42
Total	**50**

Fuente: Departamento de sistemas-Grupo KFC.

10.2 Técnicas e instrumentos para recolección de información

Las técnicas de investigación permitirán la recolección de la información, hechos o documentos a los que se podrá acudir para el desarrollo de la investigación planteada; es por esto que se ha optado por la utilización de técnicas primarias que a continuación se detalla.

No.	TÉCNICAS	INSTRUMENTOS
1	Encuesta	Cuestionario
2	Entrevista	Formulario de preguntas
3	Observación	Fichas de Observación
4	Recopilación documental	Checklist

Fuente: www.monografias.com

10.3 Plan de auditoría informática COBIT 4.1

El marco metodológico para realizar la auditoría informática en el departamento de sistemas perteneciente al Grupo KFC usando el modelo de mejores prácticas COBIT 4.1, fue el siguiente:

1. Cronograma de actividades (**Ver anexo 1**)
2. Seleccionar los criterios de la Información acerca de los procesos que se lleva a cabo en cada área utilizando técnicas e instrumentos para recopilar información.

2.1 Objetivos de los instrumentos de recolección de información

- Proporcionar evidencia del trabajo realizado y de las conclusiones obtenidas
- Ayudar al equipo de trabajo para que adopte una estructura ordenada y uniforme para la presentación del trabajo.
- Facilitar la supervisión y revisión del trabajo realizado, así como dejar evidencia que dicha supervisión que fue hecha, será útil en futuros trabajos o revisiones de la auditoría.
- Mantener el registro de información para sustentar las declaraciones y los informes.
- La información que se incluya en los papeles de trabajo debe ser clara, completa y concisa.
- Debe dar testimonio verídico e inequívoco del trabajo realizado.
- Debe contener las razones que fundamenten decisiones en aspectos controvertidos.
- Deben cumplir con los más altos parámetros de calidad y así mismo limitarse en cantidad.
- No debe elaborarse para transcribir o copiar información ni para que los auditados los diligencien.

- Documentar la información que podría ser útil en futuros trabajos o revisiones de la auditoría.

2.2. Contenido de los instrumentos de recolección de información

- Descripción de las tareas que realizan cada área.
    - Determinar KPIs
- Los datos y antecedentes obtenidos durante la auditoría.
    - Checklist
- Información relevante sobre la actividad u operación del área auditada.
    - Cuestionario (**Ver anexo 4**)
    - Entrevista (**Ver anexo 5**)
- Recopilación de información y riesgos existentes.
    - Cedula de hallazgos (**Ver anexo 6**)

3. Selección de los 34 procesos de COBIT, cuales son los procesos que son impactados de manera primaria por los criterios de la información relacionados con la seguridad.
4. Desarrollo de las etapas de auditoría (dominios COBIT 4.1)
    - Dominio Planificación y organización
    - Dominio Adquisición
    - Dominio Entrega y Soporte
    - Dominio Monitoreo
5. Evaluación utilizando la aplicación MSAT (Herramienta de Evaluación de Seguridad de Microsoft) el cual se enfoca en obtener datos reales del área tecnológica (Departamento de Sistemas) para emitir los resultados en porcentajes y gráficas el cual determinan los riesgos existentes de inseguridad.
6. Elaboración de los planes de acción (Estrategias) que incluyen los controles, para poder mitigar los riesgos de alta y media exposición.
7. Creación de las políticas de seguridad en base a las políticas que establece ISACA (Sistemas de Información de Auditoría y Control) perteneciente a la organización mundial SANS (Formación en seguridad), enfocada para organizaciones grandes que precautelan su información de manera confidencial y a la vez la correcta organización de la misma.

10.4 Desarrollo de las etapas de auditoria

10.4.1 Dominio Planificación y organización

Presentación del área auditada (Departamento de Sistemas-Grupo KFC)

GRUPO KFC: Su función principal es la comercialización y venta de productos de comida rápida, la cual maneja alrededor de 17 marcas, una variedad de productos de buena calidad, con una excelente atención al cliente, factores que le han permitido posicionarse en el mercado en diferentes provincias del país.
Además de la organización proporciona fuentes de empleo en todas sus áreas, ofreciendo un buen ambiente laboral, buen trato, remuneraciones acordes al desempeño y todas las bonificaciones de ley.

El enfoque de este trabajo dentro de lo que corresponde al Departamento de Sistemas (IT) es el controlar el ambiente informatizado, con herramientas de supervisión, para que la empresa logre niveles de excelencia en el cuidado y aprovechamiento de los datos, y en conjunto con los involucrados aplicar soluciones que optimicen sus recursos informáticos.

Es necesario recordar que el Departamento de Sistemas (IT) tiene objetivos comunes entre todos los departamentos respecto al uso de los recursos informáticos y mediante el aprovechamiento de la tecnología mediante políticas, procedimientos y métodos apropiados propende a que el servicio al usuario-cliente sea de calidad. En este sentido, el papel que cumple la Auditoría Informática es que se convierte en un medio muy importante para lograr dicho fin.

Matriz FODA del Departamento de Sistemas

Análisis FODA del Departamento de Sistemas (IT) Luego de un análisis mediante observación, indagación y entrevistas se identificaron las fortalezas, oportunidades, debilidades y amenazas en general del Departamento de Sistemas (**Ver Tabla 2**).

Determinación de KPIs de cada área.

Para determinar los KPIs se tomó en consideración las entrevistas y cuestionarios de preguntas realizadas para la recopilación de la información el cual se tomó en consideración de qué manera se trabaja en cada área, las principales actividades en las que se proyecta cada

área al igual que un porcentaje el cual deduce el cumplimiento de cada función. (**Ver anexo 2**).

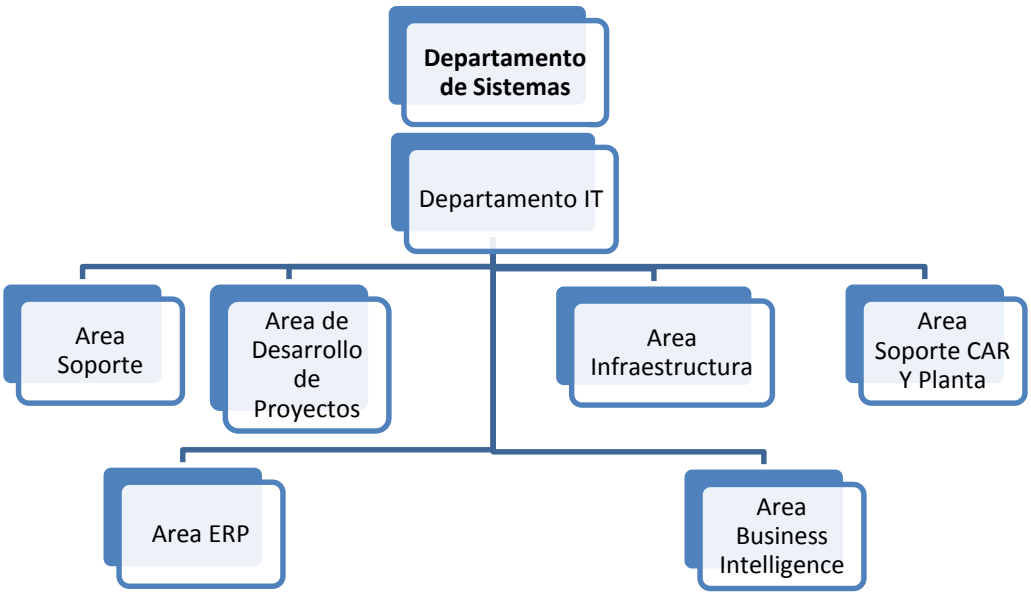
Checklist "Información de gestión de la seguridad BS ISO IEC 17799: 2005 SANS".

Se realizó una evaluación utilizando el Checklist ISO, el cual está enfocado en realizar un control de lo que se está realizando de correcta manera, determinando si cumple o no cumple con aspectos determinados en el formato. (**Ver Gráfico 18**)

Áreas examinadas:

Las áreas que se examinaron en el Departamento de Sistemas (IT) para realizar la Auditoría Informática fueron; Soporte, Desarrollo y Proyectos, Infraestructura, Soporte CAR y Plantas, ERP, Business Intelligence.

Organigrama Estructural del Departamento de Sistemas.



Fuente: Departamento de sistemas-Grupo KFC.

Hay que tener en cuenta los aspectos principales en los que se enfoca la metodología COBIT 4.1.

- Hardware.
- Software.
- Redes.
- Seguridad e integridad.

Servicios informáticos de acuerdo a los objetivos institucionales

Para evaluar la tecnología y recursos informáticos con los que cuenta esta dirección se realizó una entrevista a Xavier Gómez Gerente del Departamento de Sistemas (IT), adicionalmente se partió de los objetivos institucionales que se deben dar cumplimiento en cada área.

Como también se puede evidenciar en los Análisis de resultados las gráficas obtenidas en base a los instrumentos y técnicas aplicadas para la recopilación de información.

10.4.2 Adquisición e implementación

Con este dominio se identifica soluciones de Tecnologías Informáticas (TI) adquiridas o desarrolladas, y por supuesto hacerlas operativas, integrándolas como procedimientos del día a día, lo que permite ser mejores y tener una continuidad operativa.

Se puede visualizar en el análisis de resultados las tablas en el cual se determina el Hardware y Software que utilizan en el Departamento de Sistemas al igual que se detalla la ubicación y organización del DATA CENTER el cual almacena información confidencial proveniente de los procesos que se realizan en cada área.

Evaluación utilizando la aplicación MSAT (Herramienta de Evaluación de Seguridad de Microsoft) el cual se enfoca en obtener datos reales del área tecnológica para emitir un los resultados en porcentajes y gráficas el cual determinan los riesgos existentes de inseguridad. (**Gráfico 17**)

10.4.3 Entrega y Soporte

Mediante este dominio se llega a comprender las actividades de soporte a los sistemas en producción. En esta área se incluye el procesamiento de los datos por sistemas de aplicación.

Se puede visualizar en el análisis de resultados la manera en la que trabaja el Departamento de Sistemas, cumpliendo con un porcentaje valorado al 100% el cual determina los procesos del dominio si cumplen de manera general.

Efectividad	Información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
Eficiencia	Provisión de información a través de la utilización óptima (más productiva y económica) de recursos.

Confidencialidad	Protección de información sensible contra divulgación no autorizada.
Integridad	Precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.
Disponibilidad	Disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
Cumplimiento	Cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo criterios de negocio impuestos externamente.
Confiabilidad de la información	Provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

Fuente: http://www.monografias.com/trabajos38/cobit/cobit.shtml

Los recursos de TI identificados en COBIT 4.1, es la estructura en la que está enfocada cada matriz como se detalla en la tabla.

Datos	Los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.
Aplicaciones	Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.
Tecnología	La tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.
Instalaciones	Recursos para alojar y dar soporte a los sistemas de información.
Personas	Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

Fuente: http://www.monografias.com/trabajos38/cobit/cobit.shtml.

Criterios de la seguridad

Los criterios de la seguridad usados a nivel mundial por los modelos de mejores prácticas y estándares son los siguientes:

Confidencialidad	Protección de información sensible contra divulgación no autorizada.
Integridad	Precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

Disponibilidad	Disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

Fuente: http://www.monografias.com

Los procesos en COBIT satisfacen uno o varios criterios de la información de la siguiente manera, el cual para llenar la matriz se enfoca en los siguientes aspectos.

(P) Primario.- es el grado al cual el objetivo de control definido impacta directamente el requerimiento de información de interés.

(S) Secundario es el grado al cual el objetivo de control definido satisface únicamente de forma indirecta o en menor medida el requerimiento de información de interés.

Blanco (vacío) podría aplicarse; sin embargo, los requerimientos son satisfechos más apropiadamente por otro criterio en este proceso y/o por otro proceso.

Se toma en consideración de que manera es la seguridad del Departamento de Sistemas mediante la investigación a realizar.

Seguridad del Departamento

a. Seguridad Física

- Proteger el área del data center frente a posibles inundaciones.
- Contar con las instalaciones eléctricas adecuadas para resguardar la integridad de los equipos.
- Un lugar adecuado y fresco que mantenga los servidores trabajando a temperaturas ideales.

b. Seguridad legal:

- Aplicación de estándares y metodologías de calidad (IEE, ISO, TIER, entre otros) de manera tal que se garantice la ejecución de procesos blindados y seguros.
- Adquirir las licencias de los sistemas operativos (Microsoft) en uso, de igual forma con antivirus u otro software: esto para no incurrir en faltas legales.
- Contar con las licencias de los sistemas.

c. Seguridad de Datos

- Ejecutar las tareas de respaldo según la planificación
- Establecer niveles de acceso acordes a la realidad tanto para los sistemas de información como la de los servidores, para impedir acceso y manipulación no autorizada a la información.

d. Seguridad de personas

- Instituir políticas de seguridad física y mental para el personal.
- Dotar al departamento con las herramienta de protección necesarias para garantizar la seguridad de los empleados.
- Instruir a los empleados de cómo actuar ante situaciones de desastre (incendios, inundaciones, sismos, entre otros).

10.4.4. Monitoreo

Mediante este dominio todos los procesos de TI (Tercer y cuarto dominio) deben ser evaluados regularmente, tanto en cuanto a su calidad, como al cumplimiento de los requerimientos de control.

Procesos y Objetivos de Control COBIT	
ENTREGAR Y DAR SOPORTE	
DS1	Definición y administración de los niveles de servicio
DS2	Administración de los servicios de terceros.
DS3	Administración del desempeño y capacidad de TI
DS4	Garantías en la continuidad del servicio
DS5	Garantías en la seguridad de los sistemas.
DS6	Identificación y asignación de costos de TI.
DS7	Educación y entrenamiento a los usuarios
DS8	Administración de la mesa de servicios de TI y los incidentes.
DS9	Administración de la configuración de TI.
DS10	Administración de los problemas con TI.
DS11	Administración de los datos.
DS12	Administración del ambiente físico
DS13	Administración de las operaciones de TI.
MONITOREAR Y EVALUAR	
ME1	Monitoreo y evaluación del desempeño de TI.
ME2	Monitoreo y evaluación el control interno.
ME3	Garantías en el cumplimiento regulatorio
ME4	Proporciona gobierno de TI

Fuente: http://www.monografias.com/cobit/cobit.shtml

Tabla genérica acerca del Modelo de Madurez

Se toma en consideración los siguientes detalles para evaluar el tercer (Entrega y soporte) y cuarto (Monitoreo) dominio el cual determina el porcentaje de madurez del Departamento de Sistemas.

MODELO GENERICO DE MADUREZ COBIT		
0	No Existente	Carencia completa de cualquier proceso reconocible. La institución no ha reconocido siquiera que existe un problema a resolver.
1	Inicial	Existe evidencia que la institución ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.
2	Repetible	Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.
3	Definido	Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.
4	Administrado	Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.
5	Optimizado	Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras instituciones. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la institución se adapte de manera rápida.

Fuente: http://www.monografias.com/cobit/cobit.shtml

Políticas de seguridad

Una vez finalizado el proceso de la metodología se tomó en consideración la creación de las Políticas de seguridad en base a las políticas que establece ISACA (Sistemas de Información de Auditoría y Control) perteneciente a la organización mundial SANS (Formación en seguridad), enfocada para organizaciones grandes que precautelan su información de manera confidencial y a la vez la correcta organización de la misma. (**Ver anexo 10**).

Estrategias

Como también se creó estrategias (plan de acción y acuerdo de confidencialidad) para controlar los procesos que se llevan a cabo dentro de cada área perteneciente al Grupo KFC.

- **Plan de acción**

  Documento realizado para controlar de qué manera se están cumpliendo los procesos de acuerdo al área en la que pertenece cada jefe, tomando en consideración que es la persona encargada de revisar en qué estado de cumplimiento se encuentra cada proceso. (**Ver anexo 11**)

- **Acuerdo de Confidencialidad**

El propósito del acuerdo de confidencialidad es la creación de un documento formal el cual detalle las condiciones o políticas de privacidad que deben cumplir los proveedores que se relacionan a diario con cada una de las áreas y manejan la información confidencial de la empresa. **(Ver anexo 12)**

11. ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS

11.1 Dominio Planificación y organización

TABLA 2: Análisis FODA

FORTALEZAS	**OPORTUNIDADES**
Buen nivel de conocimiento técnico Equipo humano homogéneo Servicio de gran calidad y especializado en el área. Infraestructura física actualizada para cada área del Departamento de Sistemas.	Participación en proyectos institucionales. Servicio eficaz y eficiente por parte de cada área del Departamento de Sistemas. Nuevos servicios
DEBILIDADES	**AMENAZAS**
Espacio físico limitado Economía	Falta de una normativa adecuada Altos costos de la tecnología

FUENTE: Departamento de Sistemas

TABLA 3: Diagnóstico documental departamento de sistemas

RECURSOS		
EXISTENTES		**NO EXISTENTES**
1°	Inventario contable de Hardware (Incompleto Mouse, Teclado, Monitor)	Normativas para el uso de Internet
2°	Contratos de servicios profesionales sobre recursos informáticos	Cronograma de capacitación al personal.
3°	Organigrama del Departamento IT	Monitoreo de mantenimiento de Hardware,

4°	Software con licencia (Sistema Operativo)	Plan de actualización de Hardware/Software.
5°	Manual del usuario	Políticas para la adquisición de equipos informáticos.
6°		Página Web (Internet).
7°		Inventario de Software

Fuente: Formulario de visita Previa

11.2 Adquisición e implementación

Existe el Hardware y Software necesario para realizar los procesos en los que se enfoca el Departamento de Sistemas, pero se debe tomar en consideración Software el cual se pueda administrar la información de manera segura y confiable **(Ver Anexo 7)**

11.3 Entrega y Soporte.

Entrega y Soporte se preocupa de la entrega de servicios requeridos y de garantizar la seguridad y continuidad de operaciones tradicionales, en el **Anexo 8** se puede evidenciar la matriz correspondiente a los 13 procesos del mencionado dominio tomando en consideración aspectos importantes como los criterios de información en los que se enfoca la metodología, los cuales se detalla a continuación.

IMPACTO SOBRE LOS CRITERIOS DE INFORMACIÓN		
CRITERIOS DE LA INFORMACIÓN	**PORCENTAJE**	**OBSERVACIONES**
Efectividad	100 %	La información es entregada de forma oportuna, correcta, consistente y utilizable.
Eficiencia	95 %	El objetivo es alcanzar el 100%, para esto se debe capacitar a los usuarios de tal manera que puedan alcanzar un buen desempeño al momento de utilizar las aplicaciones.
Confidencialidad	88, 57%%	El objetivo es alcanzar el 100%, para lo cual se debe proteger la información sensitiva contra revelación no autorizada, y realizar una auditoría

		independiente.
Integridad	88 %	El objetivo es alcanzar el 100%, para lo cual la información debe ser precisa, completa y valida.
Disponibilidad	84,62 %	El objetivo es alcanzar el 100%, para lo cual la información debe estar disponible cuando esta se requiera por parte de las áreas del negocio en cualquier momento.
Cumplimiento	82,85 %	El objetivo es alcanzar el 100%, para lo cual se debe respetar las leyes, reglamentos y acuerdos contractuales a los que está sujeta el proceso del negocio, como políticas internas.
Confiabilidad	86 %	El objetivo es alcanzar el 100%, para lo cual se debe proporcionar la información apropiada, con el fin de que la Gerencia General administre la entidad.

Fuente: http://www.monografias.com/cobit/cobit.shtml

Informe Estadístico

En el Informe Estadístico se detalla los resultados de la evaluación a cada uno de los 34 procesos que recomienda COBIT 4.1, siendo evaluado y enfocado al dominio 3 y 4 generando 18 procesos importantes en lo que determinan los procesos que se cumple en cada área del Departamento de Sistemas.

Los criterios de información que resumen las gráficas de cada Matriz y en los aspectos que se enfoca COBIT en evaluar dentro de una organización se encuentran en el siguiente porcentaje todos sobre el 100%.

Gráficos estadísticos del impacto sobre los criterios de información, obtenidos de la matriz COBIT 4.1.

Efectividad

Gráfico 7: Efectividad

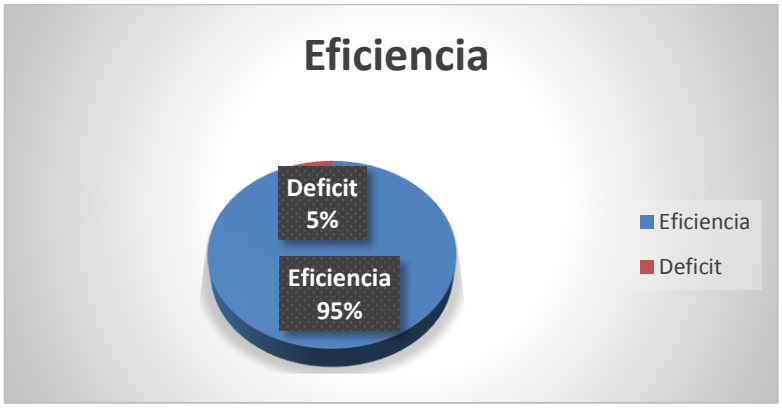
Realizado por: Daniel Ortiz

Análisis

La efectividad consiste en que la información relevante sea entregada de forma oportuna, correcta, consistente y utilizable, este criterio tiene un promedio del 100% de efectividad en el Departamento de Sistemas ya que los procesos, actividades y objetivos propuesto por cada jefe de área se cumple de manera importante ya que la prioridad es el cliente por lo tanto los objetivos planteados por el Departamento de Sistemas se enfoca en tener un alto porcentaje de cumplimiento al momento de cumplir con las actividades, mientras que en un 0% existe un déficit de cumplimiento, determinando que no existe dificultades al momento de realizar los procesos y actividades correspondientes a cada área.

Eficiencia

Gráfico 8: Eficiencia



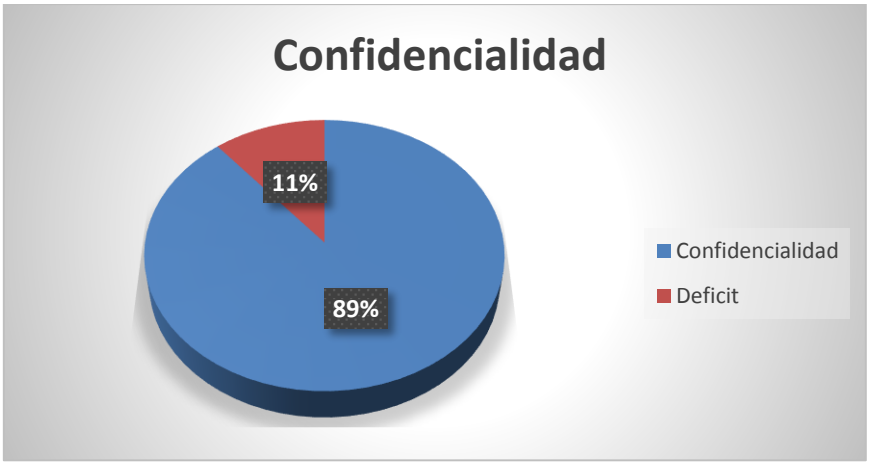
Realizado por: Daniel Ortiz

Análisis

El objetivo es alcanzar el 100%, para esto se debe capacitar a los usuarios de tal manera que puedan alcanzar un buen desempeño al momento de utilizar las aplicaciones, por lo tanto el porcentaje de eficiencia es de 95% y un déficit de 5% esto quiere decir que en su mayoría los usuarios saben utilizar las aplicaciones desarrolladas por el Departamento de Sistemas.

Confidencialidad

Gráfico 9: Confidencialidad



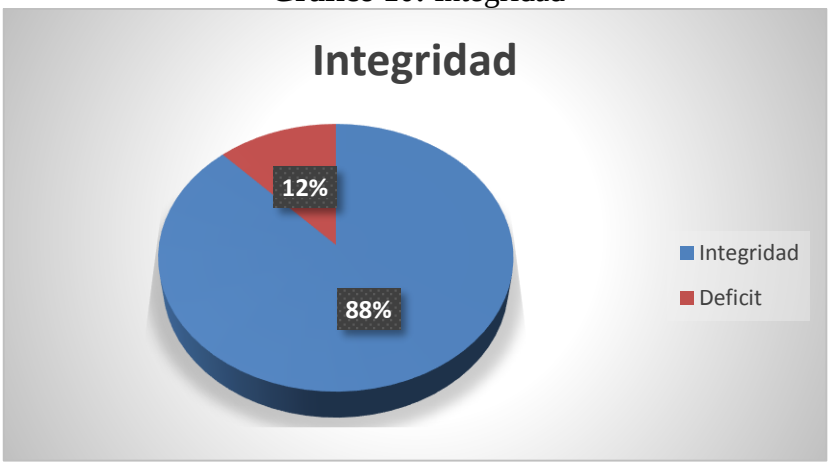
Realizado por: Daniel Ortiz

Análisis

El objetivo es llegar a un 100% en seguridad de la información, esto quiere decir que se debe proteger la información sensitiva contra revelación no autorizada, y realizar una auditoría independiente, realizando documentos, actas de confidencialidad el cual pueda determinar el grado de importancia cuando se utilice dicha información privada, determinando el 89% de Confidencialidad, mientras que en un 11% existe déficit ya que no se realiza con documentos formales el manejo de la información confidencial

Integridad

Gráfico 10: Integridad



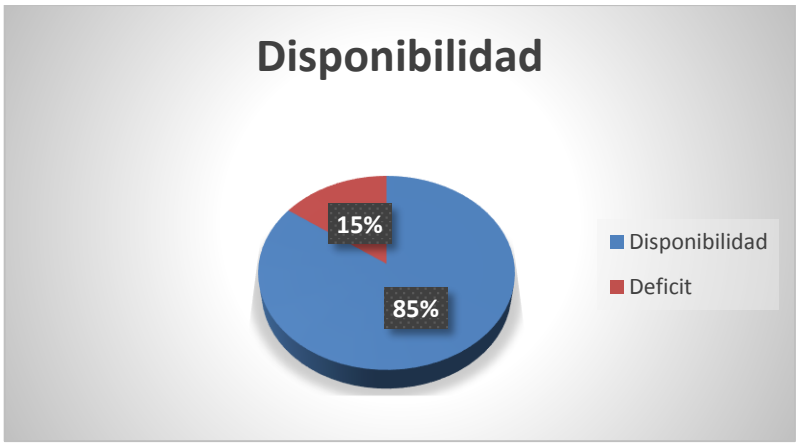
Realizado por: Daniel Ortiz

Análisis

La integridad consiste en que la información debe ser precisa, completa y válida para obtener el 100%, este criterio tiene un promedio del 88% ya que no se maneja un proceso adecuado para administrar y determinar las actividades que se realizan dentro de cada área, siendo un pilar muy importante ya que en el Departamento de Sistemas cada área comparte información confidencial con otras áreas según los objetivos planteados, y un déficit de 12% el cual determina que existe un bajo porcentaje de procesos mal documentados.

Disponibilidad

Gráfico 11: Disponibilidad



Realizado por: Daniel Ortiz

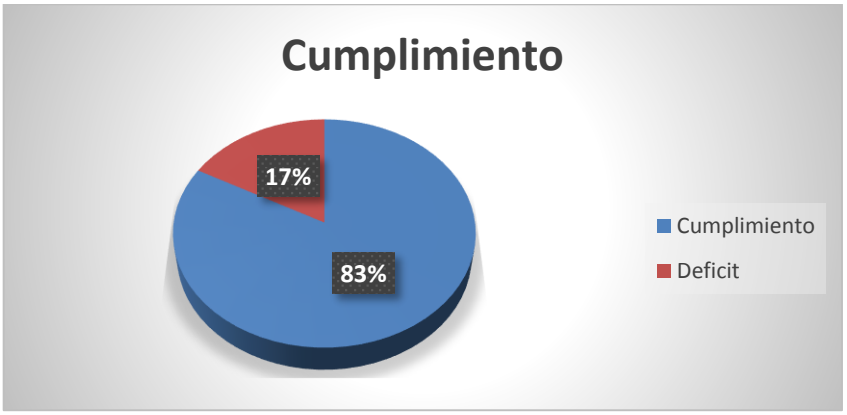
Análisis

La disponibilidad consiste en que la información esté disponible cuando esta sea requerida por parte de las áreas del negocio en cualquier momento, este criterio tiene un promedio de 85%, esto quiere decir que existe en las áreas intercambio de información pero no en todas ya que

existen áreas que manejan robustas bases de datos como lo es Infraestructura el cual maneja y administra las bases de datos de la mayoría de área del Departamento de Sistemas, y un déficit de 15% en lo que se mencionó que en el área de Infraestructura no se maneja con facilidad la información con otras áreas ya que se tiene que seguir un proceso para poder obtener acceso a la información.

Cumplimiento

Gráfico 12: Cumplimiento



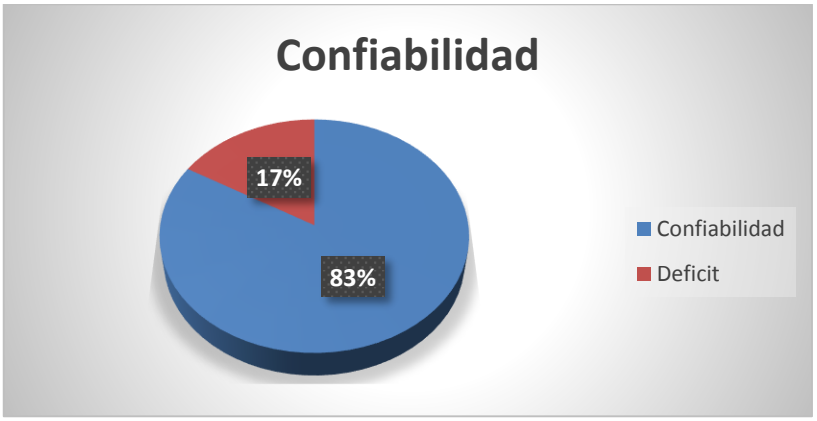
Realizado por: Daniel Ortiz

Análisis

El cumplimiento consiste en que se debe respetar las leyes, reglamentos y acuerdos contractuales a los que está sujeta el proceso del negocio para obtener un 100%, este criterio tiene un promedio del 83% debido a que en el Departamento de Sistemas se cumple a cabalidad con las reglas y propósitos que se deben cumplir pero existe un déficit de 17% porque no existen políticas de seguridad tanto para el Departamento de Sistemas como para cada área perteneciente al Departamento.

Confiabilidad

Gráfico 13: Confiabilidad



Realizado por: Daniel Ortiz

Análisis

El objetivo de confiabilidad consiste en que se debe respetar, proporcionar la información apropiada, con el fin de que la Gerencia General administre la entidad para poder obtener un alto porcentaje 100%, este criterio tiene un promedio del 83% debido a que existen procesos que se deben realizar de manera confiable ya sea utilizando documentos formales de confidencialidad con proveedores externos o de manejo de información confidencial interno determinando un déficit de 17% ya que no existe un proceso formal de manejo de información.

Evaluación del cumplimiento de objetivos en el Departamento de Sistemas a nivel general, enfocado a los KPIs determinados en cada área.

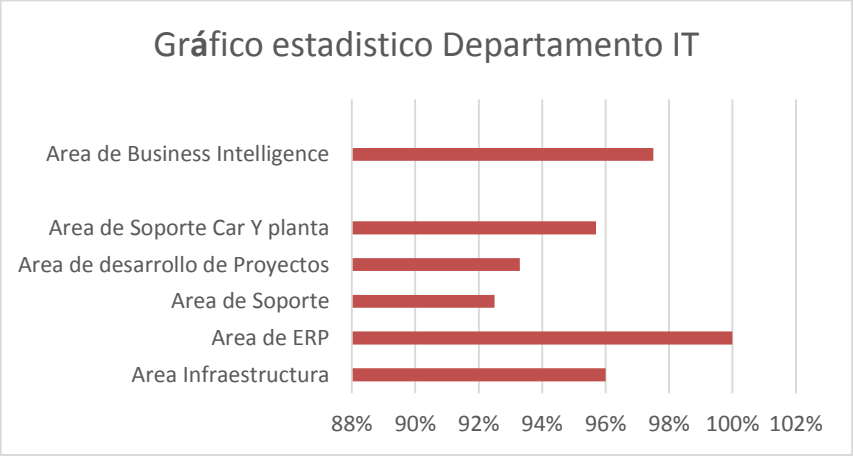
Áreas Departamento IT	Porcentaje
Área Infraestructura	96%
Área de ERP	100%
Área de Soporte	92,50%
Área de desarrollo de Proyectos	93,30%
Área de Soporte Car y planta	95,70%
Área de Business Intelligence	97,50%

Fuente: Determinación de KPI

Análisis

La tabla representa el porcentaje de cumplimiento de actividades en cada área del Departamento de Sistemas, obteniendo indicadores principales (KPI) de cada área, el cual se pudo determinar utilizando el método de semáforo para determinar KPI, el que consiste en evaluar el grado de cumplimiento de cada área utilizando los colores del semáforo como el verde el cual deduce que es un desempeño aceptable, amarillo es un desempeño preocupante y rojo es un desempeño inaceptable, analizando cada indicador principal perteneciente a cada área, como se puede evidenciar en el **Anexo 2.**

Gráfico 14: Porcentaje KPIs



Fuente: KPI'S obtenidos en el Departamento IT

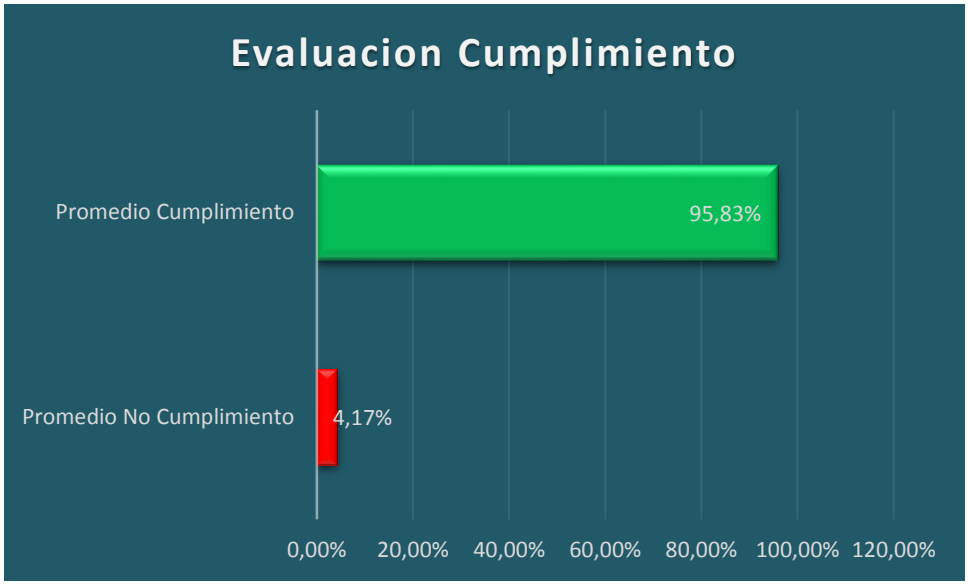
Elaborado: Daniel Ortiz

Nivel de Cumplimiento del Departamento de Sistemas en base a los KPI'S obtenidos

Evaluación del cumplimiento a nivel general	
Promedio Cumplimiento	95.83 %
Promedio No Cumplimiento	4.17 %

Fuente: Determinación de KPI

Gráfico 15: Cumplimiento



Fuente: Información obtenida de los KPI'S del Departamento IT

Elaborado: Daniel Ortiz

Análisis:

En el análisis de cumplimiento se verifica que el departamento de sistemas obtuvo un porcentaje de 95,83%, hay que tomar en cuenta que únicamente los indicadores (KPI) determinan si cumplen o no con los objetivos propuestos cada área mas no el proceso que se lleva a cabo para cumplirlos, el cual es considerado como un nivel aceptable, con relación al modelo de madurez de COBIT 4.1 se lo ubicaría en el nivel 3.

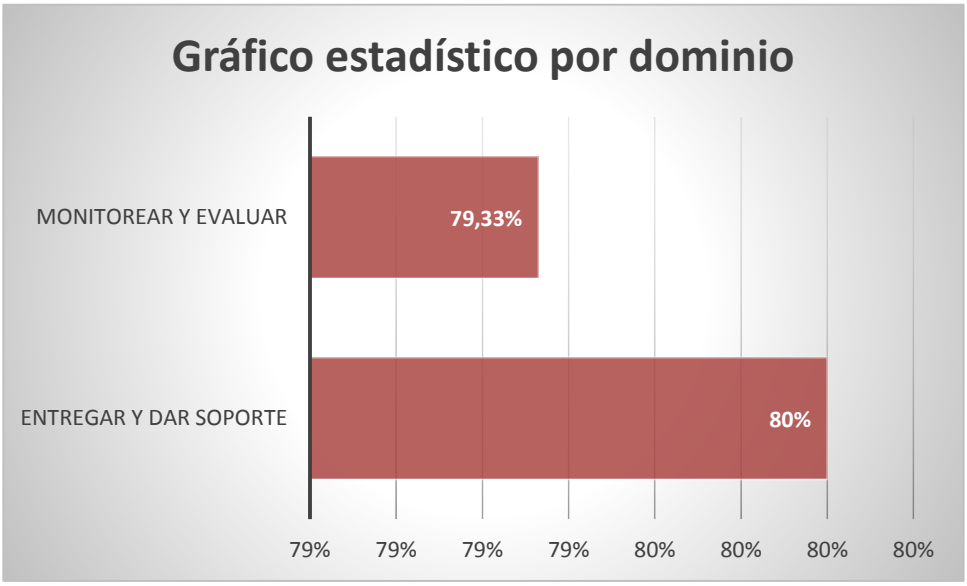
El promedio de los procesos no cumplidos están relacionados en un 4,17%, es decir que aún falta completar el desarrollo de más políticas, procedimientos, documentación, y capacitación al personal involucrado para controlar los procesos, que permita reducir las brechas existentes con lo establecido por COBIT 4.1.

Porcentaje de evaluación por dominio COBIT4.1, obtenido de la matriz en la que se enfoca al tercer y cuarto dominio con sus respectivos procesos.

Evaluación por dominio		
Dominio (3 y 4)	**# Procesos**	**%**
Entregar y dar soporte	13	80%
Monitorear y evaluar	4	79,33%

Fuente: Matriz tercer y cuarto dominio COBIT 4.1

Gráfico 16: Evaluación por dominio



Realizado por: Daniel Ortiz

11.4 Monitoreo

Reporte general de grados de madurez enfocados al tercer y cuarto dominio. (Ver Anexo 9)

Dominio	Procesos	Nivel de madurez
Entregar y dar Soporte	Definir niveles de servicio	1
	Administrar servicios de tercero	3
	Administrar desempeño y capacidad	1
	Asegurar continuidad de servicio	1
	Garantizar la seguridad de sistemas	1
	Identificar y asignar costos	1
	Educar y capacitar a usuarios	1
	Apoyar y orientar a clientes	1
	Administrar la configuración	1
	Administrar problemas e incidentes	1
	Administrar la información	1
	Administrar las instalaciones	1
	Administrar la operación	1
	Definir niveles de servicio	1
	Administrar servicios de tercero	1
Monitorear y Evaluar	Monitorear el proceso	0
	Evaluar lo adecuado del control interno	0
	Obtener aseguramiento independiente	1
	Proporcionar Auditoria Independiente	0

Fuente: Determinación de grados de madurez

Resumen de Análisis por Dominios:

- **Dominio: Planificación y Organización (PO)**

La información que manejan no se la realiza de una manera correcta ya que se cumple con los procesos que se realizan pero no existe constancia de lo que se realiza, se debe manejar de forma organizada documentando cada proceso que se realiza.

- **Dominio: Adquisición e Implementación (A)**

Existe el Hardware y Software necesario para realizar los procesos en los que se enfoca el Departamento de Sistemas, pero se debe tomar en consideración Software para el manejo y administración de la información de cada proceso que se realiza, prácticamente seria como administrarlo en la nube a diferencia que sin tener ningún costo por almacenamiento más bien si se adquiere el software únicamente el costo sería por licencia o si se crea por parte del área de Desarrollo y proyectos prácticamente no se invertiría y seria un ahorro económico en licencia y almacenamiento, permitiendo organizar la información confidencial de la empresa.

- **Dominio: Entrega y Dar Soporte (DS)**

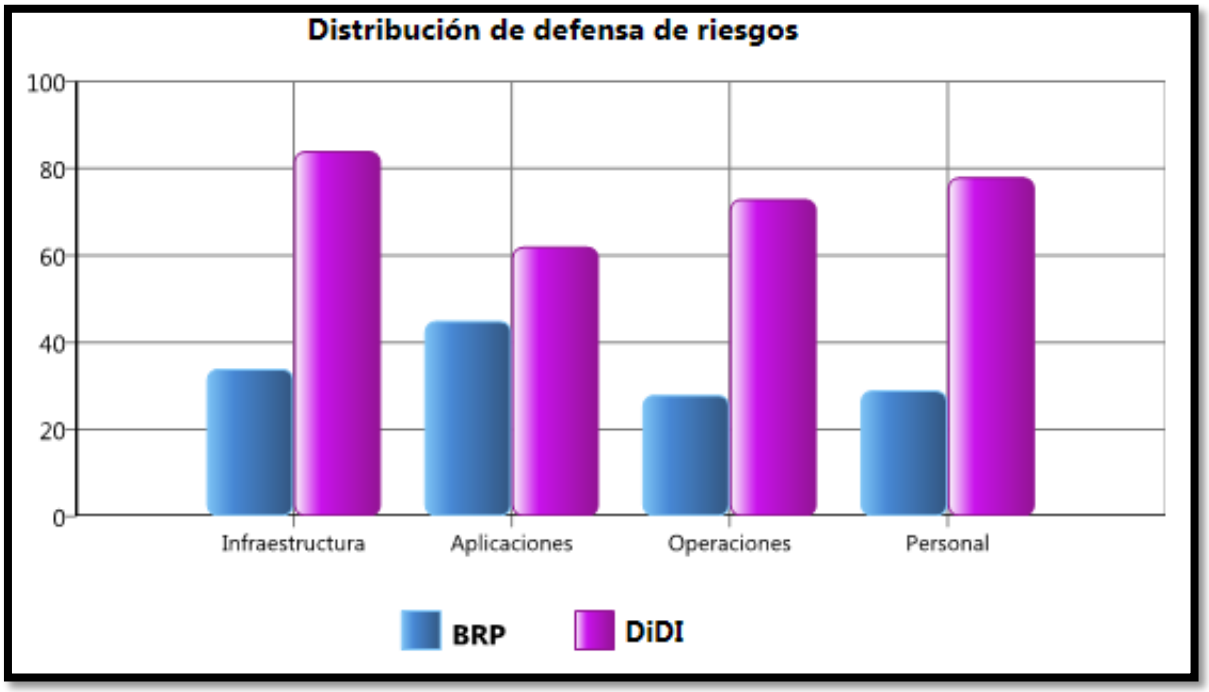
Los servicios de TI son medianamente entregados de acuerdo a las prioridades del negocio.
Los costos de TI no se encuentran totalmente optimizados.
Puesto que no existe un plan de continuidad no es implementada la disponibilidad de forma completa de los sistemas de TI, de igual forma la integridad y la confidencialidad no se encuentran implementadas de forma óptima.

- **Dominio: Monitorear y Evaluar (ME)**

La gerencia no monitorea ni evalúa el control interno en “DATA CENTER”.
Existe una poca vinculación en el desempeño de TI con las metas del negocio, no existe una medición óptima de riesgos y el reporte de estos, así como el cumplimiento, desempeño y control.

Aplicación MSAT (Herramienta de Evaluación de Seguridad de Microsoft).

Gráfico 17: Gráfico herramienta MSAT



Fuente: Aplicación MSAT

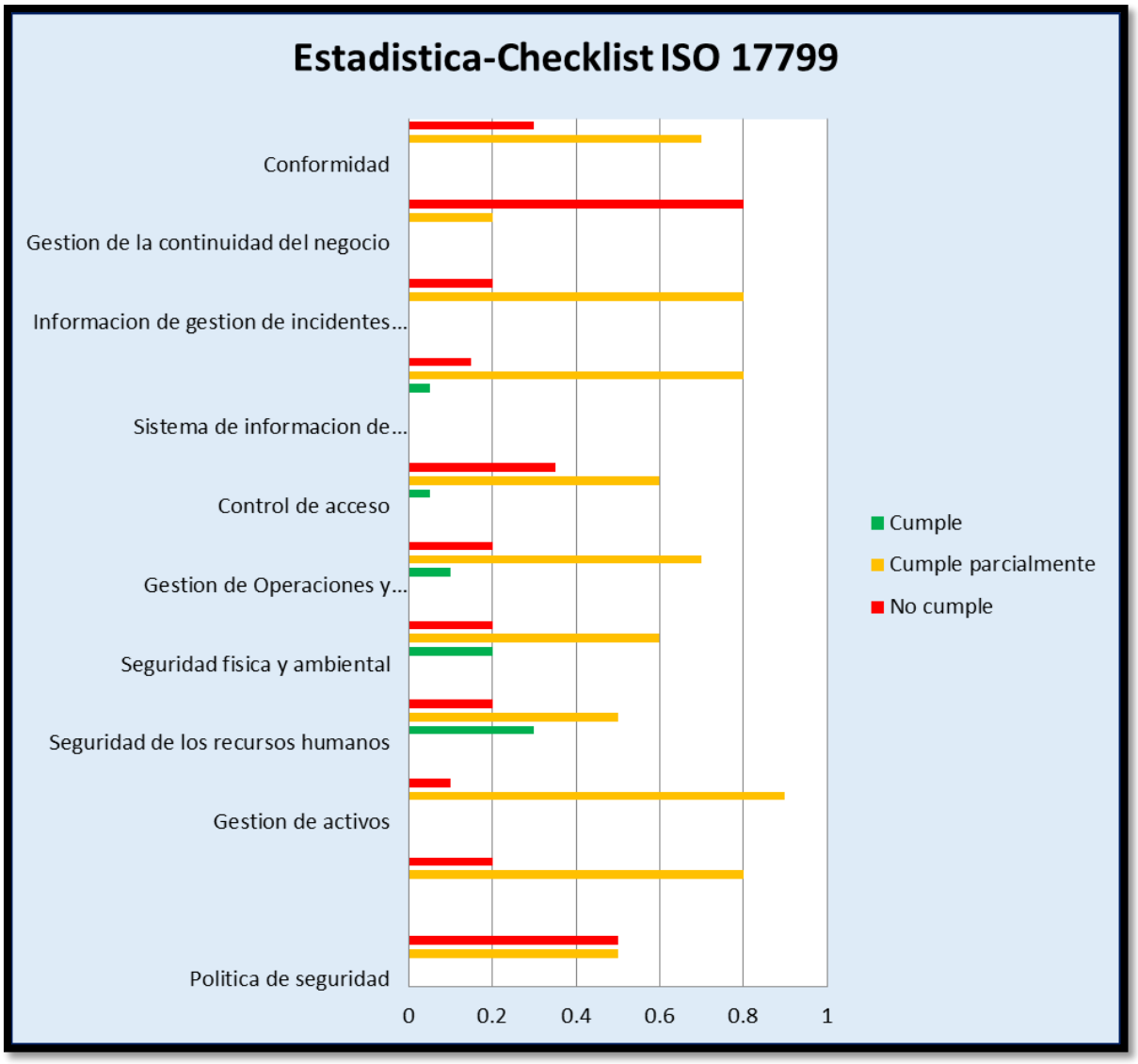
BRP es una medición del riesgo relacionado al modelo empresarial y al sector de la empresa. **DiDI** es una medición de las defensas de seguridad utilizadas en el personal, los procesos y la tecnología para ayudar a reducir los riesgos identificados en una empresa.

Análisis

La Aplicación MSAT (Herramienta de Evaluación de Seguridad de Microsoft) es una herramienta que permite evaluar los riesgos y las defensas de un lugar, área, departamento específico, en este caso se evaluó con datos reales el Departamento de Sistemas enfocándose en preguntas vinculadas al área de Infraestructura ya que es en dicha área en la cual se maneja los protocolos de seguridad de red, analizando después de lo evaluado que el Departamento de Sistemas se encuentra protegido y debidamente seguro frente a cualquier inconveniente ya que el índice de riesgo es muy bajo por lo tanto quiere decir que los procesos que se realizan son debidamente protegidos ya sea por antivirus, contraseñas o políticas de seguridad virtual mas no documental, es un breve análisis de cómo se encuentra la empresa actualmente.

Gráfico estadístico obtenido de Checklist ISO 17799 aplicado al Departamento de Sistemas.

Gráfico 18: Gráfico estadístico-Checklist ISO 17799



Fuente: www.SANS.com

Análisis

El grafico representa las etapas del Checklist ISO 17799 utilizado, determinado que en cada etapa existen diferentes actividades el cual se evaluó si existe un nivel de cumplimiento, no cumplimiento o cumple parcialmente, determinando si no cumple ninguna etapa, existe inconvenientes en la empresa, por lo que se considera aspectos fundamentales relacionados al manejo de la información, como también si cumple parcialmente quiere decir que los procesos se los realiza pero no existe evidencias de lo que se hace, esto quiere decir que no existe documentación detallada de cada actividad realizada.

12. IMPACTOS (TÉCNICOS, SOCIALES, AMBIENTALES O ECONÓMICOS):

El impacto del proyecto realizado en la empresa GRUPO KFC el cual corresponde "AUDITORÍA INFORMÁTICA APLICANDO LA METODOLOGÍA COBIT 4.1 EN EL DEPARTAMENTO DE SISTEMAS PERTENECIENTE AL GRUPO KFC" es de aspecto económico debido que ahorró a la empresa una cantidad de dinero reduciendo la inversión en la posible adquisición de software de terceras personas para que pueda automáticamente realizar la auditoria, receptando los procesos que se realizan en cada área, realizando inventarios tanto de hardware como de software o como también se ahorró en la posible contratación de un auditor externo para realizar la auditoria informática, debido que la misma se la realizo sin ningún costo o gasto para la empresa.

En el aspecto Técnico la auditoria informática toma como referencia únicamente el software en el que se trabaja, mas no precisamente el hardware, porque la auditoria es realizada y enfocada en la documentación sin la utilización de ningún software que facilite el proceso de la auditoria. Mientras que en el aspecto social la auditoría realizada se puede aplicar en empresas grandes ya que COBIT 4.1 está orientada a realizar auditorías de manera compleja a nivel mundial.

13. PRESUPUESTO PARA LA PROPUESTA DEL PROYECTO:

13.1. Gastos Directos

Detalle	Cantidad	V. Unitario	Valor Total
Hojas de Papel Bon	2 Resma	5.00	10.00
Tinta	2 Cartuchos	5.00	10.00
Memoria USB	1	8.00	8.00
Carpetas	6	0.40	2.40
Anillados del Anteproyecto	1	2.00	2.00
Empastado del Proyecto	1	8.00	8.00
Esferos	10	0.50	5.00
Copias	200	0.02	4.00
Internet	8 meses	22.00	176.00
		Total	**125.40**

Fuente: Presupuesto proyecto

13.2. Gastos Indirectos

Detalle	Cantidad	V. Unitario	Valor Total
Alimentación	130 almuerzos	1.75	227.50
Transporte	15 viajes	2.00	30.00
Comunicación celular	20 recargas	1.00	20.00
		Total	**227.50**

Fuente: Reporte de gastos

Gastos Directos + Gastos Indirectos= 125.40 + 227.50 = 352.50

10% DE IMPREVISTOS = 431.90 X 10% = 43.19

Valor Total = 352.50 + 43.19= 395.69

14. CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- La auditoría informática realizada en el Departamento de Sistemas aplicando la metodología COBIT 4.1 permitió analizar los resultados obtenidos mediante los procesos de los cuatro dominios aplicados, al igual que se pudo determinar en qué grado de madurez se encuentra la empresa, precisamente en el 3nivel el cual se encuentra en un nivel de creación del Gobierno IT para precautelar la información confidencial en los procesos con los que se trabaja, tomando en consideración los aspectos que evalúa la metodología para poder tener un manejo de la información eficaz y eficiente, determinando que los procesos se cumplen de manera correcta en cada área de acuerdo a los objetivos planteados, pero se bebe llevar la documentación debidamente organizada de los procesos que se realizan.
- La planificación que se consideró para llevar a cabo la auditoria estuvo enfocada a los procesos en los que se maneja la metodología tomando en consideración las técnicas e instrumentos para realizar las entrevistas y encuestas, para la recopilación de información, concluyendo después de obtener la información necesaria que el departamento de Sistemas cumple con los procesos tecnológicos para administrar la

información de forma correcta pero con el déficit de no documentar el proceso de las actividades realizadas.

- Después de haber determinado los KPI'S correspondientes a cada área, se pudo analizar las principales funciones que cumplen cada área generando u obteniendo resultados tales como, la satisfacción del cliente-usuario, en base al porcentaje de cumplimiento de cada función principal, de tal manera que se cumpla a cabalidad los objetivos del Departamento de Sistemas (IT).
- La auditoría realizada presenta las debilidades en los aspectos definidos por la matriz de análisis de acuerdo a los dominios de la Metodología COBIT 4.1 y por la aplicación MSAT el cual se puede determinar que los procesos que cumple cada área del Departamento IT son efectuados de acuerdo a los objetivos que se plantee pero no de manera correcta, debido a que no existe evidencias de lo que se realiza, no existe una correcta documentación de los procesos efectuados, es muy importante, porque con ello se puede respaldar el proceso de la información de acuerdo a lo que determina la metodología.
- El checklist de las normas ISO utilizado permitió determinar si cumple o no cumple los procesos que se enfocan en etapas principales que el documento evalúa, basándose en si cumple con los procesos de forma completa, esto quiere decir si se manejan los procesos documentado de lo que se realiza caso contrario no cumple el proceso, determinando el déficit importante que existe en la actualidad en el Departamento de sistemas el cual es que no se documenta ni existe evidencia de lo que se realiza en cada área del departamento.
- Mediante la investigación recopilada se pudo crear las políticas de seguridad de la información para el Departamento de Sistemas al igual que para cada área, mediante el análisis de la organización mundial SANS que establecen políticas a las empresas importantes, así como también se pudo establecer estrategias para realizar un control de cómo se efectúan los procesos después de haber obtenido los resultados de la auditoría.

Recomendaciones

- Se recomienda una capacitación continua del personal para que se sigan adoptando nuevas prácticas y que se proponga un programa de trabajo para que en un tiempo determinado se logre alcanzar el nivel 5 de madurez.

- Tomar en cuenta los procesos que se encuentran con el nivel de madurez de 0 y 1, que son los de factor crítico, como también se debe realizar evaluaciones periódicas con el fin de medir el avance de cada uno de los procesos estudiados en este trabajo.
- Se debe tomar en consideración que los procesos que se realizan en cada área deben ser documentados, debido a que es una evidencia el cual ayuda a los coordinadores administrar de manera correcta las actividades en beneficio de los usuarios o personal del Departamento de Sistemas.
- Para la utilización de la herramienta MSAT se recomienda aplicar la evaluación con datos reales de un área grande de sistemas, como la que se realizó del Departamento de Sistemas de Grupo KFC, porque con datos de un área pequeña no son factibles los resultados.
- Para determinar los KPI en el Departamento de Sistemas se debe tomar en consideración el nivel de cumplimiento y las principales actividades que se realiza en cada área, para poder establecer y aplicar la estructura critica del semáforo que califica el nivel de cumplimiento existente.

15. BIBLIOGRAFÍA

15.1. Bibliografía Básica

Diccionario de Lengua Española: Terminología, 2005.

15.2. Bibliografía Citada

- Buades. B. (1985). Auditoría Informática. Sevilla-España. Editorial (P.U.F. 4)
- Mario L. (2010). COBIT. Catedra. Edición (La sevillana Pg. 124)
- Ruther R. (2012) COBIT 4.1. Madrid. Volumen-Isaca (Vol-3 Pg. 240)
- BARRIOS, Alfredo. (2013) Metodología de la investigación 3. Ecuador Rijabal S.A, 3ed. (132 p).

15.3. Bibliografía Virtual

- Monografías (01 de Abril de 2015). Auditoría Informática, Audino. Disponible http://www.monografias.com/trabajos12/audin/audin.shtml.

- Eduardo L. (02 de Enero de 2000). Auditoría Informática, Audocomp. Disponible http:/www.eduardoleyton.com/Audcomp R. html
- Monografías (10 Marzo de 2008). Objetivos Auditoría Informática, Aiditoinfo. Disponible http://.monografías.com/trabajos/aiditoinfo.shtml.
- Rocío L. (01 Septiembre de 2005). Auditoría Informática, Edit. Disponible http://www.rociolopez.8m.com/
- Rocío L. (01 Septiembre de 2005). Características Auditoría Informática, Edit. Disponible http://www.rociolopez.8m.com/
- Galeón R. (14 Agosto de 2015). COBIT misión, abcd. Disponible http://aabbccddee.galeon.com/Método.htm.

ANEXOS