ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

"EVALUACIÓN TÉCNICA INFORMÁTICA DEL SISTEMA DE INFORMACIÓN DE LA EMPRESA COSSFA, UTILIZANDO EL ESTÁNDAR INTERNACIONAL COBIT"

Previa a la obtención del título de:

INGENIERO EN SISTEMAS E INFORMÁTICA

POR:

EVELINE ALINA ESTRELLA ZAMBRANO

SARA NATALI ALVEAR MONTESDEOCA

SANGOLQUÍ, Enero del 2013

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por las Srtas. SARA NATALI ALVEAR MONTESDEOCA y EVELINE ALINA ESTRELLA ZAMBRANO como requerimiento parcial a la obtención del título de INGENIERAS EN SISTEMAS E INFORMÁTICA.

Sangolquí, 24 de Enero del 2013.

_____

Ing. Silvia Arévalo

Profesor Director

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por las Srtas. SARA NATALI ALVEAR MONTESDEOCA y EVELINE ALINA ESTRELLA ZAMBRANO como requerimiento parcial a la obtención del título de INGENIERAS EN SISTEMAS E INFORMÁTICA.

Sangolquí, 24 de Enero del 2013.

_____

Eco. Gabriel Chiriboga

Profesor Codirector

AUTORIZACIÓN

Nosotras, Sara Natali Alvear Montesdeoca y Eveline Alina Estrella

Autorizamos a la ESCUELA POLITÉCNICA DEL EJÉRCITO la publicación, en la Biblioteca Virtual de la Institución, del trabajo "EVALUACIÓN TÉCNICA INFORMÁTICA DEL SISTEMA DE INFORMACIÓN DE LA EMPRESA COSSFA, UTILIZANDO EL ESTÁNDAR INTERNACIONAL COBIT", cuyo contenido, ideas y criterios es de mi exclusiva responsabilidad y autoría.

Sangolquí, 24 de Enero del 2013.

_____ _____

Sara Natali Alvear Montesdeoca. Eveline Alina Estrella Zambrano.

ÍNDICE DE CONTENIDO

LISTADO DE TABLAS

LISTADO DE FIGURAS

LISTADO DE ANEXOS

Los anexos se adjuntan al proyecto en medio magnético. Listados como se detalla a continuación:

Entrevista	Planear y Organizar	ENT-PO1
		ENT-PO2
		ENT-PO3
		ENT-PO4
		ENT-PO5
		ENT-PO6
		ENT-PO7
		ENT-PO8
		ENT-PO9
		ENT-PO10
		ENT-PO11

Entrevista	Adquirir e Implementar	ENT-AI1
		ENT-AI2
		ENT-AI3
		ENT-AI4
		ENT-AI5
		ENT-AI6
		ENT-AI7
		ENT-AI9
		ENT-AI10
	Entrega y dar Soporte	ENT-DS4
		ENT-DS5
		ENT-DS6
		ENT-DS7
		ENT-DS9
		ENT-DS10
		ENT-DS11
		ENT-DS12
	Monitorear y Evaluar	ENT-ME1
		ENT-ME2
		ENT-ME3

Observación	Adquirir e Implementar	OBS-AI8
	Entrega y Dar Soporte	OBS-DS8
	Entrega y Dar Soporte	OBS-DS13

Documentación	Entrega y dar Soporte	DOC-DS1
		DOC-DS2
		DOC-DS3

NOMENCLATURA UTILIZADA

AICPA:	American Institute of Certified Public Accountants / Instituto Norteamericano de Contadores Públicos.
CICA:	Instituto Canadiense de Contadores Certificados.
COSO:	Committee of Sponsoring Organizations
CPA:	Certified Public Accountant
CRM:	Customer relationship management
DHCP:	Dynamic Host Configuration Protocol / Configuración Dinámica de Host
DNS:	Domain Name System / Sistema de Nombres de Dominio
DTI:	Dirección de Tecnologías de la Información.
EDIFACT:	Electronic Data Interchange for Administration, Commerce and Transport / Intercambio Electrónico de Datos para la Administración, Comercio y Transporte
ERP:	Enterprise Resource Planning / Planificación de Recursos Empresariales
ESF:	Foro Europeo de Seguridad
GAO:	Government Accountability Office
IFAC:	International Federation of Automatic Control
IIA:	Institute of Internal Auditors
ISACA:	Information Systems Audit and Control Association
ISACF:	Information Systems Audit and Control Foundation / Fundación para la Auditoría y Control de los Sistemas de Información
ISO/IEC:	International Organization for Standardization/International Engineering Consortium
IP:	Internet Protocol / Protocolo de Internet
ITGI:	TI Governance Institute/ Instituto para la administración global de Tecnologías de la información
ITIL:	Information Technology Infrastructure Library/ Biblioteca de Infraestructura de Tecnologías de Información

ITRB:	Managing Systems Information: A Practical Assessment Tool.- Tabla de Recursos para la tecnología de la Información
ITSEC:	Information Technology Security Evaluation Criteria
LAN:	Local Area Network / Red De Área Local
MAN:	Metropolitan Area Network / Red De Área Metropolitana
NIST:	National Institute of Standards and Technology
OECD:	Organization for Economic Co-operation and Development
PCIE:	Peripheral Component Interconnect Express
QMS:	Quality Management System.
SAC:	Systems Auditability and Control.
SAS:	Consideraciones de la estructura de Controles Internos en los Informes de los Estados Financieros
SCM:	Supply Chain Management / Administración De Redes De Suministro
SEI:	Software Development Capability Maturity Model: Instituto de Ingeniería de Software.
SI:	Sistema de Información.
SPICE:	Simulation Program with Integrated Circuits Emphasis / Programa de simulación con énfasis en circuitos integrados.
TI:	Tecnologías de la Información.
TCSEC:	Trusted Computer System Evaluation Criteria.
TIC:	Tecnologías de la Información y la Comunicación
WAN:	Wide Area Network/ Red De Área Amplia.

RESUMEN

El proyecto realizado busca evaluar el correcto desempeño, y aplicar las buenas prácticas que deben establecerse en la gestión de TI, para esto se realizó una Auditoría Informática utilizando el marco de referencia COBIT, el mismo que permitió evaluar como se está desarrollando la administración de la tecnología en la Gerencia de TI del Comisariato de Servicio Social de las Fuerzas Armadas – COSSFA.

Se determinaron los procesos críticos que maneja el comisariato, lo que permitió determinar los riesgos que vulneran la Gerencia de TI, lo que conllevó a la elaboración de una investigación de campo para evidenciar las debilidades de la Gerencia de TI.

A través del Marco de Referencia COBIT y los instrumentos utilizados para evaluar las diferentes áreas que componen la Gerencia de TI. Se emitieron recomendaciones basadas en el criterio de las mejores prácticas de TI que propone COBIT.

Se presentaron informes con el detalle de los hallazgos críticos que afectan la gestión de la gerencia de TI, y un resumen ejecutivo con los principales hallazgos de la evaluación realizada. Esta evaluación les va a permitir mejorar la administración de las tecnologías que gestiona la gerencia de TI del comisariato.

CAPÍTULO 1

1. DESCRIPCIÓN DEL PROYECTO

1.1 Antecedentes

COSSFA S.A. desde el año 2009 se integró al grupo empresarial HOLDINGDINE S.A. la cual contribuyó a la gestión empresarial; por ello las normas y estándares informáticos deben estar sometidos e implantados mediante la aprobación de la Gerencia de Sistemas que se encargará de la implementación de controles a la información que se maneja en los diversos procesos.

Lo que trajo retos exclusivos para la empresa, con el apoyo de la tecnología, las tareas de los responsables de informática y los auditores informáticos facilita para enfrentar los desafíos. Entre los retos que tuvieron que enfrentar fueuna auditoría informática, la que permitirá evaluar y verificar políticas, controles, procedimientos y seguridad de los recursos dedicados al manejo de la información.

1.2 Justificación

Es de interés institucional, el considerar este tipo de prácticas, normas, controles de seguridad a los sistemas de información, con la finalidad de que se registre la información correctamente entorno a las operaciones que involucran sus procesos facilitando así la toma de decisiones sobre situaciones observables identificadas en evaluaciones informáticas.

1.2.1 Descripción del Problema

Se puede observar que se requiere de controles a los que hay que someter el sistema de información que maneja el Comisariato de Servicio Social de las Fuerzas Armadas, en sus 3 categorías, Controles de Entrada, Controles de Procesos y Controles de Salida.

1.2.2 Solución Propuesta

Con el objetivo de dar una solución oportuna, se ha identificado la realidad de aplicar una Auditoría Informática, la misma que cumplirá con el trabajo de detectar debilidades en el sistema de información de la entidad auditada para conocer las causas de origen de la problemática que se presenta para a futuro contrarrestarles con las recomendaciones necesarias para mejorar o eliminar las debilidades.

1.3 Alcance

El proyecto pretende entregar un informe final que contenga observaciones y recomendaciones para el funcionamiento y desarrollo del Sistema de Información del COSSFA (Matriz).

Los procesos de TI serán revisados considerando el nivel de detalle provisto por COBIT, enfocados en los criterios de: efectividad, eficiencia, disponibilidad, confiabilidad, cumplimiento, confidencialidad, e integridad. Así mismo políticas, procesos, procedimientos y prácticas de trabajo serán evaluados a diferentes niveles de organización, abarcando desde la Gerencia de TI, hasta el nivel operacional, y

complementando con trabajo más detallado a nivel de las diferentes plataformas operativas.

1.4 Objetivo General

Realizar una Auditoría Informática al Sistema de Información del COSSFA, mediante la metodología que plantea la herramienta COBIT del ambiente de control implementado en los procesos automatizados y en el gerenciamiento de los mismos, utilizando la metodología COBIT, a fin de identificar debilidades y emitir recomendaciones que permitan eliminar o minimizar los riesgos.

1.5 Objetivos Específicos

- Elaborar el Plan de Investigación de Campo.
- Recopilar información detallada de la situación actual del sistema de información.
- Realizar el análisis de la información.
- Verificar las observaciones.
- Elaborar el informe borrador.
- Validar el informe borrador.
- Elaborar y entrega del informe final.

1.6 Condiciones de Ejecución

1.6.1 Metodología

COBIT es un marco de referencia de procesos y objetivos de control de TI que pueden ser implementados para controlar, auditar y administrar la organización tecnológica. Este marco de referencia está basado en las mejores prácticas y sistemas de información de auditoría y control.

Ofrece un conjunto de herramientas para administrar los procesos de TI, unificando los dos puntos de vista, el de la administración y el del auditor. Las Guías de Administración de TI consideran los controles de TI desde una perspectiva de la administración, mientras que las Guías de Auditoría proveen asistencia específica a los auditores internos en el diseño de programas adecuados de auditoría para cada dominio. COBIT también provee herramientas detalladas y personalizables de autoevaluación en forma de matrices y plantillas para asistir en la evaluación y medición de la organización comparada con los criterios de COBIT.

CAPÍTULO 2

2. MARCO TEÓRICO

2.1 Necesidad de Información y Conocimiento en las Empresas

Las empresas durante los últimos años han multiplicado esfuerzos para obtener información veraz, la cual le permita una mejor toma de decisiones, tanto para atacar nuevos mercados, como para proteger a la empresa de agentes externos que puedan vulnerar su estabilidad, motivo por el cual se caracteriza a la información como uno de los activos de la empresa, un recurso que se encuentra al mismo nivel que los recursos financieros, materiales y humanos, que hasta el momento habían constituido los ejes sobre los que había girado la gestión empresarial. Si la Teoría económica tradicional mantenía el capital, la tierra y el trabajo como elementos primarios de estudio, la información se ha convertido, ahora, en el cuarto recurso a gestionar.

El conocimiento del entorno, en un mundo cada vez más complejo y cambiante, origina la necesidad de evaluar los sistemas tecnológicos, que es donde se genera la información que permite el correcto desarrollo de la empresa.

2.2 Influencia de la tecnología en las Empresas

A medida que la evolución de las tecnologías de la información ha ido revolucionando al mundo, también se han vuelto parte imprescindible de las organizaciones, y es tal la penetración dentro de todos los niveles de una empresa, que la han vuelto parte vital de su funcionamiento.

La incorporación de la tecnología dentro del entorno empresarial, educativo, salud, administración pública, etc., ya no es una opción, sino una necesidad derivada de su evolución en un mercado cada vez más avanzado tecnológicamente.

La tecnología ha mejorado los niveles de producción, administración y comercialización de productos y/o servicios ofertados, en base a ciertos criterios:

- Flujos ágiles de información.- la aparición y evolución de las redes de computadores, han dado origen al concepto de redes corporativas dentro de las organizaciones, las cuáles se han convertido en el canal vital de comunicación dentro de las mismas, permitiendo la obtención de información rápida y en tiempo real.
- Reducción de la estructura jerárquica.- el flujo ágil de la información ha generado la reducción de niveles jerárquicos innecesarios, eliminando mucha de la burocracia que dificultaba los procesos del negocio. Actualmente los sistemas de información se han convertido en entes de entrega, control y coordinación de muchas actividades del negocio.
- Relaciones empresariales.- con el advenimiento del Internet y la posterior globalización, las tecnologías de información y comunicaciones, no solo se han convertido en herramientas de ayuda dentro del ámbito del negocio, sino también en herramientas de comunicación inter empresarial, eliminando la brecha física de posición geográfica entre proveedor y cliente.
- Costos.- todos los factores analizados han ido en pro del ahorro de costos, ya que han mejorado los métodos de trabajo tradicionales, y la forma en

que se establecen los contactos y se cierran los negocios, ya que actualmente, es posible obviar los encuentros cara a cara, para la formalización de contratos.

Solo con analizar los cuatro factores mencionados, es indudable el alto impacto que la tecnología puede llegar a tener en las organizaciones, permitiendo convertirlas en entes ágiles y dinámicos dentro del negocio, lo que les brinda una ventaja competitiva con respecto a sus rivales.

Pero con esto no quiere decir que por el simple hecho de emplear TIC en las empresas, los factores analizados se convertirán en realidad, ya que todo dependerá del como se implementen y apliquen, ya que un correcto uso brindará una ventaja, pero de la misma manera, un uso incorrecto, terminará en desventajas difíciles de remediar.

2.3 Importancia de las mejores Prácticas de TI aplicada en empresas

"Las mejores prácticas y los estándares ayudan a posibilitar un gobierno eficaz de las actividades de TI incrementalmente, el uso de estándares y mejores prácticas tales como ITIL, COBIT e ISO/IEC 27002, está siendo conducido por requerimientos de negocio para mejoras de desempeño, transparencia y control sobre actividades de TI."[1]

El creciente uso de estándares y mejores prácticas ha generado nuevos desafíos y demandas, a profesionales, gerentes y asesores de TI, quienes pueden adoptarlos y

[1] Tomado de AlineandoCOBIT4.1,ITIL3ISO27002enbeneficiodelaempresa

utilizarlos con la mejor intención; sin embargo, no tienen un enfoque de negocio o no cuentan con la participación y la ayuda del cliente.

Para obtener el máximo valor de las mejores prácticas para el negocio, se necesita involucrar a los clientes de los servicios de TI, dado que el uso eficaz de TI debería ser una experiencia colaborativa entre el cliente y los proveedores del servicio tanto internos como externos.

El siguiente cuadro resume quien tiene interés en la forma en que los estándares y las mejores prácticas de TI pueden ayudar a considerar los aspectos de gestión de TI.

Figura 1: Grupos de interés en aspectos de gestión de TI

Aspectos de alta gestión basados en COBIT	¿Quién tiene interés primario?			
	Alta Dirección	Gerencias funcionales	Gerencia de TI	Auditoria / Cumplimiento
Planificar y Organizar				
¿TI está alineada con las estrategias del negocio?	√	√	√	
¿La empresa está logrando el uso óptimo de los recursos internos y externos?	√	√	√	√
¿Todo el personal de la empresa entiende los objetivos de TI?	√	√	√	√
¿Se ha entendido el impacto de TI en los riesgos de la empresa? ¿Se ha establecido la responsabilidad de la gestión de los riesgos de TI?	√			
¿Se han entendido y se están gestionando los riesgos de TI?		√	√	√
¿La calidad de los sistemas es apropiada para las necesidades de la empresa?		√	√	
Adquirir e Implementar				
¿Es probable que los nuevos proyectos entreguen soluciones que satisfagan las necesidades del negocio?		√	√	
¿Es probable que los nuevos proyectos se entreguen a tiempo y dentro del presupuesto?		√	√	√
¿Los nuevos sistemas trabajarán correctamente cuando se implementen?		√	√	√
¿Los cambios serán realizados sin trastornar la actual operación del negocio?		√	√	
Entrega y Soporte				
¿Los servicios de TI se entregan en línea con los requerimientos y las prioridades del negocio?		√	√	
¿Están optimizados los costos de TI?		√	√	√
¿El personal está capacitado para utilizar los sistemas de TI en forma productiva y segura?		√	√	
¿Los sistemas de TI tienen adecuada confidencialidad, integridad y disponibilidad?		√	√	√
Monitorear y Evaluar				
¿Se puede medir el desempeño de TI y detectar los problemas antes que sea demasiado tarde?	√	√	√	
¿Los controles internos están operando eficazmente?	√			√
¿La empresa está cumpliendo las disposiciones regulatorias?	√	√	√	√
¿El gobierno de TI es eficaz?	√	√	√	√

Figura 2.1: Grupos de interés en aspectos de gestión de TI[2]

[2] Alineando COBIT4.1,ITIL3 ISO 27002 en beneficio de la empresa

El uso efectivo de TI es crítico para el éxito de la estrategia de la empresa, como se ilustra en el siguiente comentario:

"El uso de TI tiene el potencial para ser el mayor impulsor de riqueza económica en el siglo XXI. Además de que TI ya es crítica para el éxito empresarial, proporciona oportunidades para obtener una ventaja competitiva y ofrece medios para incrementar la productividad, e incluso hará aún más en el futuro.

TI también implica riesgos. Es evidente que en estos días de negocios globales, la caída de los sistemas y las redes puede resultar muy costosa para cualquier empresa. En algunas industrias, TI es un recurso competitivo necesario para diferenciarse y obtener una ventaja competitiva, mientras que en otras, no sólo determina la prosperidad sino la supervivencia."[3]

2.4 Introducción a la Auditoría

La auditoría nace como un órgano de control de algunas instituciones estatales y privadas; es considerada como un "proceso sistemático de obtención y evaluación objetiva acerca de aseveraciones efectuadas por terceros referentes a hechos y eventos de naturaleza económica, para testimoniar el grado de correspondencia entre tales afirmaciones y un conjunto de criterios convencionales, comunicando los resultados obtenidos a los destinatarios y usuarios interesados".

La auditoría contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones. Aunque pueden aparecer sugerencias y planes de acción

[3] ITGI, "Board Briefing on IT Governance", 2nd Edition, USA, 2003

para eliminar las disfunciones y debilidades; queda a cargo de la empresa tomar las decisiones pertinentes.

Las funciones de análisis y revisión que el auditor informático realiza, puede chocar con la psicología del auditado, ya que es un informático y tiene la necesidad de realizar sus tareas con racionalidad y eficiencia. La reticencia del auditado es comprensible y, en ocasiones, fundada. El nivel técnico del auditor es a veces insuficiente, dada la gran complejidad de los Sistemas, unidos a los plazos demasiado breves de los que suelen disponer para realizar su tarea.

Además del chequeo de los Sistemas, el auditor somete al auditado a una serie de cuestionarios. Dichos cuestionarios, son guardados celosamente por las empresas auditoras, ya que son activos importantes de su actividad. Estos tienen que ser comprendidos por el auditor al pie de la letra, ya que si son mal aplicadas, se pueden llegar a obtener resultados distintos a los esperados. Se puede llegar a explicar cómo ocurren los hechos pero no por qué ocurren. El cuestionario debe estar subordinado a la regla, a la norma, al método. Sólo una metodología precisa puede desentrañar las causas por las cuales se realizan actividades teóricamente inadecuadas o se omiten otras correctas.

El auditor sólo puede emitir un juicio global o parcial basado en hechos y situaciones incontrovertibles, careciendo de poder para modificar la situación analizada por él mismo.

2.4.1 Tipos de Auditoría

2.4.1.1 Auditoría de Procesos

La auditoría de procesos se basa en acreditar la eficacia del sistema de calidad de servicios orientados al planeamiento estratégico en un proceso en particular, el cual asegurará la calidad de un producto o servicio.

Las características de un proceso son las siguientes:

- Qué debe hacerse.
- Quién debe llevarlo a cabo.
- Dónde y cómo debe ser hecho.
- Qué materiales, equipamientos y documentos son necesarios.
- Cómo debe ser dirigido y registrado.

La rigurosidad con que deben ser analizadas y cumplidas las características del proceso depende de la complejidad del proceso.

Contar con un proceso estandarizado y documentado sobre la forma como debe efectuarse la supervisión de actividades de una función las cuales emitan resultadospara la mejora continua con el fin de determinar el cumplimiento de los indicadores establecidos dentro de una organización.

Después de analizar la información obtenida se presentan informes de auditoría, se verifica el cumplimiento de los requerimientos sobre el estado de los procesos, así como los errores encontrados.

A continuación se efectúa el análisis de los problemas detectados, así como sugerencias de mejoras, finalmente se hace el seguimiento de las acciones correctivas tomadas, para analizar su efectividad y eficiencia.

2.4.1.2 Auditoría de Producto / Servicio

La auditoría de Producto / Servicio es diseñada con el fin de obtener información sobre la realidad de la adecuación de las características de uno o de varios productos o servicios con las necesidades de los clientes, basadas en estándares y normas, se podría como una “supervisión del producto”.

Se debe identificar las marcas participantes dentro de cada mercado de los diferentes participantes.

Los resultados de este tipo de auditorias se presentan al responsable del sector auditado que extraerá personalmente las conclusiones oportunas, de acuerdo con la dirección y con el cliente.

El análisis de resultados y las conclusiones de la auditoría son documentos internos de la empresa y deben permanecer en el marco de relaciones cliente/suministrador.

2.4.1.3 Auditoría de Calidad

El Sistema de la Gestión de Calidad ayuda a las empresas a demostrar su responsabilidad al establecer y mejorar las políticas, objetivos, estándares y otros requerimientos de calidad. Las normas 9000:2000 y la 9001:2000 son la base del proceso de auditoría.

Es importante la información suficiente y apropiada sobre los hechos verificables sobre la gestión de la empresa que respalden y avalen a la auditoría.

Para dar inicio, las actividades a realizar es una reunión inicial, detección de evidencia y resultados de la auditoría y reunión final, posteriormente se incluirá un resumen de los resultados de la auditoría, de forma clara y sencilla.

2.4.1.4 Auditoría Operacional

La auditoría operacional es el análisis del flujo de transacciones llevadas a cabo en una o varias áreas funcionales, con el propósito de incrementar la eficiencia y la eficacia operativas a través de proponer recomendaciones que se consideren necesarias.

Existen 3 elementos fundamentales que se debe considerar:

- Debe encausarse hacia los aspectos administrativos de los métodos y procedimientos que integran un sistema.
- La auditoría debe tener un enfoque constructivo
- El auditor o sus colaboradores no deben intervenir en el diseño detallado de los cambios que requiere un sistema o sus procedimientos.

En este tipo de auditoría se involucran cambios inmediatos a nivel financiero, estas son llamadas transacciones, en una empresa existe un flujo abundante y contante de transacciones.

2.5 Estándares de Auditoría

En los últimos años se ha incrementado la atención sobre los controles internos, tanto para los auditores, los gerentes, los contadores, como para las entidades reguladoras en general. Como resultado de un continuo y trabajoso esfuerzo, se han desarrollado varios documentos para definir, valorizar, reportar y mejorar el control interno y ser utilizados como marco de referencia en las organizaciones. En resumen, éstos son:

- Informe COSO.- (Committee of Sponsoring Organizations), de la Comisión de Estudios de Controles Internos.
- SAC.- (Systems Auditability and Control), de la Fundación de Investigación del Instituto de Auditores Internos.
- SAS 55 y SAS 78.- Consideraciones de la estructura de Controles Internos en los Informes de los Estados Financieros, del Instituto Americano de Contadores Públicos (CPA)
- COBIT.- (Control Objectives for Information and related Technology), de la Fundación de Auditoría y Control de Sistemas de Información.

Cada uno de ellos ha sido definido para una audiencia en particular: el "COSO" fue diseñado para la Gerencia; el "SAC" para los auditores internos; los “SAS 55” y “SAS 78”, para los auditores externos, y finalmente el "COBIT" enfocado principalmente para los auditores de sistemas de información.

2.6 Control Interno

El Control Interno es un proceso efectuado por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Fiabilidad de la información financiera.
- Cumplimiento de las leyes y normas aplicables.

La anterior definición refleja ciertos conceptos fundamentales:

- El control interno es un proceso. Es un medio utilizado para la consecución de un fin, no es un fin en si mismo.
- El control interno lo llevan a cabo las personas. No se trata solamente de manuales de políticas e impresos, sino de personas en cada nivel de la organización.
- El control interno sólo puede aportar un grado de seguridad razonable, no la seguridad total.
- El control interno está pensado para facilitar la consecución de objetivos.

2.7 Auditoría de TI[4]

2.7.1 Antecedentes

Publicado por primera vez por la Fundación para la Auditoría y Control de Sistemas de Información, en 1996, COBIT se encuentra actualmente en su cuarta edición. La segunda edición, publicada en el año 1998 incrementa la base de recursos sobre las cuales los objetivos de control se basan e incorporaba un práctico conjunto de herramientas de implementación. A la edición actual se incluyeron guías de administración, tanto para el campo de la Auditoría informática como para la administración de sistemas de información.

Las actividades de investigación y publicación fueron soportadas significativamente por PriceWaterhouseCoopers, donaciones de capítulos y miembros de ISACA a nivel mundial, material de investigación del Foro Europeo de Seguridad (ESF) y soporte adicional de The Gartner Group.

COBIT es una compilación de las mejores prácticas globales, obtenidas de un amplio espectro de fuentes, como:

- Estándares Técnicos de ISO, EDIFACT, etc.
- Códigos de Conducta emitidos por el Consejo de Europa, OECD, ISACA, etc.
- Criterios de evaluación de calidad de Sistemas TI y procesos: ITSEC, TCSEC, ISO 9000, SPICE, TickIT, Common Criteria, etc.

[4]TI.- Information Technology -por sus siglas en inglés- De esta manera se denomina a la infraestructura tecnológica que soporta las actividades del negocio. Así también se conoce al área que administra estos recursos.

- Estándares profesionales para control interno y auditoría: COSO, IFAC, AICPA, CICA, ISACA, IIA, PCIE, GAO, etc.
- Prácticas de la industria y requerimientos de foros industriales: (IBAG, NIST, DTI), etc.
- Requerimientos específicos de industrias incluyendo bancos, comercio electrónico y manufactura.

2.7.2 Auditoría Informática

La Auditoría Informática, mediante la evaluación y control, tiene como principal objetivo mejorar la rentabilidad, seguridad y eficiencia del sistema de información. Logrando analizar procesos de gestión, con posibles correcciones, con el fin de garantizar la integridad, veracidad de la información y mantenimiento de los SI[5].

A su vez, evalúa todo, como es la parte informática, organización de centros de información, hardware y software. Se lo define como: “El conjunto de procedimientos y técnicas implementados para evaluar el ambiente informático de una empresa con el fin de proteger sus activos y recursos.”

2.7.3 Auditoría basada en riesgos

Dentro de un constante evolucionar, las empresas determinan sus metas por el cual argumentan su existencia. Es por ello que se plantea objetivos y metas condicionadas por la existencia del riesgo, desarrollando así mejoras de manera continua el proceso de auditoría.

[5] SI: Sistemas de Información

Dentro de este contexto se entendería el concepto de riesgo:

i. En la teoría de la gestión y la estrategia de los negocios, riesgo es uno de los componentes del continuo proceso de oportunidades, que lleva a resultados favorables y desfavorables y que está asociado con probabilidades —frecuencia— de materialización. El riesgo es la discontinuidad de este continuum. Es lo inesperado.[6]

ii. Riesgo es un concepto que se utiliza para expresar la incertidumbre de eventos y resultados que podrían ejercer un efecto adverso en los objetivos y las metas de la organización.[7]

Por lo que se determina que riesgo es la exposición a la posibilidad o probabilidad de enfrentar pérdidas o ganancias, como consecuencias de lograr una acción en particular.

Este tipo de auditoría no está basada solo en el riesgo sino también en los controles internos y operativos, así como también en sus conocimientos del negocio. La decisión de determinar el tipo de riesgo puede ayudar a relacionar el análisis de costo/beneficio del control para el riesgo conocido, permitiendo que se hagan elecciones prácticas. [8]

[62]http://documentos.cgr.go.cr/content/dav/jaguar/documentos/cenrel/XVI_congreso_AI/Doc_JMunozG.htm

[8] PDF - Auditoria Basada En Riesgos

2.7.4 Auditoría de Sistemas de Información

Hoy en día la Auditoría informática obtiene más importancia, ya que actualmente los datos y la información se han convertido en un bien intangible de cada organización, dando así una ventaja estratégica, por lo que no se escatiman costos ni esfuerzos en la creación de sistemas de información para conseguir un nivel óptimo de productividad y calidad.

Hoy en día, el cambio es una constante en toda empresa y/o organización, por ello deben tomar en cuenta dentro de sus estados financieros, industriales y sociales las tendencias tecnológicas y su entorno debe adaptarse de la mejor forma para que su comprensión sea particularmente se encuentre dentro de un contexto de los sistemas y tecnologías de la información.

Con mayor frecuencia, un mayor número de organizaciones considera la información y la tecnología como uno de los activos más importantes. Entonces, todos los activos de la empresa requieren de procesos de calidad, controles, seguridad e información, es por ello que se debe establecer sistemas de control interno acorde a las necesidades de la misma y tal sistema debe soportar debidamente los procesos del negocio.

Dentro de las tendencias, ISACA (InformationSystemsAudit and Control Association), publicó en 1995 a COBIT, siendo una metodología el marco de definición de estándares y conducta profesional para la gestión y el control de los SI. Adicionalmente, esta metodología aporta la orientación hacia el negocio y está

diseñada no solo para ser utilizada por usuarios y auditores, sino también como una extensa guía para gestionar los procesos de negocios.

2.7.4.1 Elementos de la Auditoría de Sistemas de Información

COBIT se materializa en una colección de referencias documentales, que tradicionalmente ha estado compuesta por los siguientes volúmenes:

- **Resumen ejecutivo.**

  Ofrece una sinopsis de los conceptos COBIT.

- **Marco de referencia.**

  Presenta la estructura COBIT de cuatro dominios de TI(PO -Planificación y Organización-; AI

- **Adquisición y Construcción/Implantación-;**

  DS -Entrega y Soporte-; y ME -Supervisión y Evaluación-), junto con sus treinta y cuatro procesos de TI normalizados, asociados.

- **Objetivos de control.**

  Muestra los objetivos de control detallados, correspondientes a cada uno de los procesos de TI u objetivos de control de alto nivel.

- **Directrices de auditoría.**

  Constituyen una referencia empleada para la revisión de los anteriores controles.

- **Directrices de gestión.**

  Desarrolladas para orientar a la Dirección en el Gobierno de TI, proporcionándole herramientas para evaluar y medir la capacidad de la

entidad en cada uno de los procesos TI definidos por COBIT, dentro de un modelo de madurez de seis niveles.

- **Herramientas de implantación.**

  Incluyen una guía para la puesta en marcha de COBITdentro de la organización.

  Desde la década de 1960, el rápido desarrollo de los sistemas automatizados ha creado la expectativa de una apropiada respuesta de las áreas que se ocupan de gestionar la tecnología informática y sistemas de información.

Muchas organizaciones se están reestructurando a fin de modernizar sus operaciones y simultáneamente aprovechar los avances en tecnologías de información a fin de mejorar su posición competitiva. La reingeniería del negocio, el dimensionamiento correcto, la tercerización y el procesamiento distribuido, son todos cambios que afectan la forma en que operan las organizaciones.

La alta velocidad con la cual se procesan las transacciones; los sistemas de administración de las bases de datos; las redes de telecomunicaciones globales; el procesamiento distribuido de datos; la comunicación sobre Internet, y muchos otros factores, han causado que en toda organización, sin excepción alguna, la información y los datos en los cuales se apoya se tornen cada día más y más importantes. Por lo que las estrategias de gerenciamiento; las políticas de seguridad; la segregación de las funciones; el impacto de las fallas computacionales; los accesos no autorizados; la revelación de la información; la continuidad del normal procesamiento de los datos; la adecuación de los sistemas de información, y otros

aspectos que surgen de la aplicación de innovadoras tecnologías, han pasado a tener un impacto mucho mayor dentro de la organización que el de hace unos años; de ahí la necesidad de contar con un adecuado marco de control.

Por lo expuesto, para muchas organizaciones, la información y la tecnología que la soporta, han pasado a representar sus activos más valiosos. Bajo esta situación, éstas han comenzado a reconocer los beneficios potenciales que las herramientas tecnológicas les pueden proporcionar. Pero sin embargo, también han comprendido la importancia de conocer y administrar los riesgos asociados con la implementación de las nuevas tecnologías.

2.8 Proceso de Auditoría

La preparación previa al comienzo de una auditoría implica la recolección de información de fondo sobre la compañía y la evaluación de recursos y habilidades requeridas para la ejecución de la auditoría. Esto permitirá que el personal con las habilidades requeridas sea asignado al proyecto.

Siempre es una buena práctica mantener una reunión de planificación con el principal responsable del área bajo revisión, de tal manera que se pueda obtener un entendimiento adecuado de las principales preocupaciones de la administración, y establecer un cronograma y una metodología de trabajo para la auditoría. Este tipo de reuniones permiten que la administración de la compañía se involucre en el proyecto, que la gente conozca el equipo de trabajo, aclarar las expectativas y establecer las principales preocupaciones.

La auditoría de sistemas debe abarcar tres grandes áreas:

- Auditoría de Infra EstructuraFísica y Lógica.
- Auditoría de Aplicaciones.
- Auditoría de estaciones de trabajo.
- Auditoría de las instalaciones físicas del departamento de Informática
- Auditoría de los conocimientos del personal del departamento de Informática.

Auditoría de Infraestructura Física y Lógica

Esta etapa de la auditoría debe de revisar múltiples áreas de la infraestructura, tales como lo son:

1. Diseño Lógico de la Red LAN.
2. Diseño Lógico de la Red WAN o MAN.
3. Diseño de DNS.
4. Tipos de servicios o aplicaciones que se ejecutaran en los servidores.
5. Fin o propósito de cada servidor y su respectiva configuración.
6. Cantidad de usuarios a los que se presta servicio con el objetivo deestablecer si el performance de cada servidor es el adecuado para las aplicaciones y cantidad de usuarios a los que presta servicio.

Diseño Lógico de la Red LAN.

Esta parte de una red abarca varias áreas, tales como lo son las diferentes subredes que se tendrán en la red, el propósito de cada una de ellas, los servicios o aplicaciones que correrán sobre dicha red.

En el caso de que una empresa u organización posea un edificio de más de 3 niveles para sus oficinas, es recomendable que se asigne una subred para cada nivel del edificio. Importante resaltar que los rangos de direccionamiento IP a utilizar. En caso de que se utilice DHCP es recomendable que se tengan bien definidos los grupos a los que pertenece cada estación de trabajo, para que así se pueda llevar un control de la subred asignada a dicho grupo.

Para el área de servidores se debecontemplar el direccionamiento fijo y una subred, la misma que se especifica a la cual apuntaran las estaciones de trabajo. Es recomendable que se haga un buen diseño de las subredes y se deje documentado el propósito de las mismas. Tomar en cuenta que los DNS y el Gateway deben pertenecer a una subred diferente a la de cada nivel o ubicación y a la subred de servidores, esto permite que se tenga una mejor seguridad.

Diseño Lógico de la Red WAN o MAN.

Tomar en cuenta que son parte de la misma empresa u organización, la única diferencia es que están retiradas de la central. Pero tienen derecho a acceder a ciertas áreas de la red, específicamente a servidores que les brindan algún tipo de servicio o aplicación. Para ello es recomendable que se diseñe una subred que utilice

direccionamiento IP privado, de preferencia que sea fijo y no dinámico, ya que esto simplifica la administración remota.

Los DNS generalmente son los mismos si tienen una sola salida al Internet, y su GateWay es variante, según la dirección IP que asigno el ISP para el enlace de punto a punto. Esimportante que se posea documentación de cómo se estructuro lógicamente la red.

Diseño de DNS.

En la mayoría de los casos una empresa u organización en Latinoamérica empieza siendo una empresa pequeña y después pasa a ser una empresa mediana. El negocio o giro es bueno y los dueños crean otras empresas que de igual manera tienen un crecimiento, posteriormente deciden unificarlas.

Esto en la mayoría de casos es muy complejo y difícil, ya que cada empresa tenia su propio domino, por ende sus propios DNS. Al unificarse el dominio, se puede complicar la unificación porque existen diversidad de aplicaciones y servicios en cada empresa, que están apuntando a su servidor de DNS.

Hay que hacer un análisis y reconfiguración de los DNS en estos casos y dejar bien configuradas las replicas o redireccionamientos en casos de ausencias de un servidor padre.

Tipos de servicios o aplicaciones que se ejecutaran en los servidores.

Es importante tener claro las aplicaciones que utiliza una empresa, como los son los ERP, CRM, SCM, u otros, servicios como Correo Electrónico, File Server, etc., las cuales se ubicaran en un "X" servidor, y la cantidad de usuarios que accederán a dicha aplicación. Hay que determinar que se necesita para cada conexión de usuario a la aplicación, para establecer si es correcta o no la configuración Física (Hardware) del servidor, con lo cual se puede establecer si el servidor posee suficientes recursos para atender las necesidades de cada requerimiento de conexión a la aplicación o servicio.

Fin o propósito de cada servidor y su respectiva configuración.

Inicialmente un servidor se adquirió con un fin o propósito especifico, y por ende posee un hardware capaz de brindar servicios para dicho fin. Generalmente, los servidores se encuentran haciendo 5 o 7 cosas mas de las que fueron su propósito inicial, y por ello es que un servicio o aplicación presentan problemas de respuesta o lentitud, ya que los recursos del hardware son menores a lo que se requiere para el software de las 5 o 7 aplicaciones corriendo simultáneamente.

Es por ello que se recomienda que un auditor verifique el propósito inicial con el que se adquirió un servidor de arquitectura, y en el caso de que no sea el adecuado se pueda hacer las recomendaciones del caso.

Cantidad de usuarios.

Hay que establecer la cantidad de usuarios a los que se presta servicio con el objetivo de establecer si el performance de cada servidor es el adecuado para las aplicaciones y cantidad de usuarios a los que presta servicio.

Auditoría de Aplicaciones:

Esta parte es muy compleja de revisar, ya que hay múltiples factores a tomar en cuenta de la aplicación a revisar, tales como:

- Lenguaje de Programación.
- Actualizaciones de la Aplicación.
- Fabricante.
- Trayectoria del Fabricante.
- Soporte en sitio.
- Tipo de base datos que utiliza.
- Diccionario de la estructura de la base de datos.
- Compatibilidad con programas generadores de reporte de terceros.
- Arquitectura de la aplicación.
- Métodos de acceso de los usuarios.
- Revisar si la aplicación posee bitácoras de tipo transaccional, con las cuales se pueda hacer rastreos de lo ejecutado por cada usuario en su sesión de trabajo.

Auditoría de Estaciones de Trabajo

Generalmente las empresas poseen un departamento de recursos humanos que tiene definidos los roles, funciones, atribuciones de cada uno de los empleados, por consiguiente informática debe tener conocimiento de que perfil tiene un empleado, para poder instalar el software necesario para el trabajo del empleado. Así poder determinar que no tenga juegos o herramientas que distraigan su atención, o que solamente consuman recursos de la estación de trabajo necesarios para su trabajo cotidiano. Por ello es que una empresa debe tener clara estas definiciones. Además se debe revisar que los usuarios no sean Administradores de sus equipos, para que no puedan instalar software a su discreción. Revisar que se posea el licenciamiento de los programas instalados en la estación de trabajo.

Auditoría de las instalaciones físicas del departamento de Informática

Esta parte es muy importante, ya que la seguridad física es parte fundamental, los puntos a revisar son:

- Métodos de acceso al cuarto de servidores.
- Bitácoras de acceso al área de servidores.
- Sistema de monitoreo por medio de video.
- Bitácoras de Video.
- Temperatura ambiente del área de servidores.
- Circuito eléctrico independiente del cuarto de servidores.

- Sistema de protección de descargas electro atmosféricas para el cuarto de servidores.
- Ubicación, distribución de los rack y propósito del rack.
- Sistemas detectores de humo.
- Equipos para apagado de fuego a base de CO2.
- Circulación del aire acondicionado en el cuarto de servidores.
- Canales aéreos de transporte del cableado estructurado que ingresa al cuarto.
- Rack independiente para equipos activos y pasivos de Voz, Datos, Video.
- Mapas disponibles de los diferentes puntos de red y su uso.
- Métodos de limpieza del área de servidores, frecuencia, entrenamiento del personal que la realiza, etc.

Auditoría de los conocimientos del personal del departamento de Informática:

Hay múltiples factores a evaluar según la función y puesto del personal, ya que el perfil y conocimientos de cada uno pueden variar según sus funciones y atribuciones.

Generalmente hay 6 tipos de personal en TI:

1. Gerente de Informática.
2. Administrador(es) de red LAN, WAN.
3. Desarrolladores de aplicaciones.
4. Administrador de bases de datos.
5. Técnico de atención a usuarios.

Según el puesto se recomienda hacer una batería de pruebas en conocimientos de las áreas que son responsables, para conocer las fortalezas y debilidades, con el objetivo de recomendar capacitación en las áreas débiles.

2.9 Modelos de Evaluación de Sistemas de Información

Los progresos realizados en un sistema deben ser medidos o evaluados para conocer las deficiencias y problemas que éste presenta. Aunque una evaluación cualitativa puede resultar útil en las etapas iniciales del desarrollo del sistema, medidas cuantitativas bajo unas mismas condiciones resultan de vital importancia para ver el progreso real del sistema y compararlo consigo mismo o con otros. Entre los principales marcos referenciales, modelos o conjunto de mejores prácticas se encuentran:

- Information Technology Control Guidelines.- Del Instituto Canadiense de Contadores (Canadian Institute of Chartered Accountants - CICA)
- Information Technology Investment Management.- Oficina de Contadores Generales de los Estados Unidos (US GAO)
- SysTrustMS/MD Principios y Criterios para la confiabilidad de los sistemas Del Instituto Canadiense de Contadores (Canadian Institute of Chartered Accountants - CICA) y el Instituto Americano de Contadores Públicos Certificados (American Institute of Certified Public Accountants - AICPA)
- Software Development Capability Maturity Model.- Instituto de Ingeniería de Software - SEI)

- Managing Systems Information: A Practical Assessment Tool.- Tabla de Recursos para la tecnología de la Información - ITRB)
- Norma para la Implementación de Políticas y Procedimientos de Seguridad para el Área Informática (ISO 17799).- Desarrollado y Publicado por la International Standard Organisation (ISO)
- Control Objectives for Information and related Technology (COBIT).- De la Fundación para la Auditoría y Control de los Sistemas de Información (Information Systems Audit and Control Foundation - ISACF) y del Instituto para la administración global de Tecnologías de la información (TI Governance Institute- ITGI).

2.10 Metodologías de la Auditoría

Existe algunas metodologías de auditoría informática que dependen de lo que se pretenda analizar y los procesos que se van auditar. En su gran mayoría de auditorías informáticas tienen procedimientos y tareas parecidas.

Las auditorías informáticas se clasifican de la siguiente manera:

- Generales
- Especificas

2.10.1 Metodologías Generales

Mediante metodologías generales permiten dar una opinión sobre la fialidad de la información, al final se entregará como resultado un informe detallado generalizando donde se encuentran las debilidades encontradas.

Es importante conocer que este tipo de auditoría tiene como material de trabajo los check list, cuestionarios, entrevistas entre otras que permiten anotar observaciones que ayudan a conservar un banco importante de pruebas sobre evidencias.

Con el uso de estas metodologías, permiten dar una opinión sobre la fiabilidad de la información, el resultado de esta metodología es un informe generalizado donde se destacan las debilidades encontradas. Es importante conocer que este tipo de auditoría tiene como material de trabajo los check list, cuestionarios, entrevistas, entre otras que permiten anotar observaciones que ayudan a conservar un banco importante de pruebas sobre hallazgos.

2.10.2 Metodologías Específicas

Las metodologías específicas son aquellas que el auditor interno o externo "crea" para su uso son mas especificas y exhaustivas, ya que sirve para evaluar un área en particular, al igual que la anterior metodología sus informes permiten el registro de observaciones.

2.10.3 Metodología de Auditoría Informática

Propone 4 fases para un correcto proceso de auditoría, estos son:

- Estudio preliminar.
- Revisión y evaluación de controles y seguridades.
- Examen detallado de áreas críticas
- Comunicación de resultados

Estudio preliminar.- esta fase es de vital importancia ya que los resultados de esta fase pueden conllevar a la interrupción de la auditoría si se considera y evidencia que no existen mayores problemas y justificativos en la aplicación de controles y seguridades; o por lo contrario constituye un valioso aporte para la planificación del examen.

Revisión y evaluación de controles y seguridades.- En esta etapa se precisa las áreas críticas que serán examinadas con profundidad en la siguiente fase, y a su vez elimina sistemas y procedimientos que no ameritan, bajo una relación costo - beneficio, invertir recursos para profundizar su examen.

Examen detallado de áreas críticas.- esta es la fase más importante de la Auditoría Informática, ya que se requiere mayor tiempo que las dos anteriores, y según sea la complejidad, se requiere de especialistas en informática que sean el soporte de las actividades técnicas que haya que profundizar. El desarrollo de esta fase se la realiza exclusivamente en el campo, y es prácticamente la culminación del trabajo de auditoría.

Comunicación de resultados.- En base a los resultados obtenidos de la fase anterior, es decir de las evidencias descritas en las hojas de apuntes, se procede a la elaboración del borrador del informe con la correspondiente aprobación de Auditoría Interna.

2.11 Técnicas y Herramientas de la Auditoría

Para desarrollar una auditoría se deben utilizar métodos, técnicas y herramientas de auditoría.

Existen diversos tipos de herramientas que se pueden utilizar y es importante que los auditores en informática deban conocer los beneficios que le brindan, así como los diferentes tipos de software que han sido diseñados para apoyar su función y para facilitar el manejo de la información.

La auditoría implica la aplicación de ciertos procedimientos, métodos o técnicas cuyos resultados, una vez obtenidos son incuestionable. La auditoría requiere el ejercicio de un juicio profesional y consistente, para encontrar los procedimientos que deben seguirse y valorar los resultados obtenidos.

Entre las herramientas y técnicas más utilizadas por los auditores se encuentran las siguientes:

2.11.1 Entrevista

Es una conversación cuya finalidad es la de obtener información; es un instrumento muy utilizado ya que permite recopilar información valiosa de la investigación que se está realizando, para realizarlo de mejor manera se debe considerar lo siguiente:

- Debe tratar respecto a un tema específico.
- Debe realizarse en un lugar cómodo e íntimo.

- Debe tener un tiempo determinado.
- Se debe realizar un número importante de preguntas en un mínimo de tiempo.

2.11.2 Encuesta

Es un método preparado para la investigación, se lo realiza a través de una observación no directa de los hechos sino por medio de lo que manifiestan los interesados. Se lo realiza a una muestra de una población con la ayuda de un cuestionario, de esta manera permite su aplicación masiva.

La utilización masiva de este instrumento en proceso de toma de decisiones, ayuda a la sistematización de procesos de trabajo en este tipo de estudios.

2.11.3 Cuestionario

Es un procedimiento de investigación, una entrevista altamente estructurada. "Un cuestionario consiste en un conjunto de preguntas respecto a una o más variables a medir". No requiere de mucho tiempo para reunir información sobre grupos numerosos. El sujeto que responde, proporciona por escrito las incógnitas planteadas.

2.11.4 Pruebas de Observación

A partir de la observación surge el planteamiento del problema que se va a estudiar, lo que lleva a emitir alguna hipótesis o suposición provisional de la que se intenta extraer una consecuencia. Existen ciertas pautas que han demostrado ser de utilidad en el establecimiento de las hipótesis y de los resultados que se basan en

ellas; estas pautas son: probar primero las hipótesis más simples, no considerar una hipótesis como totalmente cierta y realizar pruebas experimentales independientes antes de aceptar un único resultado experimental importante.

El analista de sistemas puede observar de tres maneras básicas.

1. Observar a una persona o actitud sin que el observado se dé cuenta y su interacción por aparte del propio analista. Quizá esta alternativa tenga poca importancia para el análisis de sistemas, puesto que resulta casi imposible reunir las condiciones necesarias.
2. El analista puede observar una operación sin intervenir para nada, pero estando la persona observada enteramente consciente de la observación.
3. Observar y a la vez estar en contacto con las personas observas. La interacción puede consistir simplemente en preguntar respecto a una tarea específica, pedir una explicación, etc.

2.12 COBIT

2.12.1 Análisis del Modelo de COBIT

COBIT constituye un modelo, que se enfoca en lo que se requiere para lograr una administración y un control adecuado de TI, y se posiciona en un nivel alto. Actúa como un integrador de todos estos materiales guía, resumiendo los objetivos clave bajo un mismo marco de trabajo integral que también se alinea con los requerimientos de gobierno y de negocios.

Por tal razón COBIT fue tomado como modelo de evaluación informática, ya que permite establecer controles sobre las TI y constituye una guía para realizar auditorías de esos mismos controles.

Es un modelo para implantar el Gobierno de TI, el mismo que ayuda a las organizaciones a alcanzar sus objetivos, facilitando la comprensión y la gestión de los riesgos.

2.12.2 Introducción a COBIT

COBIT es un Marco de referencia de procesos y objetivos de control TI que pueden ser implementados para controlar, auditar y administrar la organización TI. Este Marco de referencia está basado en las mejores prácticas y sistemas de información de auditoría y control. Esto en particular aspira a ayudar a los líderes empresariales a entender y administrar los riesgos relacionados con la Tecnología de la Información y la relación entre los procesos de administración, las preguntas técnicas, la necesidad de controles y los riesgos.

COBIT está estructurado por 4 campos principales de administración, los cuales a su vez implican 34 procesos de administración asociados con la tecnología de la información. Cada proceso TI provee una descripción de los requerimientos del negocio e identifica los asuntos claves que deben ser llevados a cabo para administrar exitosamente estos procesos.

COBIT ofrece un conjunto de herramientas para administrar los procesos TI unificando los dos puntos de vista, el de la administración y el del auditor. Las Guías de Administración TI consideran los controles TI desde una perspectiva de la administración, mientras que las Guías de Auditoría proveen asistencia específica a los auditores en el diseño de programas adecuados de auditoría para cada dominio. COBIT también provee herramientas detalladas y personalizables de auto evaluación en forma de matrices y plantillas para asistir en la evaluación y medición de la organización comparada con los criterios de COBIT.

Se ha definido a COBIT como: "una estructura de relaciones y procesos para direccionar y controlar la compañía para lograr la consecución de los objetivos del negocio, entregando valor agregado mientras se administra el riesgo en función del ambiente de sistemas y sus procesos".

2.12.3 Principios del Marco Referencial COBIT

COBIT enfatiza en su Marco Referencial, la relación directa existente entre la administración del negocio y la administración TI, debido a que actualmente la tecnología de la información no es exclusivamente una herramienta que facilite que la estrategia del negocio se cumpla, sino una parte integral de la estrategia del negocio. Por lo tanto es importante una administración TI que provea una estructura de control que enlace los procesos TI, recursos TI y la información con los objetivos y estrategias del negocio.

Así como la administración de un negocio tiene un soporte fundamental en la tecnología informática que posee, la administración TI debe estar en concordancia con los objetivos y estrategias de la empresa. De esta manera se concreta una relación directa y bidireccional entre la administración del negocio y de TI.

De esta manera el usuario del Marco Referencial puede entender, dentro de su organización:

- La relación entre los controles y objetivos de control.
- La importancia en el enfoque de las relaciones de los objetivos de control con los objetivos de negocio y los procesos.
- El valor de la administración de procesos y recursos relacionados a las iniciativas estratégicas.

2.12.4 Requerimientos del Negocio COBIT

Para la definición de los requerimientos del negocio sobre la información, COBIT se basó en importantes estándares de calidad (Ej. Normas ISO), regulatorios (Ej. Informe COSO) y de seguridad (Ej. Systrust). De esta manera logra definir que las principales características que la organización debe esperar de la información son (7):

- Efectividad.- Informaciónrelevante y pertinente para el proceso del negocio, así como su entrega se debe realizar de maneraoportuna, correcta, consistente y debe ser utilizable.
- Eficiencia.- Proveer la información a través de la utilización óptima (más productiva y económica) de recursos.

- Confidencialidad.- La información sensible debe ser protegida contra divulgación no autorizada.
- Integridad.- Precisión y suficiencia de la información, válida de acuerdo con los valores y expectativas del negocio.
- Disponibilidad.- De la información cuando ésta es requerida por el proceso de negocio en el presente y futuro. Salvaguardar de los recursos necesarios y capacidades asociadas.
- Cumplimiento.- De leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto.
- Confiabilidad.- Proveer de información apropiada a la administración, para operar la entidad y ejercer sus responsabilidades.

2.12.5 Relación de los Recursos TI

Para la administración exitosa de un ambiente informático se deberán tomar en cuenta los siguientes recursos:

- 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.
- Personal.- Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

La información que los procesos de negocio necesitan es proporcionada a través del empleo de recursos de TI. Con el fin de asegurar que los requerimientos de negocio para la información sean satisfechos, deben definirse, implementarse y monitorearse medidas de control adecuadas para estos recursos, esta relación (Recursos – requerimientos del negocio) se puede apreciar en el siguiente gráfico.

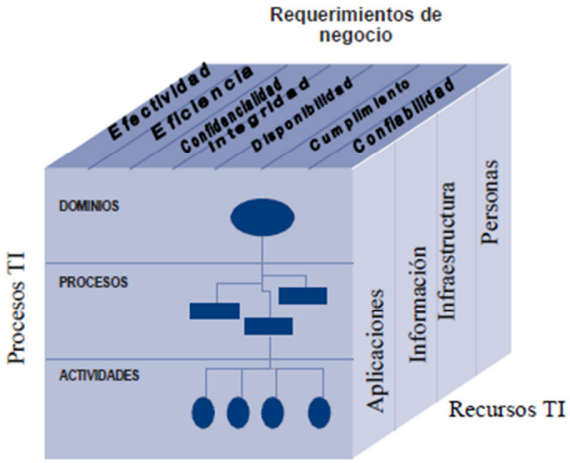

Figura 2.2: Integración COBIT (Requerimientos del Negocio – Procesos TI –Recursos TI)[9]

[9]Tomado de COBIT 4.0 Español

2.12.6 COBIT orientado a procesos

Para entender la combinación de los dos componentes anteriores (Requerimientos del Negocio y Recursos TI) se debe comprender que la información que los procesos de negocio necesitan es proporcionada a través del empleo de recursos de TI.

Un modelo de procesos fomenta la propiedad de los procesos, permitiendo que se defina sus responsabilidades. Para gobernar TI efectivamente, es importante determinar las actividades y los riesgos que requieren ser administrados.

Normalmente se ordenan dentro de dominios de responsabilidad de planear, construir, ejecutar y monitorear.

- Planeación y Organización(PO).- Este dominio cubre la estrategia y las tácticas, se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio.
- Adquisición e Implementación(AI).- Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio.
- Dar Soporte (DS).- En este dominio hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios.

- Monitorear y Evaluar (ME).- Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

2.12.7 Objetivos de Control

Los objetivos de control son un resultado de mejores prácticas para el manejo de información, que ayudan a asegurar que los procesos, los recursos de información y tecnología contribuyan al logro de los objetivos del negocio.

COBIT incluye 34 Objetivos de Control de alto nivel uno para cada uno de los procesos de tecnología informática, agrupados en cuatro dominios: planeación y organización, adquisición e implementación, entrega (de servicio) y monitoreo.

ESPACIO EN BLANCO INTENCIONAL

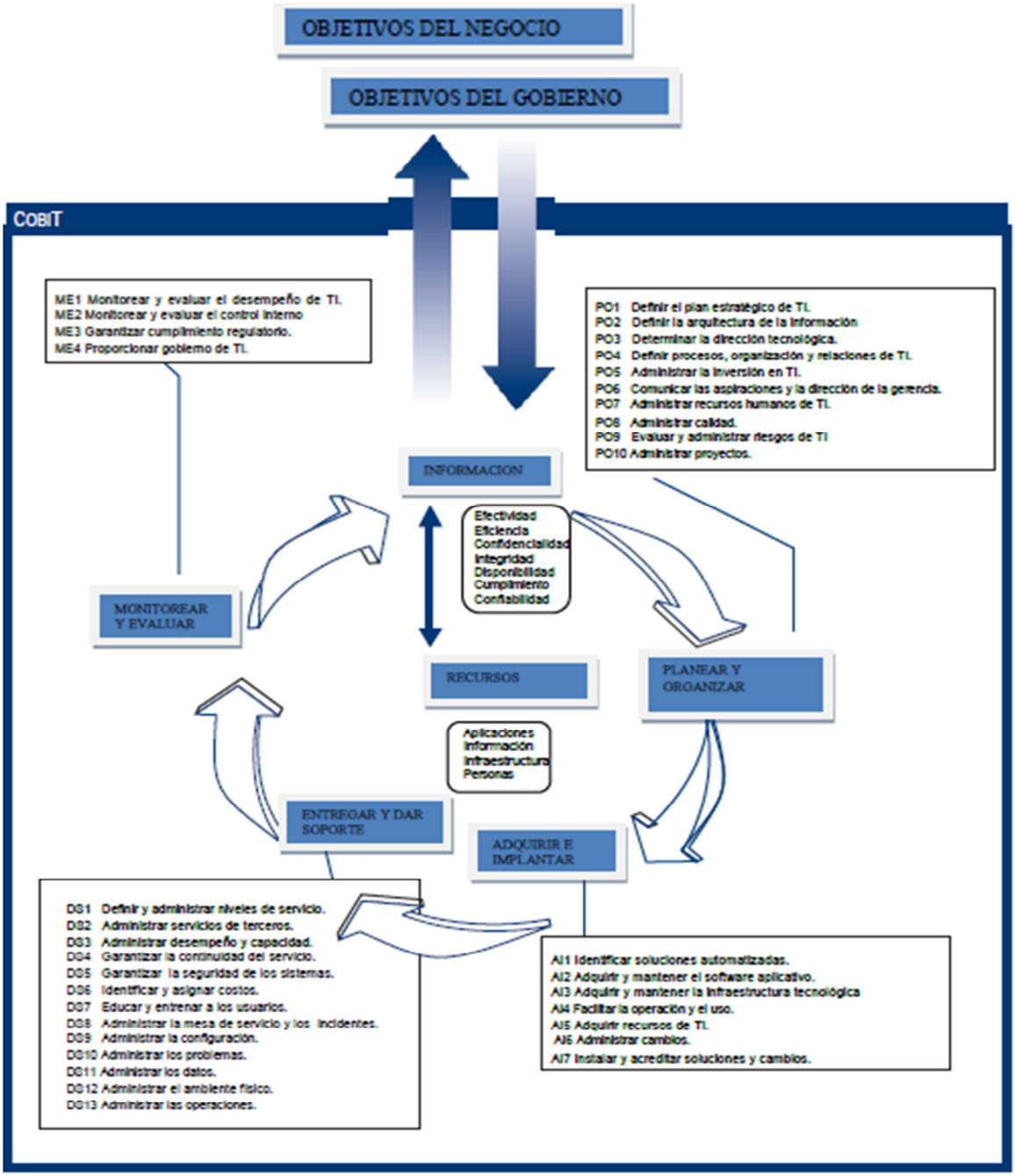

Figura 2.3: COBIT en Resumen[10]

[10]Tomado de COBIT 4.0 Español

2.12.7.1 Planear y Organizar

PO1: Definir un Plan Estratégico de TI

Objetivo: Se desarrolla y se implementa planes a largo y corto plazo que integren la misión y las metas de la organización, para lograr un balance óptimo a través de un proceso de planeación estratégica, mediante intervalos periódicos, teniendo metas claras y concretas a corto plazo.

PO2 Definir la Arquitectura de la Información

Objetivo: Satisfacer los requerimientos del negocio que se han organizado de manera que puedan satisfacer al sistema de información y que por medio de la implementación y el respectivo mantenimiento de un correcto modelo de negocio informativo, se pueda certificar que se han definido los sistemas correctos para que de esta manera se optimice la utilización de esta información.

PO3 Determinar la Dirección Tecnológica

Objetivo: Aprovechar al máximo de la tecnología que se encuentra disponible para todos, con la respectiva tecnología procedente, y así satisfacer los requerimientos del negocio, por medio de la creación y del mantenimiento respectivo para un plan de infraestructura tecnológica.

PO4 Determinar la Dirección Tecnológica

Objetivo: Realizar una organización conveniente en número y habilidades con sus respectivas tareas y sus responsabilidades definidas y comunicadas.

PO5 Administrar la Inversión en TI

Objetivo: Tener como finalidad la satisfacción de los requerimientos de negocio, para asegurar el financiamiento y el control de desembolsos de recursos financieros.

PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia

Objetivo: Asegurar que el conocimiento y comprensión de los usuarios sobre sus aspiraciones, sea concretas y verificar a través de políticas establecidas y transmitidas a los mismos, para lograr todo esto se debe basar en estándares para traducir las opciones en reglas de usuario prácticas y utilizables.

PO7 Administrar Recursos Humanos de TI

Objetivo: Maximizar las contribuciones del personal a los procesos de TI, satisfaciendo los requerimientos de negocio, mediante técnicas sólidas para administración de personal.

PO8 Administrar la Calidad

Objetivo: Cumplir con obligaciones legales, regulatorias y contractuales. Para esto se realizará una identificación y análisis respectivamente de los requerimientos externos en cuanto al impacto en TI.

PO9 Evaluar y Administrar los Riesgos de TI

Objetivo: Asegurar el cumplimiento de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI. Para ello se necesita de la

participación de la organización y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos.

PO10 Administración de proyectos

Objetivo: Establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión.

2.12.7.2 Adquirir e Implementar

AI1 Identificar Soluciones

Objetivo: Asegurar el mejor enfoque para cumplir con los requerimientos del usuario, para ello se realiza un análisis claro de las oportunidades alternativas comparadas contra los requerimientos de los usuarios.

AI2 Adquirir y Mantener Software de Aplicación

Objetivo: Proporcionar funciones automatizadas que soporten efectivamente al negocio.

AI3 Adquirir y Mantener Arquitectura Tecnológica.

Objetivo: Proporcionar las plataformas apropiadas para soportar aplicaciones de negocios.

AI4 Desarrollar y Mantener Procedimientos relacionados con T.I.

Objetivo: Asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas.

AI5 Instalar y Acreditar Sistemas

Objetivo: Verificar y confirmar que la solución sea adecuada para el propósito deseado.

AI6 Administrar Cambios.

Objetivo: Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores.

2.12.7.3 Entregar y dar Soporte

DS1 Definir Niveles de Servicio

Objetivo: Establecer una comprensión común del nivel de servicio requerido.

DS2 Administrar Servicios prestados por Terceros.

Objetivo: Asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos.

DS3 Administrar Desempeño y Capacidad.

Objetivo: Asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado.

DS4 Asegurar Servicio Continuo.

Objetivo: Mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones.

DS5 Garantizar la Seguridad de Sistemas.

Objetivo: Salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida.

DS6 Identificar y Asignar Costos.

Objetivo: Asegurar un conocimiento correcto de los costos atribuibles a los servicios de TI.

DS7 Educar y Entrenar a los Usuarios.

Objetivo: Asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados.

DS8 Apoyar y Asistir a los Clientes de T.I.

Objetivo: Asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente.

DS9 Administrar la Configuración.

Objetivo: Dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios.

DS10 Administrar Problemas e Incidentes

Objetivo: Asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que vuelvan a suceder.

DS11 Administrar Datos.

Objetivo: Asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento.

DS12 Administrar Instalaciones.

Objetivo: Proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

DS13 Administrar Operaciones.

Objetivo: Asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada.

2.12.7.4 Monitorear y Evaluar

M1 Monitorear los Procesos.

Objetivo: Asegurar el logro de los objetivos establecidos para los procesos de TI. Lo cual se logra definiendo por parte de la gerencia reportes e indicadores de desempeño gerenciales y la implementación de sistemas de soporte así como la atención regular a los reportes emitidos.

M2 Evaluar lo adecuado del Control Interno.

Objetivo: Asegurar el logro de los objetivos de control interno establecidos para los procesos de TI.

M3 Obtener Aseguramiento Independiente.

Objetivo: Incrementar los niveles de confianza entre la organización, clientes y proveedores externos. Este proceso se lleva a cabo a intervalos regulares de tiempo.

M4 Proporcionar Auditoría Independiente.

Objetivo: Incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas de su implementación, lo que se logra con el uso de auditorias independientes desarrolladas a intervalos regulares de tiempo.

ESPACIO EN BLANCO INTENCIONAL

CAPÍTULO 3

3. DESARROLLO DE LA AUDITORÍA

3.1 Introducción

Para el desarrollo de esta auditoría se realizó un análisis para identificar los riesgos más críticos de TI, a través de la Investigación de Campo y de la Matriz de Riesgos por medio de las cuales se pudo obtener una visión más clara de los problemas relacionados con TI, los mismos que se encuentran detallados y con sus respectivas recomendaciones en los informes que se presentan en este capítulo.

3.2 Matriz de Riesgos

Objetivos de Control	Auditado		Controles		Riesgo			Documentación	
	SI	NO	SI	NO	ALTO	MEDIO	BAJO	SI	NO
PLANEAR Y ORGANIZAR									
PO1 Definir un plan estratégico para IT									
PO1.4 Plan Estratégico de TI	x		x		x				x
PO1.5 Planes Tácticos de TI	x		x		x				x
PO3 Determinar la Dirección Tecnológica									
PO3.1 Planeación de la Dirección Tecnológica	x		x		x				x
PO3.2 Plan de Infraestructura Tecnológica	x				x			x	

PO4 Definir los Procesos, Organización y Relaciones de TI									
PO4.8 Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento	x		x		x				x
PO5 Administrar la Inversión en TI									
PO5.2 Prioridades Dentro del Presupuesto de TI	x		x		x			x	
PO7 Administración de Recursos Humanos de TI									
PO7.2 Competencias del Personal	x		x		x			x	
PO8 Administrar la Calidad									
PO8.1 Sistema de Administración de Calidad	x		x		x				x
PO8.2 Estándares y Prácticas de Calidad	x		x		x				x
PO9 Evaluar y Administrar los Riesgos de TI									
PO9.1 Marco de Trabajo de Administración de Riesgos	x		x		x			x	
PO10 Administración de Proyectos									
PO10.2 Marco de Trabajo para la Administración de Proyectos	x		x		x			x	

ADQUISICIÓN E IMPLEMENTACIÓN									
AI1 Identificar Soluciones Automatizadas									
AI1.1 Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del Negocio			x		x			X	

AI1.2 Reporte de Análisis de Riesgos				x	x				x
AI2 Adquirir y Mantener Software Aplicativo									
AI2.3 Control y Posibilidad de Auditar las Aplicaciones			x		x			x	
AI2.8 Aseguramiento de la Calidad del Software			x		x			x	
AI2.10 Mantenimiento de Software Aplicativo			x		x			x	
AI3 Adquirir y Mantener Infraestructura Tecnológica									
AI3.1 Plan de Adquisición de Infraestructura Tecnológica			x		x			x	
AI3.3 Mantenimiento de la Infraestructura			x		x			x	
AI4 Facilitar la Operación y el Uso									
AI4.4 Transferencia de Conocimiento al Personal Operaciones y Soporte			x		x			x	
AI6 Administración de cambios									
AI6.3 Cambios de Emergencia			x		x			x	
AI6.4 Seguimiento y Reporte del Estatus de Cambio									x

ENTREGA DE SERVICIOS Y SOPORTE									
DS1 Definir y administrar los niveles de servicio									
DS1.3 Acuerdos de Niveles de Servicio			x		x			x	

DS1.5 Monitoreo y Reporte del Cumplimiento de los Niveles de Servicio			x		x			x	
DS4 Garantizar la continuidad del servicio									
DS4.1 Marco de Trabajo de Continuidad de TI			x		x			x	
DS4.3 Recursos Críticos de TI			x		x			x	
DS4.4 Mantenimiento del Plan de Continuidad de TI			x		x			x	
DS4.5 Pruebas del Plan de Continuidad de TI			x		x			x	
DS5 Garantizar la seguridad de los sistemas									
DS5.1 Administración de la Seguridad de TI			x		x			x	
DS8 Administrar la Mesa de Servicio y los Incidentes									
DS8.1 Mesa de Servicios			x		x			x	
DS10 Administrar los problemas									
DS10.1 Identificación y Clasificación de Problemas			x		x			x	
DS10.2 Rastreo y Resolución de Problemas			x		x			x	
DS12 Administrar el ambiente físico (Instalaciones)									
DS12.1 Selección y Diseño del Centro de Datos				x	x				x
DS12.2 Medidas de Seguridad Física			x		x			x	

DS13 Administrar las operaciones									
DS13.5 Mantenimiento Preventivo del Hardware			x		x			x	

MONITOREAR Y EVALUAR									
M1 Monitorear y Evaluar el Desempeño de TI									
ME1.4 Evaluación del Desempeño	x		**x**		alto			x	
ME1.5 Reportes al Consejo Directivo y a Ejecutivos	x		**x**		alto			x	
M2 Monitorear y Evaluar el Control Interno									
ME2.1 Monitoreo del Marco de Trabajo de Control Interno	x		x		alto			x	

Tabla 3.1 Matriz de Riesgos

ESPACIO EN BLANCO INTENCIONAL

3.3 Plan de Investigación de Campo

No	Objetivo de Control	Objetivo de Control Detallado	Control	Documentos de Referencia	Fuente	Inst. de Inv. de campo
PO1 Definir un plan estratégico para IT						
PO1.4	**Plan Estratégico de TI**	Crear un plan estratégico que defina, en cooperación con los interesados relevantes, cómo TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados.	Plan estratégico de TI basado en los objetivos estratégicos del COSSFA (metas)	No existe	Gerente TI	Entrevista
PO1.5	**Planes Tácticos de TI**	Crear un portafolio de planes tácticos de TI que se deriven del plan estratégico de TI.	Como TI dará soporte a los programas de inversión facilitados por TI y a la entrega de los servicios operativos. Cómo se cumplirán y medirán los objetivos.	No existe	Gerente TI	Entrevista
PO3 Determinar la Dirección Tecnológica						
PO3.1	**Planeación de la Dirección Tecnológica**	Analizar las tecnologías existentes y emergentes y planear cuál dirección tecnológica es apropiada tomar para materializar la estrategia de TI y la arquitectura de sistemas del negocio.	Planear cuál dirección tecnológica es apropiada tomar para materializar la estrategia de TI y la arquitectura de sistemas del negocio	No existe	Gerente TI	Entrevista

No	Objetivo de Control	Objetivo de Control Detallado	Control	Documentos de Referencia	Fuente	Inst. de Inv. de campo
PO3.2	**Plan de Infraestructura Tecnológica**	Establecer un plan de infraestructura tecnológica que esté de acuerdo con los planes estratégicos y tácticos de TI.	Identificar en el plan qué tecnologías tienen el potencial de crear oportunidades de negocio. El plan debe abarcar la arquitectura de sistemas, la dirección tecnológica, las estrategias de migración y los aspectos de contingencia de los componentes de la infraestructura.	POA 2012	Gerente TI	Entrevista
PO4 Definir los Procesos, Organización y Relaciones de TI						
PO4.8	**Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento**	Establecer la propiedad y la responsabilidad de los riesgos relacionados con TI a un nivel superior apropiado	Definir y asignar roles críticos para administrar los riesgos de TI, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento.	No existe	Gerente TI	Entrevista
PO5 Administrar la Inversión en TI						
PO5.2	**Prioridades Dentro del Presupuesto de TI**	Implementar un proceso de toma de decisiones para dar prioridades a la asignación de recursos a TI.	Optimizar el retorno del portafolio empresarial de programas de inversión en TI y otros servicios y activos de TI.	No existe	Gerente TI	Entrevista

No	Objetivo de Control	Objetivo de Control Detallado	Control	Documentos de Referencia	Fuente	Inst. de Inv. de campo
PO7 Administración de Recursos Humanos de TI						
PO7.2	**Competencias del Personal**	Verificar de forma periódica que el personal tenga las habilidades para cumplir sus roles con base en su educación, entrenamiento y/o experiencia.	Evaluar que las competencias del personal están acorde a las funciones que requiere la gerencia de TI para mantener el negocio.	Descriptivo de Funciones	Gerente TI	Entrevista
PO8 Administrar la Calidad						
PO8.1	**Sistema de Administración de Calidad**	Establecer y mantener un QMS que proporcione un enfoque estándar, formal y continuo, con respecto a la administración de la calidad	Usar las buenas prácticas de la industria como referencia al mejorar y adaptar las prácticas de calidad de la organización.	No existe	Gerente TI	Entrevista
PO8.2	**Estándares y Prácticas de Calidad**	Identificar y mantener estándares, procedimientos y prácticas para los procesos clave de TI	Identificar y mantener estándares, procedimientos y prácticas para los procesos clave de TI para orientar a la organización hacia el cumplimiento del QMS.	No existe	Gerente TI	Entrevista

No	Objetivo de Control	Objetivo de Control Detallado	Control	Documentos de Referencia	Fuente	Inst. de Inv. de campo
PO9 Evaluar y Administrar los Riesgos de TI						
PO9.1	**Marco de Trabajo de Administración de Riesgos**	Integrar el gobierno, la administración de riesgos y el marco de control de TI, al marco de trabajo de administración de riesgos de la organización.	Desarrollar y mantener un proceso de respuesta a riesgos diseñado para asegurar que controles son efectivos y mitigan la exposición en forma continua.	No existe	Gerente TI	Entrevista
PO10 Administración de Proyectos						
PO10.2	**Marco de Trabajo para la Administración de Proyectos**	Establecer y mantener un marco de trabajo para la administración de proyectos que defina el alcance y los límites de la administración de proyectos.	Identificar las tareas de aseguramiento requeridas para apoyar la acreditación de los proyectos e incluirlos en el plan integrado.	Sistema 9000DOC	Gerente TI	Entrevista

AI1 Identificar Soluciones Automatizadas						
AI1.1	**Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del Negocio**	Identificar, dar prioridades, especificar y acordar requerimientos de negocio funcionales y técnicos que cubran el alcance completo de las iniciativas requeridas para lograr resultados en los programas de inversión en TI.	Definir requerimientos técnicos en base a la naturaleza del negocio	No Existe	Gerente TI	Entrevista

No	Objetivo de Control	Objetivo de Control Detallado	Control	Documentos de Referencia	Fuente	Inst. de Inv. de campo
AI1.2	**Reporte de Análisis de Riesgos**	Identificar, documentar y analizar los riesgos asociados con los procesos del negocio como parte de los procesos organizacionales para el desarrollo de los requerimientos.	Reportes de los riegos de TI analizados	No Existe	Gerente TI	Entrevista
AI2 Adquirir y Mantener Software Aplicativo						
AI2.3	**Esquema de Clasificación de Datos**	Implementar controles de negocio, cuando aplique, en controles de aplicación automatizados tal que el procesamiento sea exacto, completo, oportuno, autorizado y auditable.	Controles de Aplicaciones Automatizadas	No Existe	Gerente TI	Entrevista
AI2.8	**Aseguramiento de la Calidad del Software**	Desarrollar, implantar los recursos y ejecutar un plan de aseguramiento de calidad del software, para obtener la calidad que se especifica en la definición de los requerimientos y en las políticas y procedimientos de calidad.	Realizar un Plan de Aseguramiento de la Calidad en el que se especifique criterio de calidad y los procesos de validación y verificación.	No Existe	Gerente TI	Entrevista

No	Objetivo de Control	Objetivo de Control Detallado	Control	Documentos de Referencia	Fuente	Inst. de Inv. de campo
AI2.10	**Mantenimiento de Software Aplicativo**	Desarrollar una estrategia y un plan para el mantenimiento de aplicaciones de software.	Plan de Mantenimiento de Aplicaciones	No Existe	Gerente TI	Entrevista
AI3 Adquirir y Mantener Infraestructura Tecnológica						
AI3.1	**Plan de Adquisición de Infraestructura Tecnológica**	Generar un plan para adquirir, Implementar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio.	Evaluar el Plan de Adquisición de Infraestructura	POA2012	Gerente TI	Entrevista
AI3.3	**Mantenimiento de la Infraestructura**	Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios.	Verificar el Plan de Mantenimiento y procesos relacionados con el mismo.	Contratos de Mantenimiento	Gerente TI	Entrevista

No	Objetivo de Control	Objetivo de Control Detallado	Control	Documentos de Referencia	Fuente	Inst. de Inv. de campo
AI4 Facilitar la Operación y el Uso						
AI4.4	**Transferencia de Conocimiento al Personal Operaciones y Soporte**	Transferir el conocimiento y las habilidades para emitir al personal de soporte técnico y de operaciones que entregue, apoye y mantenga la aplicación y la infraestructura asociada de manera efectiva y eficiente	Documentación o Manuales donde se encuentre detallado las actividades o procesos que el encargado de cada área realiza	No Existe	Gerente TI	Entrevista
AI6 Administración de cambios						
AI6.3	**Cambios de Emergencia**	Establecer un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido.	Bitácora de Cambios de Emergencia	No Existe	Gerente TI	Entrevista
AI6.4	**Seguimiento y Reporte del Estatus de Cambio**	Establecer un sistema de seguimiento y reporte para mantener actualizados a los solicitantes de cambio y a los interesados relevantes	Cómo se da el seguimiento a los cambios que se realizan y como se administran los mismo	No Existe	Gerente TI	Entrevista

No	Objetivo de Control	Objetivo de Control Detallado	Control	Documentos de Referencia	Fuente	Inst. de Inv. de campo
DS1 Definir y Administrar los Niveles de Servicio						
DS1.3	**Acuerdos de Niveles de Servicio**	Definir convenios de niveles de servicios para todos los procesos críticos de TI en base en los requerimientos de negocio.	Contratos con el cliente. Documentación sobre los SLA's	No existe	Gerente TI Especialista de Redes	Entrevista
DS1.5	**Monitoreo y Reporte de Cumplimiento de los Niveles de Servicio**	Brindar seguimiento a los criterios definidos en los SLA's. Generar reportes para los interesados.	Evidencia de reportes. Hojas de control sobre el monitoreo. Contrato con los proveedores	No existe	Gerente TI Especialista de Redes	Entrevista
DS4 Garantizar la continuidad del servicio						
DS4.1	Marco de trabajo de continuidad de TI	Realizar un marco de trabajo de continuidad de TI que ayude a la determinación de la resistencia de la infraestructura.	Plan de Continuidad	No existe	Gerente TI Especialista de Redes	Entrevista
DS4.3	**Recursos Críticos de TI**	Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para establecer prioridades en situaciones de recuperación.		No existe	Gerente TI	Entrevista

No	Objetivo de Control	Objetivo de Control Detallado	Control	Documentos de Referencia	Fuente	Inst. de Inv. de campo
DS4.4	**Mantenimiento del Plan de Continuidad de TI**	Ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio.	Registro de actualizaciones al Plan de Continuidad de TI	No existe	Gerente TI	Entrevista
DS4.5	**Pruebas del Plan de Continuidad de TI**	Realizar pruebas de para asegurar que los sistemas puedan ser recuperados de una forma efectiva.		No existe	Gerente TI	Entrevista
DS5 Garantizar la seguridad de los sistemas						
DS5.1	**Administración de la Seguridad de TI**	Administración de la Seguridad de TI a un nivel acorde a la organización. Asegurar que el plan de seguridad este implementado políticas y procedimientos. Comunicar las políticas y procedimientos de seguridad.	Documentación del Plan de Seguridad	No existe	Gerente TI	Entrevista

No	Objetivo de Control	Objetivo de Control Detallado	Control	Documentos de Referencia	Fuente	Inst. de Inv. de campo
DS8 Administrar la Mesa de Servicio y los Incidentes						
DS8.1	**Mesa de Servicios**	Establecer la función de mesa de servicios. Debe existir procedimientos de monitoreo y escalamiento basados en los niveles de servicio acordados. Medir la satisfacción del usuario final relacionado con la calidad de la mesa de servicios.	Funcionalidad del Software aplicativo que ayuda en la gestión de incidentes. Documentación sobre procedimientos de monitoreo y escalamiento en base a los niveles de servicio	No existe documentación	Gerente TI	Entrevista
DS10 Administrar los problemas						
DS10.1	**Identificación y Clasificación de Problemas**	Verificar procesos para reportar y clasificar problemas que han sido identificados como parte de la administración de incidentes.	Revisar procedimiento para reportar y clasificar problemas que han sido identificados.	No existe documentación	Gerente TI	Entrevista
DS10.2	**Rastreo y Resolución de Problemas**	Mantener pistas de auditoría adecuadas que permitan rastrear y analizar la causa de los problemas reportados. Identificar y dar soluciones sostenibles indicando la causa raíz. Obtener reportes de la administración de cambios.	Reporte de administración de cambios. Evidenciar como se obtiene pistas de auditoría.	No existe documentación	Gerente TI	Entrevista

No	Objetivo de Control	Objetivo de Control Detallado	Control	Documentos de Referencia	Fuente	Inst. de Inv. de campo
DS12 Administrar el ambiente físico (Instalaciones)						
DS12.1	**Selección y Diseño del Centro de Datos**	Definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia del negocio.	Plan de mantenimiento a los equipos de seguridad. Controles de acceso al Centro de Cómputo.	No existe documentación sobre el plan de mantenimiento a los equipos de seguridad.	Gerente TI, Personal de HelpDesk	Entrevista
DS12.2	**Medidas de Seguridad Física**	Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio.	Verificar que en el plan de seguridad existan políticas para escoltar a invitados al área, donde se indique el motivo del acceso y la fecha y duración del mismo.	No existe documentación del plan seguridad.	Gerente TI, Técnico de Redes	Entrevista
DS13 Administración de Operaciones						
DS13.5	**Mantenimiento Preventivo del Hardware**	Procedimientos que garanticen el mantenimiento de la infraestructura.	Verificar procedimientos para dar mantenimiento preventivo del hardware de la empresa.	No existe documentación	Gerente TI, Técnico de Redes	Entrevista

M1 Monitorear y Evaluar el Desempeño de TI						
ME1.4	**Evaluación del Desempeño**	Comparar periódicamente el desempeño contra las metas, realizar análisis de la causa raíz e iniciar medidas correctivas.	Verificar si existe un proceso de control sobre la evaluación de desempeño.	No existe	Gerente TI Especialista de Redes	Entrevista

No	Objetivo de Control	Objetivo de Control Detallado	Control	Documentos de Referencia	Fuente	Inst. de Inv. de campo
ME1.5	**Reportes al Consejo Directivo y a Ejecutivos**	Proporcionar reportes administrativos para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas.	Comprobar si se proporciona reportes que indique el avance de la empresa.	No existe	Gerente TI	Entrevista
M2 Monitorear y Evaluar el Desempeño de TI						
ME2.1	**Monitoreo del Marco de Trabajo de Control Interno**	Monitorear de forma continua el ambiente de control y el marco de control de TI.	Verificar si se realiza el monitoreo del control interno.	No existe	Gerente TI	Entrevista

Tabla 3.2 Plan de Investigación de Campo

CAPÍTULO 4

4 RESULTADOS

4.1 Informe Detallado

En conformidad con el Plan del Proyecto de Tesis, “Evaluación Técnica Informática del Sistema de Información de la Empresa COSSFA, utilizando el Estándar Internacional COBIT”, se ha realizado la revisión de los controles referentes al dominio de Entrega de Servicios y Soporte implantados en Tecnología de la Información y Comunicaciones del COSSFA, de la que se detalla a continuación las observaciones y recomendaciones resultantes, en base del modelo COBIT.

ESPACIO EN BLANCO INTENCIONAL

PLANEAR Y ORGANIZAR (PO)

PO1 Definir un plan estratégico de TI

PO2 Definir la arquitectura de la información

PO3 Determinar la dirección tecnológica

PO4 Definir los procesos, organización y relaciones de TI

PO5 Administrar la inversión en TI

PO6 Comunicar las aspiraciones y la dirección de la gerencia

PO7 Administrar recursos humanos de TI

PO8 Administrar la calidad

PO9 Evaluar y administrar los riesgos de TI

PO10 Administrar proyectos

OBJETIVO DE CONTROL PO 1 Definir un plan estratégico para TI

PO1.4 Plan Estratégico de TI

Observación.-

La Gerencia de TI no cuenta con un plan estratégico.

Criterio.-

"Crear un plan estratégico que defina, en cooperación con los interesados relevantes, como TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados. Incluye cómo TI dará soporte a los programas de inversión facilitados por TI y a la entrega de los servicios operativos. Define cómo se cumplirán y medirán los objetivos y recibirán una autorización formal de los interesados. El plan estratégico de TI debe incluir el presupuesto de la inversión / operativo, las fuentes de financiamiento, la estrategia de obtención, la estrategia de adquisición, y los requerimientos legales y regulatorios. El plan estratégico debe ser lo suficientemente detallado para permitir la definición de planes tácticos de TI."

Condición.-

No se cuenta con un plan estratégico que permita una visión de cómo se cumplirán los objetivos del área. **(Evidencia: ENT-PO1)**

Causa.-

Debido a las siguientes situaciones:

- Falta de un plan de toda la empresa
- Falta de proyectos donde todas las áreas apoyen en la gestión de TI.

- Urgencia que hubo de levantar el área con la nueva razón social.
- Falta de información de toda el área entregada de la empresa anterior a la nueva razón social.

Efecto.-

Al no contar con una Planeación Estratégica no se podrá garantizar una efectiva administración en base a: prioridades organizacionales, uso eficiente de los recursos y materializar los portafolios de proyectos y servicios.

Toma de decisiones que ayuden y permitan prever el futuro del área de Tecnología, así como el establecimiento de perspectivas y metas para el mejoramiento de la Función de TI.

Recomendaciones.-

El Gerente de TI debe considerar la elaboración de un Plan Estratégico de TI que le permita tener una visión de las actividades tácticas que se deben realizar en el área.

Para realizar este fin, se debe considerar lo siguiente:

- Capacitar a todo el personal en norma, estándares y mejores prácticas que colabore para realizar una Planificación Estratégica de Tecnologías de Información.
- Realizar el Plan Estratégico de Tecnologías de Información, seleccionando una metodología (Anexo: Guía de Elaboración de un Plan Estratégico)

acorde con la institución y considerar asesoría especializada, a fin de garantizar niveles de calidad requeridos. El plan deberá:

  - Integrar las posibilidades de TI y la participación activa de las Unidades Organizacionales.
  - Estar alineado con los objetivos estratégicos de la empresa.
  - Identificar los costos y riesgos relacionados.
  - Identificar las estrategias para cumplir con los objetivos y sus mediciones.

- Recibir una autorización formal y aprobación de la Gerencia General de COSSFA.
- Incluir el presupuesto de la inversión / operativo, las fuentes de financiamiento, la estrategia de procuración, la estrategia de adquisición, y los requerimientos legales y regulatorios.
- Ser lo suficientemente detallado para permitir la definición de planes técnicos de TI.

- Involucrar a la administración en temas de planificación estratégica que tengan que ver con el área de TI y de esta forma lograr que los proyectos que se plantean para TI estén alineados con los objetivos institucionales. De igual manera la administración deberá involucrarse en temas de inversión para TI y de esta manera lograr una adecuada planificación del presupuesto.

Punto de vista.-Aprueba las recomendaciones, considerando que todas las unidades organizacionales de la institución deben estar involucradas en el levantamiento de los proyectos de TI que aporten a la consecución de los objetivos planteados para la institución.

PO1.5 Planes Tácticos de TI

Observación.-

No existe un portafolio de planes tácticos de TI.

Criterio.-

"Crear un portafolio de planes tácticos de TI que se deriven del plan estratégico de TI. Estos planes tácticos deben describir las iniciativas y los requerimientos de recursos requeridos por TI, y cómo el uso de los recursos y el logro de los beneficios serán monitoreados y administrados. Los planes tácticos deben tener el detalle suficiente para permitir la definición de planes de proyectos. Administrar de forma activa los planes tácticos y las iniciativas de TI establecidas por medio del análisis de los portafolios de proyectos y servicios. Esto incluye el equilibrio de los requerimientos y recursos de forma regular, comparándolos con el logro de metas estratégicas y tácticas y con los beneficios esperados, y tomando las medidas necesarias en caso de desviaciones."

Condición.-

No se encuentra un portafolio de proyectos que especifique cuáles son los planes tácticos de TI. **(Evidencia: ENT-PO2)**

Causa.-

No hay un plan estratégico de TI.

No hay planes tácticos de TI definidos.

Efecto.-

Al no contar con un portafolio de planes tácticos no se puede tener una concepción de cómo proceder, que es preciso realizar y cómo dirigir la Gerencia de TI, para el correcto desenvolvimiento de la misma que permita lograr el objetivo propuesto.

Recomendaciones.-

El Gerente de TI debe considerar la creación de un portafolio de planes tácticos que se deriven del Plan estratégico los mismos que sean una guía para las actividades que se ejecutan.

Punto de vista.-

Al contar con el plan estratégico donde se partió, con los objetivos trazados por la empresa, se puede establecer un plan táctico de TI donde se describa con más detalle la parte operativa.

OBJETIVO DE CONTROL PO 3 Definir la arquitectura de información

PO3.1 Planeación de la Dirección Tecnológica

Observación.-

El área de TI del COSSFA no cuenta con un planeación que le permita tomar decisiones acertadas.

Criterio.-

"Analizar las tecnologías existentes y emergentes y planear cuál dirección tecnológica es apropiado tomar para materializar la estrategia de TI y la arquitectura de sistemas del negocio. También identificar en el plan qué tecnologías tienen el potencial de crear oportunidades de negocio. El plan debe abarcar la arquitectura de sistemas, la dirección tecnológica, las estrategias de migración y los aspectos de contingencia de los componentes de la infraestructura".

Condición.-

No existe una planeación decisiva, el cual contemple: la arquitectura de sistemas, la dirección tecnológica, las estrategias de migración y los aspectos de contingencia de los componentes de la infraestructura. **(Evidencia: ENT-PO3)**

Causa.-

Falta de conocimiento para seguir una planeación por parte del personal de TI.

Efecto.-

- Se dejan de plantear y ejecutar proyectos tecnológicos de mayor impacto estratégico porque las unidades organizacionales "cliente" (producción, comercial, etc.) ignoran el potencial que ofrece un mejor manejo de la tecnología.

Recomendaciones.-

El Gerente de TI tendrá que desplegar sus conocimientos, habilidades en:

- La dirección de los proyectos tecnológicos y de investigación, visualizados desde su concepción como idea hasta la etapa de factibilidad comercial.

- La difusión e implantación de la tarea tecnológica en el resto de las áreas que componen la organización.
- Ejecución del plan técnico en la parte operativo en todas las áreas que componen TI.

Punto de Vista.-

La empresa tiene poco años de creación, para lo cual se debe considerar un plan que comprometa a la institución, enfocado en normas, estándares y buenas prácticas, realizando capacitaciones para lograr este fin.

PO3.2 Plan de Infraestructura Tecnológica

Observación.-

No existe un Plan de infraestructura tecnológica, ni se realiza un monitoreo de nuevas tendencias tecnológicas, debido a la falta de presupuesto para la posible implementación de las mismas, por cambio de prioridades para continuar con la operación de la institución.

Criterio.-

"Establecer un plan de infraestructura tecnológica que esté de acuerdo con los planes estratégicos y tácticos de TI. El plan se basa en la dirección tecnológica e incluye acuerdos para contingencias y orientación para la adquisición de recursos tecnológicos. También toma en cuenta los cambios en el ambiente competitivo, las economías de escala en la obtención de equipo de sistemas de información, y la mejora en la interoperabilidad de las plataformas y las aplicaciones".

Condición.- No existe evidencia de que se haya desarrollado un plan de infraestructura tecnológica, esto se encuentra rezagado debido al limitante en el presupuesto económico. **(Evidencia: ENT-PO4)**

Causa.-

- La falta de un Plan Estratégico Informático que defina la infraestructura tecnológica, los estándares tecnológicos a utilizar, en base a un estudio de las tendencias tecnológicas en el entorno local y mundial, puede provocar que el COSSFA no aproveche los adelantos que en el ámbito de las TI pueden brindarle una ventaja competitiva.
- No se cuenta con el presupuesto para la implementación de nuevas tecnologías, solo para mantener la operatividad de la institución.

Efecto.-

No se logra mantener la innovación tecnológica en la Institución, por lo que se pierde competitividad.

Recomendaciones.-

La Gerencia de TI debe hacer concientizar a los altos mandos sobre tendencias tecnológicas futuras dándole a conocer la ventaja a nivel competitivo que la organización puede asegurar.

Punto de Vista.-

En este momento la institución ha realizado un cambio de prioridades en los objetivos trazados para mantener la operación, por dicho motivo no se puede avanzar en el análisis para un plan de infraestructura tecnológica.

OBJETIVO DE CONTROL PO4 Definir los procesos, organización y relaciones de TI

PO4.8 Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento

Observación.-

No se realiza administración de riesgos.

Criterio.-

"Establecer la propiedad y la responsabilidad de los riesgos relacionados con TI a un nivel superior apropiado. Definir y asignar roles críticos para administrar los riesgos de TI, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento. Establecer responsabilidad sobre la administración del riesgo y la seguridad a nivel de toda la organización para manejar problemas a nivel de toda la empresa. Puede ser necesario asignar responsabilidades adicionales de administración de la seguridad a nivel de sistema específico para manejar problemas relacionados con seguridad. Obtener orientación de la alta dirección con respecto al apetito de riesgo de TI y la aprobación de cualquier riesgo residual de TI".

Condición.-

Se conoce acerca de cuáles son los riesgos relacionados con TI pero no se encuentra plasmado cuales son las posibles acciones que deben tomarse ante los mismos. **(Evidencia: ENT-PO5).**

Causa.-

Falta de recursos económicos e interés por parte de los dueños del COSSFA que permitan mitigar los riesgos de TI, motivo por el cual se encuentra rezagado la administración y análisis de riesgos, que ayude a evaluar las vulnerabilidades y los impactos potenciales, para así proponer resguardos y tácticas de mitigación.

Efecto.-

Al no realizar una administración de riesgos no se podrá:

- Priorizar y establecer niveles de riesgo para sus procesos y recursos empresariales críticos.
- Pasar de un enfoque de mitigar el riesgo a prevenir proactivamente las fallas.
- Tomar decisiones más informadas sobre cómo proteger su empresa.
- Evaluar las tácticas y los costos de la administración de riesgos relacionados con los diferentes niveles de protección.

Recomendaciones:

- Identificar eventos o amenazas que podrían tener impacto en la continuidad de las operaciones empresariales, y la probabilidad de que ocurran.
- Realizar un análisis detallado de amenazas o establecer planes de avance para mitigar riesgos.
- Determinar cómo las nuevas iniciativas empresariales o la nueva tecnología tendrán impacto en la empresa.
- Establecer planes de avance para mitigar riesgos.

Punto de Vista.-Se aprueba la observación, se requiere el apoyo para mitigar estos riesgos.

OBJETIVO DE CONTROL PO5 Administrar las inversiones de TI

PO5.2 Prioridades Dentro del Presupuesto de TI

Observación.-

El presupuesto de TI se lo asigna solo para el mantenimiento de la operatividad del COSSFA.

Criterio.-

"Implementar un proceso de toma de decisiones para dar prioridades a la asignación de recursos a TI para operaciones, proyectos y mantenimiento, para maximizarla contribución de TI a optimizar el retorno del portafolio empresarial de programas de inversión en TI y otros servicios y activos de TI".

Condición.-

Se encuentra plasmado en el POA las asignaciones de presupuesto a la Gerencia de TI para la administración de TI que permite mantener la correcta operación a nivel tecnológico del COSSFA **(Evidencia: ENT-PO6)**

Causa.-

Bajo presupuesto asignado para la gestión de TI.

Efecto.-

El COSSFA no cuenta con nueva tecnología que le ayude a mejorar su operatividad e implementar servicios de mayor calidad, por lo que se encuentra rezagada en relación con la competencia.

Recomendaciones.-

Informar a los altos mandos de los proyectos de TI que se pueden implementar para mejorar la operatividad de la organización si se la dota de nuevos y potentes recursos tecnológicos, los mismos que proporcionen tiempos de respuesta rápidos y eficientes.

Punto de Vista.-En este momento por condiciones de la empresa, la prioridad en el uso de los recursos asignados a TÏ van visualizados a mantener la operación de la empresa y no la inversión en nuevos proyectos acordes al avance tecnológico del mercado.

OBJETIVO DE CONTROL PO7 Administrar recursos humanos de TI

PO7.2 Competencias del Personal

Observación PO.-

No existen Políticas adecuadas para la Gestión de Recursos Humanos.

Criterio.-

“Verificar de forma periódica que el personal tenga las habilidades para cumplir sus roles con base en su educación, entrenamiento y/o experiencia. Definir

los requerimientos esenciales de habilidades para TI y verificar que se les dé mantenimiento, usando programas de calificación y certificación según sea el caso".

Condición.-

No se realizan evaluaciones específicas orientadas a medir el desempeño técnico y la calidad del servicio del personal del área. **(Evidencia: ENT-PO7)**

Causa.-

Desconocimiento sobre la importancia de contar con personal experimentado y que conoce el giro del negocio en el área de TI.

Efecto.-

- No contar con la cantidad de personal necesario para cada una de las actividades a realizar, consecuentemente no poder brindar un servicio de calidad a los usuarios.
- Demora o paralización de proyectos por la falta de personal**.**
- No contar con un personal motivado para realizar su trabajo de la mejor manera.

Recomendaciones:

- Evaluar y monitorear el grado de satisfacción de los empleados.
- Debería implantarse un sistema de evaluación del desempeño interno para cada área.

Punto de Vista.-

Se tiene conocimiento de este análisis pero no se cuenta con presupuesto asignado a capacitación del personal por las prioridades en las que COSSFA se encuentra.

OBJETIVO DE CONTROL PO8 Administrar la calidad

PO8.1 Sistema de Administración de Calidad

Observación.-

No existe un Sistema de Administración de Calidad en TI.

Criterio.-

“Establecer y mantener un QMS que proporcione un enfoque estándar, formal y continuo, con respecto a la administración de la calidad, que esté alineado con los requerimientos del negocio. El QMS identifica los requerimientos y los criterios de calidad, los procesos claves de TI, y su secuencia e interacción, así como las políticas, criterios y métodos para definir, detectar, corregir y prever las no conformidades. El QMS debe definir la estructura organizacional para la administración de la calidad, cubriendo los roles, las tareas y las responsabilidades. Todas las áreas clave desarrollan sus planes de calidad de acuerdo a los criterios y políticas, y registran los datos de calidad. Monitorear y medir la efectividad y aceptación del QMS y mejorarla cuando sea necesario”.

Condición.-

Según la documentación y en base a la entrevistas se ha comprobado que no existe personal dedicado al aseguramiento de la calidad de los servicios de TI. **(Evidencia: ENT-PO8)**

Causa.-

El área de TI no ha determinado políticas tendientes al logro de la calidad de sus servicios.

Efecto.-

La falta de un Sistema de Administración de Calidad conlleva a que la Función de TI no logre satisfacer los requerimientos de la institución en su totalidad, por ende no aporte a alcanzar las metas establecidas en el Plan Estratégico Institucional y no se puedan efectuar procesos de mejora.

Recomendaciones.-

- Diseñar e implementar un Sistema de Administración de la Calidad dentro de los procesos que se llevan a cabo en la Gerencia de TI.
- Determinar la responsabilidad para la administración de la calidad de los servicios brindados por la Gerencia de TI.
- Establecer una comisión responsable del aseguramiento de la calidad conformada por los miembros de la función de Servicios de información y establecer sistemas de aseguramiento de calidad apropiados.

Punto de Vista-Implementar un sistema consolidado para realizar esto.

PO8.2 Estándares y Prácticas de Calidad

Observación.-

El Área de TI mantiene un esquema de brindar servicios de calidad en los procesos que realiza, pero no se lo realiza en base a estándares de calidad.

Criterio.-

"Identificar y mantener estándares, procedimientos y prácticas para los procesos clave de TI para orientar a la organización hacia el cumplimiento del QMS. Usar las buenas prácticas de la industria como referencia al mejorar y adaptar las prácticas de calidad de la organización."

Condición.-

Se trata de desarrollar los procesos basados en calidad pero no se tiene un procedimiento para realizarlo. **(Evidencia: ENT-PO9)**

Causa.-

Falta de conocimiento del personal de TI acerca de las mejores prácticas de calidad.

Efecto.-

No asegurar la calidad de los servicios brindados por TI.

Recomendaciones.-

- Identificar cuáles son los estándares y mejores prácticas de calidad, e implementar los mismos en los procesos claves de TI.

Punto de Vista.-

El área de TI cuenta de acuerdo al presupuesto con niveles básicos de calidad para brindar solución a todos los requerimientos internos.

OBJETIVO DE CONTROL PO9 Evaluar y administrar los riesgos de TI

PO9.1 Marco de Trabajo de Administración de Riesgos

Observación.-

Los riesgos operativos relacionados con tecnologías de información no han sido evaluados a un nivel adecuado.

Criterio.-

“Integrar el gobierno, la administración de riesgos y el marco de control de TI, al marco de trabajo de administración de riesgos de la organización. Esto incluye la alineación con el apetito de riesgo y con el nivel de tolerancia al riesgo de la organización”.

Condición.-

No se encuentra plasmado un plan de acción para mitigar los riesgos, se tiene un conocimiento empírico de las acciones que se deben tomar en caso de un contingente. **(Evidencia: ENT-PO10)**

Causa.-

Desconocimiento de los fundamentos y metodologías para la gestión de riesgos en TI.

Efecto.-

- Los activos de la organización se encuentran expuestos a riesgos.
- No se consideran todos los riesgos que puedan afectar el área y los actores que se encuentren implicados a mitigarlos para evitar un alto impacto.

Recomendaciones.-

- El Gerente de TI deberá integrar la gestión del riesgo de TI a la gestión del riesgo institucional, mediante la elaboración del plan de seguridad y continuidad del negocio.

Punto de Vista.-No se tiene plasmado en un documento el marco de trabajo de administración de riesgo, pero se tiene empíricamente el conocimiento para aplicar un procedimiento en caso de que se presente un riesgo.

OBJETIVO DE CONTROL PO 10 Administrar proyectos

PO10.2 Marco de Trabajo para la Administración de Proyectos

Observación.-

No se cuenta con un marco de trabajo para la administración de proyectos.

Criterio.-

"Establecer y mantener un marco de trabajo para la administración de proyectos que defina el alcance y los límites de la administración de proyectos, así como las metodologías a ser adoptadas y aplicadas a cada proyecto emprendido. Las metodologías deben cubrir, como mínimo, el inicio, la planeación, la ejecución, el

control y el cierre de las etapas de los proyectos, así como los puntos de verificación y las aprobaciones. El marco de trabajo y las metodologías de soporte se deben integrar con la administración del portafolio empresarial y con los procesos de administración de programas".

Condición.-

- No existe evidencia de estudios de factibilidad de los proyectos de TI.
- No existe evidencia de un procedimiento de priorización de los proyectos, en base de las necesidades del plan estratégico institucional.

(Evidencia: ENT-PO11)

Causa.-

No se cumple con una metodología establecida para la administración de los proyectos TI.

Efecto.-

No se encuentra bien administrados los recursos financieros.

Recomendaciones.-

- Revisar las políticas y normativa relacionada con la administración de proyectos como la metodología PMI.
- El Responsable del Área de Proyectos deberá verificar el cumplimiento de las metodologías y políticas para la administración de los proyectos.

Punto de Vista-Se acepta la observación.

ADQUIRIR E IMPLEMENTAR (AI)

AI1 Identificar soluciones automatizadas

AI2 Adquirir y mantener software aplicativo

AI3 Adquirir y mantener infraestructura tecnológica

AI4 Facilitar la operación y el uso

AI5 Adquirir recursos de TI

AI6 Administrar cambios

AI7 Instalar y acreditar soluciones y cambios

OBJETIVO DE CONTROL AI1 Identificar soluciones automatizadas

AI1.1 Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del Negocio

Observación.-

El proceso de definición y mantenimiento de los requerimientos técnicos y funcionales no se efectúa para todos los proyectos de TI.

Criterio.-

"Identificar, dar prioridades, especificar y acordar los requerimientos de negocio funcionales y técnicos que cubran el alcance completo de todas las iniciativas requeridas para lograr los resultados esperados de los programas de inversión en TI. Definir los criterios de aceptación de los requerimientos. Estas iniciativas deben incluir todos los cambios requeridos dada la naturaleza del negocio, de los procesos, de las aptitudes y habilidades del personal, su estructura organizacional y la tecnología de apoyo".

Condición.-

- No existe evidencia de análisis costo-beneficio en los proyectos de TI.
- No existe evidencia de un proceso, metodología ni estándares para soluciones automatizadas.
- Los registros de solicitud de asistencia técnica, se llevan a mano porque TI no cuenta con un aplicativo que automatice este subproceso.
- En el control de inventario de TI, no existe un aplicativo que automatice el proceso de ingreso de recursos.

- HelpDesk lleva un registro de existencias tecnológicas, con sus respectivas cantidades, lugar de ubicación, descripción, en hojas electrónicas (Excel).

(Evidencia: ENT-AI1)

Causa.-

Falta de políticas y normatividad referente al tema.

Efecto.-

- Al no definir un análisis costo-beneficio difícilmente se podrá establecer las ventajas al ejecutar los proyectos.
- Si TI no cuenta con un aplicativo que controle los recursos de TI, se hace imposible analizar el desempeño y estado de los mismos, provocando perjuicios considerables por falta de información oportuna.

Recomendaciones.-

Establecer y poner en ejecución, política y normativa, que permita:

- Asegurar que la justificación de los proyectos de TI contemplen el análisis costo-beneficio, para permitir la priorización de cada proyecto.
- Definir una metodología para la identificación y evaluación de las soluciones de TI que estará sujeta a una mejora continua y con flexibilidad para proyectos de pequeña y gran escala sobre el conocimiento interno y externo, con referencia de soluciones tecnológicas probadas con éxito.

Punto de Vista.-

Se debe realizar una consideración de los requerimientos que se tiene dentro del área para definir la envergadura del proyecto, dependiendo la envergadura del proyecto para realizar estas observaciones.

AI1.2 Reporte de Análisis de Riesgos

Observación.-

No existe evidencia de análisis de riesgos para cada proyecto de tecnología de información.

Criterio.-

"Identificar, documentar y analizar los riesgos asociados con los procesos del negocio como parte de los procesos organizacionales para el desarrollo de los requerimientos. Los riesgos incluyen las amenazas a la integridad, seguridad, disponibilidad y privacidad de los datos, así como el cumplimiento de las leyes y reglamentos".

Condición.-

- La única referencia de análisis de riesgos se encuentra en el Plan de Contingencia realizado en el 2010, pero este no se encuentra actualizado. (Evidencia: Plan de Contingencia del 2010).
- No existe evidencia de análisis de riesgos detallada para cada proyecto de TI
- No existe evidencia de algún plan de acción para la mitigar riesgos de TI, tampoco se detallan políticas ni normas para evitar incidentes.
- No existe documentación de los sistemas críticos.
- El personal del área de TI, no conoce acerca de los estándares o metodología utilizada para la realización del Plan de Contingencia.

(Evidencia: ENT-AI2)

Causa.-

- En el análisis de riesgos solamente se enumera el riesgo pero no se detalla la incidencia del riesgo en los proyectos ni en las actividades que se cumplen.
- No se determina una metodología a nivel organizacional para la identificación de amenazas que afecten las vulnerabilidades de los activos tecnológicos, procedimientos para la cuantificación del riesgo, análisis de costo y de impacto, definición de controles preventivos y correctivos que mitiguen la incidencia del riesgo sobre las actividades que realiza el COSSFA.
- No identifican los sistemas críticos.
- No existe ninguna norma definida para seguridades informáticas que se contemple en el Plan de Contingencia.

Efecto.-

- La falta de una evaluación de riesgos afecta principalmente a los requerimientos de efectividad, confidencialidad, integridad y disponibilidad de información de las áreas de TI.
- Si no se identifican debilidades y amenazas, los proyectos relacionados con hardware, software y comunicaciones no se ejecutan de manera óptima.
- Si no controlan los recursos de tecnología de información, fácilmente el COSSFA sigue retrasado en tecnología.

Recomendaciones.-

- El proceso de administración de riesgos TI debe considerar las siguientes características:

- Análisis vulnerabilidades asociadas a los recursos de TI (errores, daño intencional, vandalismo, equivocaciones, ataque, robo, acceso no autorizado, falla de hardware o software),
- Evaluación de la probabilidad de ocurrencia de las amenazas,
- Diseño de nuevos controles que permitan reducir las debilidades hasta un nivel aceptable de riesgo.

- El resultado de la implementación de una evaluación de riesgos debe ser el generar controles tanto preventivos como correctivos que permitan mitigar la incidencia del riesgo. El nivel remanente de riesgo (riesgo residual), una vez que los controles hayan sido implementados debe ser conocido y aprobado por las autoridades más relevantes del COSSFA.
- Se debe elaborar un Plan de Contingencia actualizado, basándose en el Plan Estratégico del COSSFA, análisis de vulnerabilidades y contar con estándares y normas necesarias que garanticen la protección de los recursos de TI.

Punto de Vista.-Se acepta la observación.

OBJETIVO DE CONTROL AI2 Adquirir y Mantener Software Aplicativo

AI2.3 Control y Posibilidad de Auditar las Aplicaciones

Observación.-

No existen controles, solo se realiza auditabilidad de la aplicación más crítica del COSSFA, el cual se encuentra medianamente administrado.

Criterio.-

"Implementar controles de negocio, cuando aplique, en controles de aplicación automatizados tal que el procesamiento sea exacto, completo, oportuno, autorizado y auditable."

Condición.-

Se detalla la definición de pistas de auditoría, pero no existe ninguna descripción de esta actividad. **(Evidencia: ENT-AI4)**

Causa.-

No está definido por parte de la Institución un proceso de auditoría exclusivo para tecnologías de información; la Unidad de Auditoría Interna se enmarca a actividades de control financiero y cumplimiento de proyectos.

Efecto.-

- Al no existir controles de hardware y software en el COSSFA, tampoco se realizan planes preventivos de seguridades para el desarrollo de aplicativos.
- No se cuenta con un equipo especializado de auditoría informática en la Unidad de Auditoría Interna de la COSSFA, ni con procesos o reglamentos definidos para llevar a cabo la implementación de auditorías informáticas que respondan a los controles existentes.

Recomendaciones.-

Se deben establecer controles físicos y lógicos para cada aplicativo, de forma que el procesamiento sea exacto, completo, oportuno, aprobado y auditable, deberá

manejar mecanismos de autorización, integridad de la información, control de acceso, respaldo y diseño de pistas de auditoría.

Los controles deben ser manuales y automatizados con software especializado, enmarcados en los estándares de calidad más relevantes como ITIL, ISO, COBIT. Los encargados de implantar estos controles deberán tener conocimientos de auditoría informática.

Punto de Vista.-

El área cuenta con un proceso de análisis, diseño e implementación de desarrollo de software, que se lo realiza sin contar con documentos que respalden estos procesos. Se realizan pruebas con el usuario previo al paso a producción. Adicionalmente estos procesos son revisados por auditoría interna para ajustar los controles que se requiere.

OBJETIVO DE CONTROL AI2.-Adquirir y Mantener Software Aplicativo

AI 2.3.-Control y Posibilidad de Auditar las Aplicaciones

No existen controles, solo se realiza auditabilidad de la aplicación más crítica del COSSFA, el cual se encuentra medianamente administrado.

Criterio.-

“Implementar controles de negocio, cuando aplique, en controles de aplicación automatizados tal que el procesamiento sea exacto, completo, oportuno, autorizado y auditable.”

Condición.-

Se detalla la definición de pistas de auditoría, pero no existe ninguna descripción de esta actividad. **(Evidencia: ENT-AI4)**

Causa.-

No está definido por parte de la Institución un proceso de auditoría exclusivo para tecnologías de información; la Unidad de Auditoría Interna se enmarca a actividades de control financiero y cumplimiento de proyectos.

Efecto.-

- Al no existir controles de hardware y software en el COSSFA, tampoco se realizan planes preventivos de seguridades para el desarrollo de aplicativos.
- No se lleva a cabo pruebas donde se tenga que especificar como resultados el tiempo de respuesta de los aplicativos.
- No se cuenta con un equipo especializado de auditoría informática en la Unidad de Auditoría Interna de la COSSFA, ni con procesos o reglamentos definidos para llevar a cabo la implementación de auditorías informáticas que respondan a los controles existentes.

Recomendaciones.-

Se deben establecer controles físicos y lógicos para cada aplicativo, de forma que el procesamiento sea exacto, completo, oportuno, aprobado y auditable, deberá manejar mecanismos de autorización, integridad de la información, control de acceso, respaldo y diseño de pistas de auditoría.

Los controles deben ser manuales y automatizados con software especializado, enmarcados en los estándares de calidad más relevantes como ITIL, ISO, COBIT.

Los encargados de implantar estos controles deberán tener conocimientos de auditoría informática.

Punto de Vista.-Se acepta la observación.

AI2.8 Aseguramiento de la Calidad del Software

Observación.-

No existen recursos definidos para ejecutar un plan de aseguramiento de calidad del software en COSSFA.

Criterio.-

"Desarrollar, implantar los recursos y ejecutar un plan de aseguramiento de calidad del software, para obtener la calidad que se especifica en la definición de los requerimientos y en las políticas y procedimientos de calidad de la organización. Los asuntos a considerar en el plan de aseguramiento de calidad incluyen el especificar el criterio de calidad y los procesos de validación y verificación, incluyendo inspección, revisión de algoritmos y código fuente y pruebas".

Condición.-

No existe documentación sobre un plan de aseguramiento de calidad, donde se incluyan los procesos de validación, revisión de código fuente. **(Evidencia: ENT-AI3)**

Causa.-

El personal no cuenta con los conocimientos necesarios de los mejores estándares de calidad utilizados para el desarrollo de aplicativos.

Efecto.-

No se puede comprobar que el software adquirido o desarrollado sea apropiado según los requerimientos, y con los estándares propios de la metodología de desarrollo de software e ingeniería de software, que proporcionen aseguramiento de la calidad del software.

Recomendaciones.-

Desarrollar, implantar los recursos y ejecutar un plan de aseguramiento de calidad del software con especificaciones de requerimientos, políticas y procedimientos de calidad. El plan de aseguramiento de calidad debe contener los criterios de calidad y los procesos de validación y verificación, incluyendo inspección, revisión de algoritmos y código fuente y pruebas.

Punto de Vista.-

El área de tecnología cuenta con un proceso de análisis, diseño e implementación de desarrollo de software empíricamente mas no plasmado en un documento.

AI 2.10.- Mantenimiento de Software Aplicativo

No existe mantenimiento para todos los aplicativos del COSSFA

Criterio.-

“Desarrollar una estrategia y un plan para el mantenimiento de aplicaciones de software.”

Condición.-

No se realiza ningún tipo de mantenimiento programado a los aplicativos, el único que se puede mencionar es el que se lo realiza a petición de usuario en caso de problemas con los aplicativos. (**Evidencia: ENT-AI5)**

Causa.-

No existe el proceso definido de mantenimiento de aplicativos específicamente, por lo que no se realiza planes de mantenimiento, el único registro es acerca de cambios efectuados en el Aplicativo.

Efecto.-

El mantenimiento de software aplicativo es trascendental en la funcionalidad de los aplicativos y en el éxito de las transacciones, la falta de un plan para el mantenimiento provoca ineficiencia en los aplicativos existentes, defectos de programa y no se permiten corregir fallas de manera eficiente.

Recomendaciones.-

La Gerencia de TI debe desarrollar un plan para el mantenimiento preventivo que registre la planeación y evaluación de recursos, reparación de defectos de programa y corrección de fallas después de cumplirse el ciclo de vida definido.

Se debe evaluar las pequeñas mejoras a los aplicativos en períodos trimestrales, documentando cambios de efectuados de emergencia, interdependencia con otras aplicaciones e infraestructura, estrategias de actualización, soporte, riesgos y requerimientos de seguridad.

Punto de Vista.-

El área de TI debe trabajar en conjunto con las demás áreas y sobre todo en el área de procesos, para que en conjunto se defina un plan de mantenimiento programado a los procesos que se encuentran en el sistema.

OBJETIVO DE CONTROL AI3.-Adquirir y Mantener Software Aplicativo

AI 3.1.- Plan de Adquisición de Infraestructura Tecnológica

No está definido un Plan de Infraestructura Tecnológica en un documento físico debido a la falta de presupuesto para su adquisición.

Criterio.-

"Generar un plan para adquirir, implementar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio, y que esté de acuerdo con la dirección tecnológica de la organización. El plan debe considerar extensiones futuras para adiciones de capacidad, costos de transición, riesgos tecnológicos y vida útil de la inversión para actualizaciones de tecnología. Evaluar los costos de complejidad y la viabilidad comercial del proveedor y el producto al añadir nueva capacidad técnica."

Condición.-

- Se realiza un Plan de Adquisiciones Anual, como **se evidencia POA2012**, pero no se utiliza un estándar para su realización, solamente se lo hace teniendo en cuenta los requerimientos de los usuarios y el criterio de la Gerencia de TI.

- El Director de Logística no tiene nada que ver en la elaboración del Plan de Adquisiciones de Tecnologías de Información, está unidad solo se encarga de realizar las adquisiciones solicitadas en base a la documentación enviada por la Gerencia de TI.**(Evidencia: ENT-AI6)**

Causa.-

- La Unidad de Logística al encargarse de la mayoría de adquisiciones del Comisariato como se describe en el Reglamento Interno de Adquisiciones, debería contar con un técnico en TI permanentemente, el mismo que brindará asesoramiento al momento de realizar algún tipo de adquisición referente con software, hardware y comunicaciones.
- El Plan de Adquisiciones de Hardware y Software se encuentra establecido de cierta manera en el PLAN OPERATIVO ANUAL (evidencia POA2012), el cual contiene las adquisiciones de Hardware y Software. A nivel institucional, el Plan de Adquisiciones de Hardware y Software como tal no existe individualmente, ni tampoco una Planificación de Adquisiciones de Infraestructura que contemple estándares y políticas para el manejo y mantenimiento de infraestructura tecnológica.
- Falta de Planificación estratégica Informática, que establezca bases sólidas de las funcionalidades de la Gerencia de TI y sus respectivos responsables.

Efecto.-

- El Plan de Adquisiciones actual solo favorece a la sede COSSFA Matriz, mientras a las otras sedes se les deja en segundo plano los requerimientos planteados.

- La satisfacción del usuario no es medida, y no se exigen controles de calidad para las actividades que se cumple en el COSSFA, la insuficiencia de políticas, normas y estándares para el manejo, adquisición y mantenimiento de tecnologías de información, no permite mantener confiabilidad en los sistemas de información, lo que conlleva a un nivel alto de riesgo en las actividades.
- Al no existir un monitoreo del desempeño de los recursos de TI, se desaprovecha la funcionalidad de los mismos, y la vida útil que estos pueden proveer a la Institución.
- La falta de asignación del suficiente recurso económico para adquisiciones hace que la Gestión de TI se quede rezagada y que no se realicen planes para hacer nuevas implementaciones de software, hardware y redes de comunicaciones.

Recomendaciones.-

- La Unidad de Logística debe ser la única unidad encargada de realizar todo el proceso de adquisiciones de infraestructura del COSSFA, estas actividades incluyen la convocatoria a proveedores, calificación a los mismos, evaluación y estudios de las ofertas con un técnico designado de la Gerencia de TI.
- El Gerente de TI juntamente con los analistas de cada área deben definir procesos de calidad para satisfacción del usuario y para los recursos de TI que interactúan con las actividades de los usuarios.
- Debería existir un monitoreo de los recursos de TI, y esto tendría que ser manejado por cada área de la Gerencia de TI.

- Se debería documentar normas y estándares para el manejo de Infraestructura tecnológica en un plazo máximo de tres meses, aplicando normas internacionales: ITIL para definición de procesos; ISO 20000 y 270001 para procesos, controles y seguridades informáticas.
- Se debe realizar actualizaciones periódicas del estado de tecnología cada dos meses y analizar si los avances tecnológicos favorecen al COSSFA para implementar nuevas tecnologías.

Punto de Vista.-Se acepta la observación.

OBJETIVO DE CONTROL AI4 Facilitar la Operación y el Uso

AI4.4 Transferencia de Conocimiento al Personal Operaciones y Soporte

Observación.-

No cuenta con manual ni documentación sobre la transferencia de conocimientos al personal de operaciones y soporte.

Criterio.-

"Transferir el conocimiento y las habilidades para emitir al personal de soporte técnico y de operaciones que entregue, apoye y mantenga la aplicación y la infraestructura asociada de manera efectiva y eficiente de acuerdo a los niveles de servicio requeridos. La transferencia de conocimiento debe incluir al entrenamiento inicial y continuo, el desarrollo de las habilidades, los materiales de entrenamiento, los manuales de operación, los manuales de procedimiento y escenarios de atención al usuario."

Condición.-

- Al momento no cuentan con manuales de operaciones para la administración de Sistemas, Redes y / o Aplicaciones.
- No se realiza manuales sobre procesos creados recientemente.
- La capacitación al personal lo da el Gerente del Departamento de TI y Comunicaciones donde se le explica sobre que servicios, estado de recursos, habilidades, a partir de ello la persona debe actuar de forma empírica. **(Evidencia: ENT-AI7)**
- El colaborador, entrega un acta al término del período de trabajo donde se describe las actividades y la entrega de claves de todo lo que administraba.

Causa.-

El recurso humano del Departamento de TI es limitado, la demanda de servicios existentes que deben atender es exorbitante con el reducido personal que cuenta el Departamento.

Efecto.-

Atención limitada para el soporte de los servicios que brinda el Departamento de TI y Comunicaciones, afectando así todos los ambientes relacionados con el proceso de negocio.

Recomendaciones.-

- Transferir el conocimiento y las habilidades para permitir al personal de soporte técnico y de operaciones que entregue, apoye y mantenga la aplicación y la infraestructura asociada de manera efectiva y eficiente de

acuerdo a los niveles de servicio requeridos, incluyendo entrenamiento inicial y continuo, desarrollo de habilidades, materiales de entrenamiento, manuales de operación, manuales de procedimientos y escenarios de atención al usuario.

- El proceso para la documentación de usuario y de operación se mejora constantemente con la adopción de nuevas herramientas o métodos, el uso de administración de conocimiento actualizada, workflow y tecnologías de distribución, que los hacen accesibles y fáciles de mantener.

Punto de Vista.-Se acepta la observación.

OBJETIVO DE CONTROL AI3 Adquirir y Mantener Infraestructura Tecnológica

AI3.3 Mantenimiento de la Infraestructura

Observación.-

No existe mantenimiento de la Infraestructura Tecnológica.

Criterio.-

"Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios de la organización. Incluir una revisión periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad."

Condición.-

- No existen manuales de actualizaciones y renovación de licencias de los recursos de TI.
- En el caso del hardware se da un mantenimiento preventivo a los equipos del COSSFA.
- Pocas computadoras tienen licencia de Software. **(Evidencia: OBS-AI8)**

Causa.-

- El recurso humano del Departamento de TI es limitado, la demanda de servicios existentes que deben atender es exorbitante con el reducido personal que cuenta el Departamento.

Efecto.-

- Atención limitada para el soporte de los servicios que brinda el Departamento de TI y Comunicaciones, afectando así todos los ambientes relacionados con el proceso de negocio.

Recomendaciones.-

- Transferir el conocimiento y las habilidades para permitir al personal de soporte técnico y de operaciones que entregue, apoye y mantenga la aplicación y la infraestructura asociada de manera efectiva y eficiente de acuerdo a los niveles de servicio requeridos, incluyendo entrenamiento inicial y continuo, desarrollo de habilidades, materiales de entrenamiento, manuales de operación, manuales de procedimientos y escenarios de atención al usuario.

- El proceso para la documentación de usuario y de operación se mejora constantemente con la adopción de nuevas herramientas o métodos, el uso de administración de conocimiento actualizada, workflow y tecnologías de distribución, que los hacen accesibles y fáciles de mantener.

Punto de Vista.-Si existiera el presupuesto y el personal completo dentro del área se pudiera cumplir con las recomendaciones.

OBJETIVO DE CONTROL AI6 Administración de cambios

AI6.3 Cambios de Emergencia

Observación.-

No existen definidos procedimientos ni políticas para la atención y manejo de cambios de emergencia.

Criterio.-

"Establecer un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido. La documentación y pruebas se realizan, posiblemente, después de la implementación del cambio de emergencia."

Condición.-

- No se tiene un proceso definido para atender cambios de emergencia.
- No se especifica nada acerca de cambios de emergencia ni procedimientos para manejar este tipo de situaciones.

- No existen controles específicos documentados para acceso a aplicativos en producción para realizar cambios de emergencia. **(Evidencia: ENT-AI9)**

Causa.-

- No se tiene definido ningún procedimiento en los diferentes procesos para manejo de cambios de emergencia en todas las áreas del Departamento de TI y Comunicaciones.
- No existen controles al momento de realizar cambios de emergencia como son los planes de retroceso para poder deshacer los cambios de manera oportuna si existiese algún conflicto o problema con el cambio implantado.

Efecto.-

- Debido a la falta de procedimientos de manejo de los cambios considerados como urgentes y al ser estos de carácter más crítico y destructivo para el sistema, estos pueden dejar sin funcionamiento por completo al sistema si no existen controles necesarios para la manipulación de los componentes que son afectados por el cambio urgente.

Recomendaciones.-

Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formalmente y controladamente. Los cambios (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar y autorizar previo a la implantación y revisar contra los resultados planeados después de la implantación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.

Punto de Vista.-

Todos los cambios de emergencia que se han realizado han obtenido resultados positivos a pesar de no tener la documentación porque se tiene claro el procedimiento a ejecutarse en cada una de las sub áreas. Los cambios de emergencia que se han ejecutado hasta el momento han sido en el servidor principal de la base de datos en el gestor de aplicativos y en el core de comunicaciones.

AI6.4 Seguimiento y Reporte del Estatus de Cambio

Observación.-

No se tiene un proceso o políticas definidas de seguimiento y reporte del estatus de cambios. Solo se contempla en el área de software y del aplicativo principal.

Criterio.-

"Establecer un sistema de seguimiento y reporte para mantener actualizados a los solicitantes de cambio y a los interesados relevantes, acerca del estatus del cambio a las aplicaciones, a los procedimientos, a los procesos, parámetros del sistema y del servicio y las plataformas fundamentales."

Condición.-

- El seguimiento de las peticiones de cambio no se tiene establecido como una de las actividades en los procesos del Departamento de TI y Comunicaciones.
- Los formatos de registro de petición de cambios establecen un mecanismo para el seguimiento de los mismos muy básico.

- No existe proceso alguno o política donde se haga conocer al usuario sobre el estado del cambio de manera formal. **(Evidencia: ENT-AI10)**

Causa.-

- No se tiene procedimientos ni políticas definidas para el seguimiento de cambios y definición de estado del mismo con respecto a la petición inicial.

Efecto.-

- Al no establecerse un seguimiento apropiado de los cambios realizados, no se puede evaluar si las acciones que se tomaron fueron óptimas y adecuadas para no afectar el funcionamiento de los sistemas.
- La falta de reporte de estatus del cambio no permite que se defina si el cambio ha sido llevado a cabo dentro de un periodo adecuado y tampoco definir un tiempo estimado de atención y solución de los pedidos receptados, provocando una falta de evaluación acerca de cómo afecto en función del tiempo al servicio proporcionado a los usuarios.

Recomendaciones.-

- El Gerente del Departamento de TI y Comunicaciones debe establecer como política que para el procedimiento de cambios debe llevarse a cabo un seguimiento detallado para poder evaluar los cursos de acciones tomadas si fuera necesario procedimientos o acciones que se puedan adaptar para manejar cambios parecidos o iguales a los presentados y así solucionarlos de manera más eficiente y más eficaz sin afectar el sistema e inclusive remediarlos antes de que suceda o se pida algún cambio semejante.

- El Gerente del Departamento de TI y Comunicaciones en conjunto con sus colaboradores del área deben lograr establecer dentro de los registros de pedidos de cambios algún ítem que permita realizar una definición del estatus de los cambios y que este se base en los pasos o procedimientos llevados a cabo para poder evaluar cuantitativamente cuanto tiempo se tomo para la realización de los diferentes pasos que se tomo para la terminación del cambio.

Punto de Vista.-

El área de tecnología ha adoptado un procedimiento de levantamiento seguimiento de los procesos a ejecutarse dentro de la sub área de aplicativos donde se ha controlado los tiempos de entrega y actividades realizadas para cumplir estos objetivos, dentro de las otras sub áreas se ha realizado un seguimiento intuitivo y no documental. Loa dos opciones antes señaladas han arrojado hasta el momento resultados positivos dentro de la operación de la empresa.

ESPACIO EN BLANCO INTENCIONAL

ENTREGAR Y DAR SOPORTE (DS)

DS1 Definir y administrar los niveles de servicio

DS2 Administrar los servicios de terceros

DS3 Administrar el desempeño y la capacidad

DS4 Garantizar la continuidad del servicio

DS5 Garantizar la seguridad de los sistemas

DS6 Identificar y asignar costos

DS7 Educar y entrenar a los usuarios

DS8 Administrar la mesa de servicio y los incidentes

DS9 Administrar la configuración

DS10 Administrar los problemas

DS11 Administrar los datos

DS12 Administrar el ambiente físico

DS13 Administrar las operaciones

OBJETIVO DE CONTROL DS 1 Definir y Administrar los Niveles de Servicio

DS1.3 Acuerdos de Niveles de Servicio

Observación.-

Existen SLA's para algunos servicios, pero no se encuentran definidos al nivel de la demanda del área, el personal conoce en forma parcial sobre los mismos.

Criterio.-

"Definir y acordar convenios de niveles de servicios para todos los procesos críticos de TI con base en los requerimientos del cliente y las capacidades en TI. Esto incluye los compromisos del cliente, los requerimientos de soporte para el servicio, métricas cualitativas y cuantitativas para la medición del servicio firmado por los interesados, en caso de aplicar los arreglos comerciales y de financiamientos y los roles y responsabilidades, incluyendo la revisión del SLA. Los puntos a considerar son disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte, planeación de continuidad, seguridad y restricciones de demanda."

Condición.-

Durante la revisión, se identificaron las siguientes novedades:

- No se encuentra documentado los SLA's entre los usuarios que reciben los servicios de tecnología y el proveedor.
- Se maneja por medio de contratos para agenciar o reportar la disponibilidad de servicio.
- No exite un método de seguimiento de desempeño, desacuerdo a las políticas de servicios.

- Las expectativas de desempeño en base a los SLA's no satisfacen las necesidades de los objetivos de la empresa. **(Evidencia: DOC-DS1)**

Causa.-

- No se mantiene definiciones básicas de las configuraciones, parámetros de calidad y disponibilidad de los servicios de tecnología.

Efecto.-

Deficiencia en el uso de tecnologías y falta de competitividad.

Recomendaciones.-

Se debe restructurar los SLA's de acuerdo a los objetivos del COSSFA, en el que se indique la disponibilidad y la calidad con la que se prestarán los servicios de TI.

Punto de Vista.-

El área de tecnología ha levantado sus propios niveles de SLA para atender todos los requerimientos solicitados en las áreas de acuerdo a la necesidad del cliente externo y entrega de servicios de calidad a ese mismo cliente. Adicionalmente el área de TI ha solicitado el cumplimiento de los niveles de SLA con sus proveedores de servicios que en este ámbito recae sobre la empresa de comunicaciones.

ESPACIO EN BLANCO INTENCIONAL

DS1.5 Monitoreo y Reporte de Cumplimiento de los Niveles de Servicio

Observación.-

No se cuenta con un proceso sobre el seguimiento que se le da a los SLA's en COSSFA.

Criterio.-

"Monitorear continuamente los criterios de desempeño especificados para el nivel de servicio. Los reportes sobre el cumplimiento de los niveles de servicio deben emitirse en un formato que sea entendible para los interesados. Las estadísticas de monitoreo son analizadas para identificar tendencias positivas y negativas tanto de servicios individuales como los servicios en conjunto."

Condición.-

- Durante la revisión, se identificaron las siguientes novedades:
    - No existe evidencia de un seguimiento a los servicios de tecnología prestados por proveedores externos y el Departamento de TI y Comunicaciones; tampoco existe evidencia de un análisis de los problemas encontrados en los servicios de tecnología. Se dió a conocer verbalmente que "De manera mensual se envía el reporte a TELCONET, para que se pueda realizar el pago, se hacen notas de crédito por el servicio caído".
    - No se realiza un monitoreo continuo de las hojas de control de soporte técnico, que permita detectar la existencia de fallas en el servicio recibido o casos no resueltos.

- No se analiza el impacto que puede causar el desempeño especificados en los SLA's.
- No se ha designado una persona responsable de monitorear y reportar el cumplimiento de los SLA's. **(Evidencia: DOC-DS2)**

Causa.-

Falta procedimientos para el seguimiento de los SLA's; desconoce de estándares de buenas prácticas.

Efecto.-

Pierde continuidad. Problemas específicos no encontrados para el aseguramiento de efectividad del proceso.

Desconocimiento de la calidad de servicios prestada, errores o fallas en los mismos que permitan aplicar medidas correctivas para mejorar los servicios de tecnología, así como sanciones y garantías estipuladas en los contratos firmados entre los proveedores de servicios externos y el Departamento de TI y Comunicaciones.

Recomendaciones.-

El Gerente de TI, desde el primer trimestre del año en curso, designará a un administrador de los SLA's, quien será responsable de monitorear y reportar los alcances de los criterios de desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento. Las estadísticas de monitoreo deberán ser analizadas oportunamente. Deberán tomarse acciones correctivas apropiadas e investigarse las fallas para poder identificar tendencias positivas o negativas de servicios.

Punto de Vista.-

El área de TI venía utilizando una herramienta propia para el seguimiento de todos los casos abiertos y se realizaba un análisis de tiempos de respuesta de y de niveles de satisfacción sobre el caso atendido con el objetivo de mejorar el servicio interno.

Todos los contratos con proveedores externos manejan y tienen clausulas de cumplimiento con niveles de SLA.

OBJETIVO DE CONTROL DS4 Garantizar la continuidad del servicio

DS4.1 Marco de Trabajo de Continuidad de TI

Observación.-

Cuenta con un marco de trabajo de Continuidad de TI incompleto.

Criterio.-

“Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias.

El marco de trabajo debe tomar en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación

de desastres y los planes de contingencia de TI. El plan debe también considerar puntos tales como la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y los principios de respaldo y recuperación."

Condición.-

- No posee un plan de continuidad realizado en base a una metodología definida, un análisis de riesgos de la información y los recursos tecnológicos más importantes.
- No toma en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes para documentar, realizar pruebas y en efecto realizar la ejecución del Plan de Contingencia. **(Evidencia: DOC-DS3)**

Causa.-

- El Departamento de TI y Comunicaciones, no ha desarrollado políticas y normatividad referente al tema.
- No se ha realizado un análisis de las operaciones del COSSFA, en el que se considere la información y las operaciones críticas de las áreas que forman parte de la Institución.

Efecto.-

- Riesgo de no mantener la continuidad de las operaciones del COSSFA, en el caso de la ocurrencia de desastres.

- Incremento de los costos implicados en la recuperación de la operatividad de los sistemas y datos.
- Errores en el procesamiento de transacciones en el período de contingencia.

Recomendaciones.-

El Gerente de TI, en cooperación con los propietarios de los procesos del negocio, definirá políticas y normatividad en el que consten los roles, responsabilidades, la metodología a seguir basada en riesgo, las reglas monitoreo y disponibilidad de los recursos críticos, procesamiento alternativos, principios de respaldo y recuperación y la estructura para documentar el plan de continuidad, así como los procedimientos de aprobación, el plan de continuidad del negocio, proveerá a la organización la habilidad para continuar operando los procesos críticos definidos, a un nivel menor al normal aceptado, en ocasiones en las que se produzcan eventos que ocasionen la paralización de los servicios informáticos.

Punto de Vista.-

A pesar de no contar documentalmente con información para mantener la continuidad del negocio, en los eventos presentados donde se vio afectada el área de ti y por ende la continuidad del negocio se ha podido solventar la operatividad con tiempos de respuesta aceptables, dentro de los recursos que tiene.

ESPACIO EN BLANCO INTENCIONAL

DS4.3 Recursos Críticos de TI

Observación.-

El área de TI no centraliza la atención en puntos determinados como los más críticos, para construir resistencia y establecer prioridades en situaciones de recuperación.

Criterio.-

"Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación. Evitar la distracción de recuperar los puntos menos críticos y asegurarse de que la respuesta y la recuperación están alineadas con las necesidades prioritarias del negocio, asegurándose también que los costos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales. Considerar los requerimientos de resistencia, respuesta y recuperación para diferentes niveles de prioridad, por ejemplo, de 1 a 4 horas, de 4 a 24 horas, más de 24 horas y para periodos críticos de operación del negocio."

Condición.-

- No existe documentación que respalde la centralización de la atención de puntos determinados como los más críticos en el plan de continuidad de TI.
- Al no contar con un plan de continuidad TI, no se centra la atención en puntos determinados como los más críticos, para construir resistencia y establecer prioridades en situaciones de recuperación.

- No existen planes de recuperación de desastre/contingencia, que sean actuales y que sea comprendido por todas las partes afectadas.
- Teóricamente existe planes de contingencia, pero no están desarrollados tomando como base la no disponibilidad de los recursos físicos para llevar a cabo procesamientos críticos manuales y computarizados. **(Evidencia: ENT-DS4)**

Causa.-

Falta de procesos y normatividad para centralizar la atención en puntos determinados como los más críticos.

Efecto.-

No existen procedimientos de resistencia y de establecimiento de prioridades en situaciones de recuperación.

Recomendaciones.-

El Especialista de Redes y Comunicaciones de TI debe implantar un plan de continuidad TI y ejecutar una revisión detallada de los objetivos del plan para asegurar una centralización de los puntos más críticos y la creación de una estrategia apropiada para garantizar la continuidad general del negocio.

Punto de Vista.-

A pesar de no contar con documentación se tiene claro que puntos son los más críticos para dar una solución emergente y mantener la continuidad dentro del negocio.

DS4.4 Mantenimiento del Plan de Continuidad de TI

Observación.-

No se actualiza el Plan de Continuidad de TI en base a los requerimientos actuales del negocio.

Criterio.-

"Exhortar a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio. Es esencial que los cambios en los procedimientos y las responsabilidades sean comunicados de forma clara y oportuna."

Condición.-

- El plan de contingencia que se ha definido para el COSSFA y en el cual se indica las acciones a ser llevadas a cabo al momento de que se produzcan desastres se encuentra desactualizado.
- COSSFA cuenta únicamente con un plan de contingencia ante un incidente, lo cual dificultaría una pronta recuperación del procesamiento de datos que soporta el proceso financiero. No existe un plan de continuidad del negocio que garantice una respuesta apropiada ante situaciones de emergencia que ocasionen pérdidas parciales o totales del servicio informático. **(Evidencia: ENT-DS5)**

Causa.-

El Departamento de Tecnología de Información y Comunicaciones, no ha desarrollado políticas y normatividad referente al tema.

Efecto.-

- No existen procedimientos de resistencia y de establecimiento de prioridades en situaciones de recuperación.
- Riesgo de pérdida de información importante y vulnerable referente a las operaciones del COSSFA.

Recomendaciones.-

La persona encargada de los procesos del negocio debe implantar el Plan de Continuidad para asegurar y garantizar que se determinen los recursos de respaldo que deben ser almacenados en el sitio alterno. La instalación de almacenamiento externo contará con medidas ambientales para los medios y otros recursos almacenados; y tendrá un nivel de seguridad suficiente, que permita proteger los recursos de respaldo contra accesos no autorizados, robo o daño. Los acuerdos/contratos del sitio alterno serán periódicamente analizados, al menos una vez al año, para garantizar que ofrezca seguridad y protección ambiental; a su vez se debe establecer un cronograma para la ejecución del mismo.

Punto de Vista.-

El área de TI ha solventado hasta el momento todos los eventos que ha causado una posible no continuidad del negocio, obteniendo resultados positivos para la empresa, el área de ti con los recursos que cuenta ha solventado todas las

necesidades del área y de la empresa, viéndose limitada siempre por el tema presupuestario.

DS4.5 Pruebas del Plan de Continuidad de TI

Observación.-

Nunca existieron Pruebas del Plan de Continuidad para asegurar que los sistemas de TI puedan ser recuperados de forma efectiva.

Criterio.-

"Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción. Considerar el alcance de las pruebas de recuperación en aplicaciones individuales, en escenarios de pruebas integrados, en pruebas de punta a punta y en pruebas integradas con el proveedor."

Condición.-

- El Plan actual fue realizado de acuerdo a los resultados de un incidente antes presentado.
- Nunca se realizaron pruebas; el plan solo contempla un solo incidente. **(Evidencia: ENT-DS6)**

Causa.-

El Departamento de Tecnología de Información y Comunicaciones, no ha desarrollado políticas y normatividad referente al tema.

Efecto.-

- No existen procedimientos de resistencia y de establecimiento de prioridades en situaciones de recuperación.
- En caso de un siniestro o catástrofe el personal actuaria de forma empírica.

Recomendaciones.-

Las pruebas del plan son esenciales para identificar las deficiencias de planificación y preparación del personal. Y en la fase de pruebas se debe contener actividades como más importantes que requieran comprobación y certeza en su funcionamiento futuro en el cual se probará dentro de un ambiente que simule las condiciones que serían aplicables en una emergencia verdadera.

Punto de Vista.-

El plan de continuidad está probado completamente, con resultados positivos por las emergencias presentadas, considerando que el core del negocio está sobre dos puntos críticos el servidor de base de datos y sobre redes y comunicaciones, que ya fueron probados.

OBJETIVO DE CONTROL DS5 Garantizar la seguridad de los sistemas

DS5.1 Administración de la Seguridad de TI

Observación.-

No se ha definido un plan de seguridad en el que se describan las políticas adoptadas por el COSSFA.

Criterio.-

"Administrar la seguridad de TI al nivel más alto apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.

Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad. Asegurar que el plan esta implementado en las políticas y procedimientos de seguridad junto con las inversiones apropiadas en los servicios, personal, software y hardware. Comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios."

Condición.-

- No se ha implementado un Plan de Seguridad de TI, que contenga las definiciones de los requisitos de seguridad del COSSFA y que permitan a los usuarios desempeñar adecuadamente sus funciones.
- La seguridad institucional se lo administra a través de firewall y software que evite la corrupción de la red.

- No existe evidencia de procedimientos para asegurar acciones oportunas relacionadas con la solicitud, establecimiento, emisión, suspensión y cierre de cuentas de usuario.
- No existe evidencia de procedimientos aprobados formalmente, que indique el propietario de los datos o del sistema que otorga los privilegios de acceso. (Evidencia: ENT-DS7)

Causa.-

Falta de políticas y normatividad relativa al tema.

Efecto.-

- Incremento en la vulnerabilidad de los sistemas de tecnología del COSSFA, que causarían sustracción o daño en la información crítica a nivel de hardware y software.
- Interrupciones en los servicios informáticos, causadas por virus y ataques informáticos.
- Accesos indebidos a información crítica lo cual impide preservar la integridad de los datos.
- Pérdida de confidencialidad de datos y privacidad de clientes y usuarios.

Recomendaciones.-

Se debe establecer políticas y procedimientos, para administrar y monitorear la seguridad en TI, de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos de negocio. Esto incluye: Trasladar información sobre evaluación de riesgos a los planes de seguridad de TI, implementar el plan de

seguridad de TI, actualizar el plan de seguridad de TI para reflejar cambios en la configuración de TI, evaluar el impacto de las solicitudes de cambio en la seguridad de TI, monitorear la implementación del plan de seguridad de TI y alinear los procedimientos de seguridad de TI a otras políticas y procedimientos.

Punto de Vista.-

La seguridad en los sistemas y en la parte de redes y comunicaciones se encuentra garantizada por la creación de usuarios y perfiles para los aplicativos, correo y para internet. Adicionalmente se cuenta con un firewall que cubre posibles ataques de la parte externa de la empresa.

OBJETIVO DE CONTROL DS8 Administrar la Mesa de Servicio y los Incidentes

DS8.1 Mesa de Servicios

Observación.-

No se ha definido un procedimiento adecuado para el reporte y solución de problemas de los usuarios.

Criterio.-

“Establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Deben existir procedimientos de monitoreo y escalamiento basados en los niveles de servicio acordados en los SLA's, que permitan clasificar y priorizar cualquier problema reportado como incidente, solicitud de servicio o solicitud de información. Medir la

satisfacción del usuario final respecto a la calidad de la mesa de servicios y de los servicios de TI."

Condición.-

- Se utilizaba un software aplicativo que ayudaba a la gestión de incidentes reportados por usuarios, este dejo de ser utilizado por falta de personal y tiempo.
- No se mantiene un cronograma de revisiones periódicas para determinar que todos los incidentes fueron solucionados correctamente, en el tiempo oportuno y que no existen pendientes.
- No se realiza mediciones de satisfacción del usuario de Help Desk a pesar de que la política contempla un monitoreo del nivel de atención.
- El procedimiento de reporte y solución de problemas e incidentes no se encuentra correctamente difundido entre los usuarios, razón por la cual los mismos no siguen el procedimiento adecuado.**(Evidencia: OBS-DS8)**

Causa.-

Falta de políticas y normatividad relativa al tema.

Efecto.-

- Si los problemas no son manejados de manera efectiva, la entidad podría desperdiciar recursos en asuntos sin importancia y/o los usuarios bien podrían no utilizar el sistema como se pretende.

- La falta de un registro y control de los problemas e incidentes, puede ocasionar que existan problemas que no se hayan resuelto debidamente y a tiempo.
- El desconocimiento del procedimiento de reporte y solución de problemas e incidentes ocasiona que no todos los problemas e incidentes se reporten de manera adecuada y sean atendidos oportunamente.
- Disminuye la calidad de servicio de TI, en apoyo a los objetivos institucionales.

Recomendaciones.-

- El Gerente de la Unidad de Desarrollo Institucional, establecerá políticas y procedimientos para monitorear tendencias y estadísticas de problemas de manera tal que se pueda aplicar un enfoque proactivo a la resolución de problemas.
- El Gerente de la Unidad de Tecnología de Información y Comunicaciones, pondrá en práctica cronogramas de revisiones periódicas de los incidentes reportados para determinar que todos los incidentes fueron solucionados correctamente, en el tiempo oportuno. Actualizará el procedimiento de reporte y solución de problemas y lo difundirá a los usuarios y personal del COSSFA.

Punto de Vista.-

Se está dando solución a todos los problemas levantados por las aéreas dentro de la empresa y los resultados lo demuestran.

OBJETIVO DE CONTROL DS10 Administrar los problemas

DS10.1 Identificación y Clasificación de Problemas

Observación.-

No existe evidencia de un procedimiento para reportar y clasificar problemas que han sido identificados en el Departamento de Tecnología de Información y Comunicaciones.

Criterio.-

"Implementar procesos para reportar y clasificar problemas que han sido identificados como parte de administración de incidentes. Los pasos involucrados en la clasificación de problemas son similares a los pasos para clasificar incidentes; son determinar la categoría, impacto, urgencia y prioridad. Los problemas deben categorizar se de manera apropiada en grupos o dominios relacionados (por ejemplo, hardware, software de soporte). Estos grupos pueden coincidir con las responsabilidades organizacionales o con la base de usuarios y clientes, y son la base para asignar los problemas al personal de soporte."

Condición.-

- No se encuentra difundido apropiadamente el procedimiento de Soporte Técnico establecido al personal del COSSFA.
- No existe un registro en el que se incluyan los problemas escalados a otras unidades y a proveedores o consultores externos.
- No existen definidas políticas para la realización del monitoreo de la calidad de los servicios prestados por los proveedores y las áreas especializadas al

resolver problemas reportados por los usuarios del COSSFA. **(Evidencia:ENT-DS10)**

Causa.-

Falta de políticas y normatividad relativa al tema.

Efecto.-

- Pérdida de tiempo en las unidades especializadas en atender problemas mínimos.
- Pérdida de dinero al solicitar soporte externo a proveedores cuando este no lo amerita.

Recomendaciones.-

El Gerente del Departamento Estratégico, establecerá e implantará políticas y normativa de escalamiento de problemas, para asegurar que los problemas identificados sean resueltos oportunamente de la manera más eficiente. Estos procedimientos deberán asegurar que las prioridades sean establecidas apropiadamente. Los procedimientos también deberán documentar el proceso de escalamiento para la activación del plan de continuidad de TI.

Punto de Vista.-

Los problemas y soluciones que se han ejecutado dentro del área han sido realizados con un análisis dentro de cada una de las sub áreas aplicando una distribución de donde debe ser atendida y solucionada a pesar de no llevar documentos.

DS10.2 Rastreo y Resolución de Problemas

Observación.-

No existe un proceso para seguimiento de problemas y pistas.

Criterio.-

"El sistema de administración de problemas debe mantener pistas de auditoría adecuadas que permitan rastrear, analizar y determinar la causa raíz de todos los problemas reportados considerando:

- Todos los elementos de configuración asociados
- Problemas e incidentes sobresalientes
- Errores conocidos y sospechados
- Seguimiento de las tendencias de los problemas

Identificar e iniciar soluciones sostenibles indicando la causa raíz, incrementando las solicitudes de cambio por medio del proceso de administración de cambios establecido. En todo el proceso de resolución, la administración de problemas debe obtener reportes regulares de la administración de cambios sobre el progreso en la resolución de problemas o errores. La administración de problemas debe monitorear el continuo impacto de los problemas y errores conocidos en los servicios a los usuarios. En caso que el impacto se vuelva severo, la administración de problemas debe escalar el problema, tal vez refiriéndolo a un comité determinado para incrementar la prioridad de la solicitud del cambio (RFC) o para implementar un cambio urgente, lo que resulte más pertinente. El avance de la resolución de un problema debe ser monitoreado contra los SLA's."

Condición.-

- No existen un procedimiento de manejo de problemas que aseguren la suficiencia del alcance de una auditoría informática para incidentes TI. **(Evidencias:ENT-DS11)**

Causa.-

No existe un sistema de administración de problemas

Efecto.-

Riesgo de repetición de incidentes por falta de seguimiento, que pueden afectar a la continuidad del servicio.

Recomendaciones.-

Se debe establecer políticas y procedimientos para estructurar el sistema de administración de problemas, el que deberá proporcionar adecuadas pistas de auditoría que permitan el seguimiento de un incidente a partir de sus causas. Deberá trabajar estrechamente con la administración de cambios, la administración de disponibilidad y la administración de configuración.

Punto de Vista.-

El área si maneja un proceso de atención a incidentes no se encuentra documentado pero es el que se tiene y se mantiene al momento, se da soporte a nivel nacional.

OBJETIVO DE CONTROL DS12 Administrar el ambiente físico (Instalaciones)

DS12.1 Selección y Diseño del Centro de Datos

Observación.-

No existe evidencia de políticas y procedimientos de seguridad física.

Criterio.-

"Definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia del negocio. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo."

Condición.-

- No existen un plan de mantenimiento a los equipos de seguridad.
- No se ha definido procedimientos de revisión del cumplimiento de los controles de acceso al Centro de Cómputo. **(Evidencia:ENT-DS12)**

Causa.-

Falta de políticas y normatividad relativa al tema.

Efecto.-

- Acceso indebido al Sistema de Información.
- Perdida de equipos, información y daños al Sistema de Información.

Recomendaciones.-

El área de Tecnología de Información y Comunicaciones, debe mejorar medidas apropiadas de seguridad física y medidas de control de acceso para las instalaciones de tecnología de información, incluyendo el uso de dispositivos de información off-site, en conformidad con la política general de seguridad. La seguridad física y los controles de acceso deben abarcar no sólo el área que contenga el hardware del sistema, sino también las ubicaciones del cableado usado para conectar elementos del sistema, servicios de soporte (como la energía eléctrica), medios de respaldo y demás elementos requeridos para la operación del sistema. El acceso deberá restringirse a las personas que hayan sido autorizadas. Cuando los recursos de tecnología de información estén ubicados en áreas públicas, deberán estar debidamente protegidos para impedir o para prevenir pérdidas o daños por robo o por vandalismo.

Punto de Vista.-

El área de ti maneja un proceso no documentado en ciertas sub áreas pero si hace un seguimiento de toda la seguridad que tiene implementado, como cámaras, cctv, firewall, se mantiene una bitácora de accesos donde se manejan los registros de las personas que ingresan.

DS12.2 Medidas de Seguridad Física

Observación.-

No existe un procedimiento de escolta de visitantes al ingreso al centro de Cómputo.

Criterio.-

"Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio. Las medidas deben incluir, pero no limitarse al esquema del perímetro de seguridad, de las zonas de seguridad, la ubicación de equipo crítico y de las áreas de envío y recepción. En particular, mantenga un perfil bajo respecto a la presencia de operaciones críticas de TI. Deben establecerse las responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física."

Condición.-

- No existe evidencia de un procedimiento para ingreso de personal visitante al Departamento de Información y Comunicación, ni un registro en donde se indique el motivo del acceso y la fecha y duración del mismo.
- No se han definido políticas de control referentes a la administración del Centro de Cómputo. **(Evidencia:OBS-DS13)**

Causa.-

Falta de políticas y normatividad relativa al tema.

Efecto.-

Riesgo de sabotaje, daño o robo que puedan producirse en los equipos que se encuentran en el Centro de Cómputo.

Recomendaciones.-

El Gerente de la Unidad de Tecnología de Información y Comunicaciones, establecerá procedimientos apropiados, que aseguren que las personas que no formen parte del grupo de operaciones de la función de servicios de información, sean escoltadas por algún miembro de ese grupo cuando deban entrar a las instalaciones de cómputo. Deberá mantenerse y revisarse regularmente una bitácora de visitantes.

Punto de Vista.-

Se mantiene un registro en cada rack de comunicaciones incluido el centro de computo donde se registran las personas que ingresan, adicionalmente hay una persona que la acompaña dependiendo la actividad.

OBJETIVO DE CONTROL DS13 Administración de Operaciones

DS13.5 Mantenimiento Preventivo del Hardware

Observación.-

No se ha implementado procesos para dar mantenimiento preventivo del hardware de la empresa.

Criterio.-

“Definir e implementar procedimientos para garantizar el mantenimiento oportuno de la infraestructura para reducir la frecuencia y el impacto de las fallas o de la disminución del desempeño.”

Condición.-

- COSSFA cuenta con un cronograma de mantenimiento preventivo de hardware el cual se lo hace anualmente mediante un cronograma de visitas a las agencias, actualmente no se lo realiza. **(Evidencia: ENT-DS14)**

Causa.-

No se ha establecido un plan para mantenimiento preventivo ni correctivo.

Efecto.-

- Falta de un buen servicio al cliente por falta de recursos tecnológicos.
- Pérdidas de clientes por mala atención.
- Pérdidas de tiempo en las labores que ejecuten los funcionarios de la cooperativa.

Recomendaciones.-

Analizar alternativas a fin de agilizar el servicio de mantenimiento a nivel de agencias y buscar oportunidades a través de proveedores externos locales, quienes puedan atender los requerimientos logrando un tiempo adecuado de atención y garantizando el funcionamiento óptimo de la infraestructura.

Punto de Vista.-

El área de ti si realizo un mantenimiento preventivo pero debido al presupuesto que tenemos actualmente se ajustaron fechas en el cronograma, donde se convirtió en un mantenimiento en ciertas ocasiones correctivo.

MONITOREAR Y EVALUAR (ME)

ME1 Monitorear y evaluar el desempeño de TI

ME2 Monitorear y evaluar el control interno

ME3 Garantizar el cumplimiento regulatorio

ME4 Proporcionar gobierno de TI

OBJETIVO DE CONTROL M1 Monitorear y Evaluar el Desempeño de TI

"Una efectiva administración del desempeño de TI requiere un proceso de monitoreo. El proceso incluye la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan motivaciones. El monitoreo se requiere garantizar que las cosas correctas se hagan y que estén de acuerdo con el conjunto de direcciones y políticas."

ME1.4 Evaluación del Desempeño

Observación.-

No se ha definido un proceso que evalúe el desempeño en TI.

Criterio.-

"Comparar de forma periódica el desempeño contra las metas, realizar análisis de la causa raíz e iniciar medidas correctivas para resolver las causas subyacentes."

Condición.-

- No existe evidencia del diseño e implantación de un proceso de monitoreo del desempeño de TI.
- Cumplimiento tardío en un 80% a satisfacción los acuerdos de niveles de servicio.
- No se realiza un reporte un monitoreo de control interno.

- No se tienen datos actualizados de la información relativa a la percepción del cliente de los últimos meses. No se realiza la encuesta trimestral. **(Evidencia: ENT-ME1)**

Causa.-

- No se han asignado las responsabilidades para realizar el monitoreo del desempeño de las actividades de TI.
- Falta de una definición formal y completa de los procesos de TI.
- Poco conocimiento sobre las mejores prácticas para evaluar el desempeño de TI.

Efecto.-

- No tomar acciones pertinentes a la mejora continua por desconocimiento de las causas raíz de los problemas.
- Riesgo del negocio, cualquier falla en los sistemas informáticos impacta directamente el resultado del negocio, especialmente en la atención a los clientes.

Recomendaciones.-

Diseñar e implementar un sistema de monitoreo de los procesos de TI, tomando en cuenta lo siguiente:

- Definición y recolección de datos de monitoreo, que incluya los datos necesarios para los indicadores de apoyo al cumplimiento del plan estratégico de TI, cumplimiento de regulaciones, satisfacción de usuarios internos y externos, desarrollo y entrega del servicio de TI.

- Identificación y registro de acciones correctivas, responsabilidades, plazos y resultados de las acciones comprometidas.
- Evaluar el desempeño de TI en diferentes dimensiones: aspectos financieros, satisfacción del cliente, eficacia de procesos y capacidad futura; y recompensar al manejo de la TI con base en medidas que generalmente incluyen: tiempo de funcionamiento planificado, niveles de servicio, tiempos de alimentación y reacción de la transacción y disponibilidad de aplicación
- Al manejo de la TI le conciernen dos cosas: que produzca valor comercial y que se mitiguen sus riesgos. La primera se lleva a cabo por la alineación estratégica de la TI con la institución. La segunda se realiza al establecer responsabilidades dentro de la COSSFA.

Punto de Vista.-

El área de tecnología no cuenta con herramientas de monitoreo de acuerdo a lo expresado en este objetivo, tenemos evaluaciones internas de desempeño en todos los aspectos, el único proceso o procedimiento que se tiene por escrito es el de talento humano, los demás se realizan pero sin tenerlo documentado.

ME1.5 Reportes al Consejo Directivo y a Ejecutivos

Observación.-

No existe evidencia sobre reportes administrativos para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas.

Criterio.-

“Proporcionar reportes administrativos para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas, específicamente en términos del desempeño del portafolio empresarial de programas de inversión habilitados por TI, niveles de servicio de programas individuales y la contribución de TI a ese desempeño. Los reportes de estatus deben incluir el grado en el que se han alcanzado los objetivos planeados, los entregables obtenidos, las metas de desempeño alcanzadas y los riesgos mitigados. Durante la revisión, se debe identificar cualquier desviación respecto al desempeño esperado y se deben iniciar y reportar las medidas de administración adecuadas.”

Condición.-

- Se presenta un informe sobre por cantidad de requerimientos, tiempo de respuesta críticos, no críticos de manera global de cuando fueron pedido y terminados, desde que la empresa entro en estado crítico.
- No se mantienen reportes de satisfacción de usuarios.
- No se encuentran actualizados y publicados Acuerdos de Niveles de Servicios (tiempos, horarios, etc.)**(Evidencia: ENT-ME2)**

Causa.-

El Departamento de TI no proporciona reportes para la alta gerencia, debido a que se limita al funcionamiento y el reporte contiene actividades ejecutadas, pero no se señala en que forma ayuda al entorno institucional.

Efecto.-

El informe resultante no tendrá bases sólidas referentes a como la organización está en la parte de TI, debido a que los indicadores de monitoreo no se encuentran, y los que se utilizan controlan los procesos de forma superficial.

Recomendaciones.-

Mantener el proceso de revisión gerencial, tomando en cuenta la nueva metodología de monitoreo a seguir por parte del Departamento de TI, e implementarla dentro de este proceso en el.

Además brindar la suficiente confiabilidad y utilidad de los reportes de desempeño para no usuarios, tales como auditores externos. Archivar la información en formato digital e impreso.

Punto de Vista.-

El área de ti emite un informe mensual de todas las actividades más relevantes del área para el apoyo de la empresa en el cumplimiento de los objetivos que se trazan.

OBJETIVO DE CONTROL M1 Monitorear y Evaluar el Desempeño de TI

ME2.1 Monitoreo del Marco de Trabajo de Control Interno

Observación.-

No existen reportes donde se gestione el control interno.

Criterio.-

"Monitorear de forma continua el ambiente de control y el marco de control de TI. Se debe realizar la evaluación usando mejores prácticas de la industria y se debería utilizar benchmarking para mejorar el ambiente y el marco de trabajo de control de TI."

Condición.-

- Se realiza el seguimiento, por cantidad de requerimientos, tiempo de respuesta críticos, no críticos de manera global de cuando fueron pedido y terminados.
- No existe un control y una evaluación de proyectos de TI para verificar cuantos no cumplieron todo lo detallado en el contrato.
- La infraestructura y los recursos disponibles de la TI no son suficientes para lograr los objetivos estratégicos que requiere el COSSFA así como para soportar el crecimiento a corto y mediano plazo, por la falta recursos en equipos, en infraestructura tecnologica y en personal, al momento se adaptó a las necesidades de la empresa, a pesar que si se tiene identificado y diferenciado donde se puede actuar para realizar mejoras. **(Evidencia: ENT-ME3)**

Causa.-

Falta de políticas y normatividad relativa al tema.

Efecto.-

Dificultades ante eventuales necesidades de rendición de cuentas y falta de separación de funciones dentro en el Departamento de TI.

Recomendaciones.-

- Implementar un procedimiento cuyo objetivo sea garantizar la implementación efectiva y eficiente de las recomendaciones dadas por auditorias y exámenes especiales.
- Las recomendaciones y aquellas acciones de mejora que se desprendan de esta auditoría y de otros exámenes realizados se deberán incorporar al Plan Operativo a fin de que se garantice su ejecución.

Punto de Vista.-

El área de tecnología tiene conocimiento de que actividades y que infraestructura aplicar o implementar para mejorar el servicio actual de apoyo a las áreas de cadena de valor fe la empresa pero debido a un limitante de presupuesto no se pueden ejecutar. Con las herramientas actuales y las herramientas que se tiene en el área, se ha implementado buenas alternativas para soporte y apoyo a la empresa.

4.2 Informe Ejecutivo

4.2.1 Antecedentes

El proyecto de Evaluación y Auditoria de los Sistemas de Información del Comisariato de Servicio Social de las Fuerzas Armadas – COSSFA, fue concebido como un estudio minucioso de la realidad actual de la tecnología de información en la que se encuentra la institución y de las posibles recomendaciones para la implantación de controles y mejoramiento de TI; el mismo que fue aprobado por el Señor Presidente Ejecutivo de Holdingdine y

ejecutado a través de la Gerencia de TI de COSSFA como proyecto de tesis de grado.

El objetivo primordial de este proyecto radica en efectuar una Evaluación y Auditoria Informática del Sistema de Información del Comisariato de Servicio Social de las Fuerzas Armadas, mediante la revisión del ambiente de control implementado en los procesos automatizados y en el gerenciamiento de los mismos, utilizando el modelo COBIT, a fin de identificar debilidades y emitir recomendaciones que permitan eliminar o minimizar los riesgos en la Institución.

.

La Evaluación y Auditoria de los Sistemas de Información va dirigido a todos los funcionarios del COSSFA y sus respectivas sedes, que tengan relación con los recursos de tecnología de información como: hardware, software, comunicaciones e infraestructura; tecnología que le permite cubrir las necesidades de los diversos usuarios del comisariato.

4.2.2 Descripción Metodológica

El proyecto de la Evaluación y Auditoria de los Sistemas de Información del Comisariato de Servicio Social de las Fuerzas Armadas fue realizado sobre los cuatro dominios del modelo de COBIT, Planificación y Organización, Adquisición e Implantación, Entrega y Soporte, y Monitoreo y Evaluación; dichos dominios fueron desarrollados

por dos estudiantes como proyecto de tesis de grado, y orientados por los dirigentes del proyecto docentes de la Escuela Politécnica del Ejército.

El desarrollo de la Evaluación y Auditoria de los Sistemas de Información del COSSFA cubrió aspectos de planificación, organización, procesos, ejecución de proyectos, seguridades, equipos, redes, comunicaciones e infraestructura, con el objeto de determinar los riesgos a los que se encuentra sometida la Institución y recomendar procedimientos que permitan minimizar o eliminar riesgos.

Dentro del análisis de los Objetivos de Control de la metodología COBIT se considera la visión objetiva e independiente, punto de vista crítico y sistemático, basado en evidencia, bajo normas y metodologías aprobadas a nivel internacional; que ayudaron en la selección de muestras de las políticas, normas, prácticas, funciones, procesos, procedimientos e informes relacionados con los sistemas de información computarizados, llegando a obtener una opinión profesional e imparcial enfocada en aspectos como: criterios de información y prácticas de controles requeridos para determinar la eficiencia en el uso de los recursos informáticos, validez de la información y efectividad de los controles establecidos.

A más de la aplicación del modelo COBIT se utilizaron herramientas de implementación para la recolección de la información como:

- Entrevistas con el Gerente de TI

- Entrevistas con los encargados de:
    - HelpDesk
    - Administrador de Redes y Comunicaciones
    - Administrador de Aplicativos y Base de Datos
- Reuniones con el Director de Gestión Estratégica.
- Reuniones con el Director de Talento Humano.
- Investigación documental de los procedimientos, actividades, proyectos, registros, pruebas, memorandos, contratos, garantías, etc. Del manejo de hardware, software, comunicaciones, infraestructura y recursos humano del comisariato.

Después de la etapa de recolección de información, se procedió al análisis de la misma que incluye la elaboración de las matrices de riesgo y de investigación de campo por cada objetivo de los cuatro dominios de COBIT, en este caso se va a tratar sobre los objetivos de alto nivel con sus respectivos sub-objetivos.

Finalmente las observaciones encontradas pasan a formar parte del análisis de presentación de resultados, donde las autoridades del COSSFA y los involucrados directos con tecnologías de información recibieron el Informe de Auditoría con las observaciones, criterios, condiciones, causas y efectos hallados en el análisis, además las recomendaciones respectivas para la aplicación en la institución.

4.2.3 Principales Hallazgos

Después de la conclusión de todo el análisis y evaluación de la realidad actual de la tecnología de información en el COSSFA, se han detectado falencias importantes que se detallan a continuación:

- El Dominio Planeación y Organización muestra para cada objetivo lo siguiente:
    - Estratégicamente la Gerencia de TI debe considerar la elaboración de un Plan Estratégico de TI y derivado de este un Portafolio de Planes Tácticos que le permita tener una visión de las actividades tácticas que se deben realizar en el área para de esta manera encontrarse sincronizada con los objetivos de la empresa.
    - En lo que respecta a Arquitectura de la Información se debe concientizar con los altos mandos sobre las tendencias tecnológicas futuras dándole a conocer la ventaja a nivel competitivo que la organización puede asegurar. Mantenerles informados de los proyectos de TI que se pueden implementar para mejorar la operatividad de la organización si se la dota de nuevos y potentes recursos tecnológicos, los mismos que proporcionen tiempos de respuesta rápidos y eficientes.
    - En los procesos relacionados con TI se debe identificar eventos o amenazas que podrían tener impacto en la

continuidad de las operaciones empresariales, y la probabilidad de que ocurran, a través de un análisis detallado de amenazas. Integrar la gestión del riesgo de TI a la gestión del riesgo institucional, mediante la elaboración del plan de seguridad y continuidad del negocio para mitigar riesgos.

- Realizar un análisis e identificar cuáles son los estándares y mejores prácticas de calidad, e implementar los mismos en los procesos claves de TI a través de una comisión que sea la responsable del aseguramiento de la calidad conformada por los miembros de la función de Servicios de información y establecer sistemas de aseguramiento de calidad apropiados.

- El Dominio Adquisición e Implantación muestra para cada objetivo lo siguiente:
  - Se debe realizar un análisis para definir una metodología para la identificación y evaluación de las soluciones de TI, la que estará sujeta a una mejora continua y con flexibilidad para proyectos de pequeña y gran escala.
  - Desarrollar una administración de riesgos TI, en la que se realice: análisis de vulnerabilidades asociadas a los recursos de TI (errores, daño intencional, vandalismo, equivocaciones, ataque, robo, acceso no autorizado, falla de hardware o

software), evaluación de la probabilidad de ocurrencia de las amenazas, diseñar nuevos controles que permitan reducir las debilidades hasta un nivel aceptable de riesgo. Con esta evaluación de riesgos se deben generar controles tanto preventivos como correctivos que permitan mitigar la incidencia del riesgo, esta administración permitirá elaborar un Plan de Contingencia actualizado, basado en el Plan Estratégico del COSSFA.

- La Gerencia de TI debe desarrollar un plan para el mantenimiento preventivo que registre la planeación y evaluación de recursos, reparación de defectos de programa y corrección de fallas después de cumplirse el ciclo de vida definido.
- La Unidad de Logística debe ser la única unidad encargada de realizar todo el proceso de adquisiciones de infraestructura del COSSFA, estas actividades incluyen la convocatoria a proveedores, calificación a los mismos, evaluación y estudios de las ofertas con un técnico designado de la Gerencia de TI.
- Transferir el conocimiento y las habilidades para permitir al personal de soporte técnico y de operaciones que entregue, apoye y mantenga la aplicación y la infraestructura asociada de manera efectiva y eficiente de acuerdo a los niveles de servicio requeridos, incluyendo entrenamiento inicial y

continuo, desarrollo de habilidades, materiales de entrenamiento, manuales de operación, manuales de procedimientos y escenarios de atención al usuario.

- El Dominio Entregar y Dar Soporte muestra para cada objetivo lo siguiente:
    - El Gerente de TI, en cooperación con los propietarios de los procesos del negocio, definirá políticas y normatividad en el que consten los roles, responsabilidades, la metodología a seguir basada en riesgo, las reglas monitoreo y disponibilidad de los recursos críticos, procesamiento alternativos, principios de respaldo y recuperación; y la estructura para documentar el plan de continuidad, así como los procedimientos de aprobación, el plan de continuidad del negocio, proveerá a la organización la habilidad para continuar operando los procesos críticos definidos, a un nivel menor al normal aceptado, en ocasiones en las que se produzcan eventos que ocasionen la paralización de los servicios informáticos.
    - El Gerente de TI debe establecer políticas y procedimientos, para administrar y monitorear la seguridad en TI, de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos de negocio. Esto incluye: Trasladar información sobre evaluación de riesgos a los planes de

seguridad de TI, implementar el plan de seguridad de TI, actualizar el plan de seguridad de TI para reflejar cambios en la configuración de TI, evaluar el impacto de las solicitudes de cambio en la seguridad de TI, monitorear la implementación del plan de seguridad de TI y alinear los procedimientos de seguridad de TI a otras políticas y procedimientos.

- El Dominio Monitoreo y Evaluación muestra para cada objetivo lo siguiente:
    - Se recomienda diseñar e implementar un sistema de monitoreo de los procesos de TI, tomando en cuenta lo siguiente:
    - Definición y recolección de datos de monitoreo, que incluya los datos necesarios para los indicadores de apoyo al cumplimiento del plan estratégico de TI, cumplimiento de regulaciones, satisfacción de usuarios internos y externos, desarrollo y entrega del servicio de TI.
    - Identificación y registro de acciones correctivas, responsabilidades, plazos y resultados de las acciones comprometidas.
    - Evaluar el desempeño de TI en diferentes dimensiones: satisfacción del cliente, eficacia de procesos y capacidad

futura; y recompensar al manejo de TI con base en medidas que generalmente incluyen: tiempo de funcionamiento planificado, niveles de servicio, tiempos de alimentación y reacción de la transacción y disponibilidad de aplicación

- Al manejo de TI le conciernen dos cosas: que produzca valor comercial y que se mitiguen sus riesgos. La primera se lleva a cabo por la alineación estratégica de TI con la institución. La segunda se realiza al establecer responsabilidades dentro del comisariato.

- Poner en ejecución un procedimiento cuyo objetivo sea garantizar la implementación efectiva y eficiente de las recomendaciones dadas por Auditorías y exámenes especiales.

Las recomendaciones y aquellas acciones de mejora que se desprendan de esta auditoría y de otros exámenes realizados se deberán incorporar al Plan Operativo a fin de que se garantice su ejecución.

4.2.4 Conclusiones

- Para esta evaluación se realizó la implementación de COBIT como marco de referencia para reforzar las actividades del COSSFA, y encontrar en los recursos de TI el sustento para el éxito de todas sus transacciones.

- La detección de los riesgos más críticos a los que se expone COSSFA, permitió detectar las vulnerabilidades en las actividades que gestiona y administra la Gerencia de TI, lo que permitió emitir recomendaciones para disminuir o evitar la afectación de estas en los principales procesos de la unidad de TI.
- La causa principal que provoca las condiciones encontradas, es la falta de un Plan Estratégico Informático y el desconocimiento de las mejores prácticas de control interno y auditoría de los sistemas de información por parte de las autoridades del COSSFA y el personal de la Gerencia de Tecnologías de Información.
- El COSSFA no cuenta con presupuesto necesario para realizar e implementar proyectos de innovación que le permitan estar a la par de otras instituciones con las mismas características de negocio; lo que le resta nivel de competitividad frente a otras instituciones.

4.2.5 Recomendaciones

- De acuerdo con lo planteado y el proyecto realizado, es responsabilidad de la entidad aplicar y poner en marcha las recomendaciones emitidas de la Auditoría Informática, llevando a cabo esto de acuerdo a su capacidad y crecimiento.

CAPÍTULO 5

5 CONCLUSIONES Y RECOMENDACIONES

Al culminar el proyecto de la evaluación técnica e informática de los sistemas tecnológicos de información del Comisariato de Servicio Social de la Fuerzas Armadas, se ha cumplido con los objetivos propuestos en el presente trabajo, por lo tanto se exponen a continuación las siguientes conclusiones y recomendaciones en torno a la realización del proyecto.

5.1 Conclusiones

- Para el desarrollo de una Evaluación Técnica Informática de los Sistemas de Información es de principal importancia contar con la guía de un marco de referencia. Para este proyecto se ha escogido el modelo COBIT, el cual el cual a través de sus 4 dominios ofrece una serie de objetivos de control que permiten evaluar eficientemente el ambiente de control de una entidad, garantizando que TI está alineada con el negocio y que los riesgos de TI se administren apropiadamente.

- Al alinear la Normativa respecto a Tecnologías de la Información y los objetivos de control propuestos por COBIT se logró identificar y valorar los riesgos dentro de la entidad para tomar las medidas pertinentes y minimizar la materialización de los riesgos identificados.

- Durante el análisis y evaluación del ambiente de control en la entidad aplicando los dominios propuestos por COBIT se logro identificar debilidades obteniendo observaciones y recomendaciones para ser emitidas en el informe final, para llevar a cabo el proceso de la Auditoría es de suma importancia contar con el compromiso y apertura a la Evaluación Técnica de los sistemas de información; de los principales involucrados como son las Autoridades superiores del COSSFA, el personal de la Gerencia de TI y el Departamento de Auditoría Interna.

- La Auditoría de TI en el COSSFA propone mejoras a los controles existentes en la misma, pues sabiendo que si los controles facilitan la rendición de cuentas mediante la evidencia; al mejorar los controles que están fallando se logrará mitigar los riesgos. La Administración debe identificarse y conocer plenamente los controles.

5.2 Recomendaciones

- Se debe realizar una coordinación adecuada con las demás unidades que conforman el COSSFA, para de esta manera concentrar esfuerzos y llegar a alcanzar los objetivos eficazmente.
- Establecer un plan para la ejecución de las recomendaciones especificadas en el Informe Detallado de la Evaluación Técnica Informática.

- Extender una evaluación informática a todas las sucursales o sedes que conforman el COSSFA, para de esta manera concentrar esfuerzos y llegar a alcanzar los objetivos eficazmente.

ESPACIO EN BLANCO INTENCIONAL

REFERENCIA BIBLIOGRÁFICA

http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-COBIT-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2,7.pdf

http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

http://www.slideshare.net/fsantiago/breve-introduccin-a-COBIT-presentation

http://www.slideshare.net/juliosantizo/introduccin-COBIT

http://es.scribd.com/doc/36672698/1-Introduccion-a-COBIT

http://es.scribd.com/doc/3410099/COSO-v-COBIT-v-ITIL

http://www.marblestation.com/?p=645

http://www.iteraprocess.com/index.php?option=com_content&task=view&id=16&Itemid=39&limit=1&limitstart=0

http://www.monografias.com/trabajos38/COBIT/COBIT2.shtml

http://www.slideshare.net/bemaguali/procesos-COBIT-4

http://es.scribd.com/doc/7823936/COBIT-4-Resumen

http://www.network-sec.com/gobierno-TI/Auditoría-COBIT

http://www.mitecnologico.com/Main/PlanesTacticos

http://www.slideshare.net/jcfdezmxestra/el-concepto-de-planeacin-estratgica

http://gtecnol.tripod.com/plantec1.htm

http://www.unap.cl/~setcheve/ati/DeterminacindelaDireccinTecnolgica.html

http://www.cop.es/colegiados/m-00451/tomadeciones.htm

http://finanbolsa.com/2009/08/13/el-planeamiento-en-la-toma-de-decisiones/

http://es.scribd.com/doc/52704273/COBIT-1-PLANEAR-ORGANIZAR

http://www.kit.com.ar/boletines-a.php?id=0000037

http://www.ccee.edu.uy/ensenian/catcomp/material/riesgo.pdf

http://www.cop.es/colegiados/m-00451/tomadeciones.htm

http://www.slideshare.net/nestorjgp/norma-27000

http://es.scribd.com/doc/6282873/Iso-27000

http://es.scribd.com/doc/11467531/Norma-ISO-27000

http://blogconsultorasur.wordpress.com/2011/09/06/que-es-coso/

http://www.monografias.com/trabajos12/coso/coso2.shtml#coso

http://www.slideshare.net/nestorjgp/norma-27000

http://es.scribd.com/doc/6282873/Iso-27000

http://es.scribd.com/doc/11467531/Norma-ISO-27000

http://www.criptored.upm.es/cibsi/cibsi2005/presentaciones/sesion10/Modelo_de_madurez_SI.pdf

http://helkyncoello.files.wordpress.com/2009/05/curso-de-gobierno-de-ti-modulo-4.pdf

http://www.network-sec.com/glosario/CSF

http://cs.uns.edu.ar/~ece/Auditoría/COBIT4.1spanish.pdf

http://www.monografias.com/trabajos14/Auditoríasistemas/Auditoríasistemas.shtml

http://www.luishaba.es/tacticavsestrategia.html

BIOGRAFÍA

Nombres y Apellidos: Sara Natali Alvear Montesdeoca.

Lugar y Fecha de Nacimiento: Quito, 04 de marzo de 1987.

Formación Académica

Educación Primaria: De Primer a Sexto Grado.

Centro de Estudios: Oscar Efrén Reyes. Año: 1993 – 1999.

Educación Secundaria: De Primer a Sexto Curso con especialidad Físico Matemáticas.

Centro de Estudios: Manuela Cañizares - Quito. Año: 1999 – 2005.

Educación Superior: Carrera de Ingeniería en Sistemas e Informática.

Centro de Estudios: ESPE - Sangolquí. Año: 2005 – 2013.

Títulos Obtenidos

CISCO – CCNA1 Exploration: Network Fundamentals: ESPE.

Semanas: 6. **Año:** 2009.

CISCO – CCNA2 Exploration: Routing Protocols and Concepts: ESPE.

Semanas: 6. **Año:** 2009.

Suficiencia en el Idioma Inglés: En la ESPE - Departamento de Lenguas.

Niveles: 8 **Año:** 2012.

BIOGRAFÍA

Nombres y Apellidos: Eveline Alina Estrella Zambrano.

Lugar y Fecha de Nacimiento: Guayaquil, 05 de noviembre de 1985.

Formación Académica

Educación Primaria: De Primer a Sexto Grado.

Centro de Estudios: Escuela Particular Alvernia. Año: 1993 – 1999.

Educación Secundaria: De Primer a Sexto Curso con especialidad Físico Matemáticas.

Centro de Estudios: La Presentación. Año: 1999 – 2004.

Educación Superior: Carrera de Ingeniería en Sistemas e Informática.

Centro de Estudios: ESPE - Sangolquí. Año: 2004 – 2013.

Títulos Obtenidos

CISCO – CCNA1 Exploration: Network Fundamentals: ESPE.

Semanas: 6. **Año:** 2009.

CISCO – CCNA2 Exploration: Routing Protocols and Concepts: ESPE.

Semanas: 6. **Año:** 2010.

CISCO – CCNA3 Exploration: LAN Switching and Wireless: ESPE.

Semanas: 6. **Año:** 2011.

CISCO – CCNA4 Exploration: LAN Accessing the WAN: ESPE.

Semanas: 6. **Año:** 2011.

Suficiencia en el Idioma Inglés: En la ESPE - Departamento de Lenguas.

Niveles: 8 **Año:** 2008.

Suficiencia en el Idioma Francés: En Alianza Francesa Quito.

Niveles: 4 **Año:** 2011.

HOJA DE LEGALIZACIÓN DE FIRMAS

ELABORADA POR

_____	_____
Sara Natali Alvear Montesdeoca.	Eveline Alina Estrella Zambrano.

DIRECTOR DE LA CARRERA

_____

Ing. Mauricio Campaña

Lugar y fecha: Sangolquí, 24 de enero de 2013