AUDITORIA A LA INFRAESTRUCTURA TECNOLOGICA EN LA EMPRESA TEXCOL LTDA. CON SEDE EN LA CIUDAD DE PASTO

RONALD DARIO CERON ACOSTA
ALEX ALBEIRO URBANO

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2016

AUDITORIA A LA INFRAESTRUCTURA TECNOLOGICA EN LA EMPRESA TEXCOL LTDA CON SEDE EN LA CIUDAD DE PASTO

RONALD DARIO CERON ACOSTA
ALEX ALBEIRO URBANO

Trabajo de grado presentado como requisito parcial para optar al título de Ingeniero de Sistemas

Director
ING. MANUEL BOLAÑOS GONZALEZ

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2016

NOTA DE RESPONSABILIDAD

Las ideas y conclusiones aportadas en este Trabajo de Grado son responsabilidad de los autores.
Artículo 1 del Acuerdo No. 324 de octubre 11 de 1966, emanado del honorable Consejo Directivo de la Universidad de Nariño.

La Universidad de Nariño no se hace responsable de las opiniones o resultados obtenidos en el presente trabajo y para su publicación prima las normas sobre el derecho de autor.
Artículo 13 del Acuerdo No. 005 de 2010 emanado del honorable Consejo Académico.

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

Jurado

_____

Jurado

San Juan de Pasto, febrero 2016

DEDICATORIA

Porque la gloria y la honra es para Dios, dedicamos este escalón de nuestras vidas a su Santo Nombre por darnos la oportunidad de haber recorrido este camino universitario y brindarle a nuestras vidas sabiduría, fortaleza alrededor de muchas personas que hicieron parte de este viaje compañeros, maestros, amigos.

A nuestros padres y familiares cercanos, que nos brindaron su apoyo incondicional y confianza, para seguir por este camino hasta llegar a un feliz término de convertirnos en profesionales.

AGRADECIMIENTOS

A Dios Padre en el nombre de Jesús por ser escudo alrededor de mí, fortaleza mía y mi libertador.

A nuestros padres y familiares que nos apoyaron para cumplir con nuestro sueño de ser profesionales.

A todo el grupo de ingeniero por orientarnos, brindarnos sus conocimientos, por su apoyo y compromiso en el desarrollo de este diplomado.

Al ingeniero Manuel Bolaños González, por su apoyo, asesoramiento y compromiso con el desarrollo de este trabajo de grado.

Al ingeniero Mauricio León, Gerente TEXCOL LTDA por permitirnos aplicar y ampliar nuestros conocimientos en esta reconocida empresa y brindarnos su confianza y apoyo.

A todos nuestros maestros y amigos por su apoyo, por brindarnos buenos momentos de calidez personal, de compañerismo, de aprendizaje, de crecimiento personal que marcaron nuestras vidas para bien nuestro y de la sociedad, mil gracias.

Dios los bendiga, los llene de su amor incondicional y su misericordia nueva cada día.

ALEX ALBEIRO URBANO

RONALD DARIO CERON

RESUMEN

El presente trabajo realiza un análisis a la infraestructura tecnológica por intermedió de una auditoría exhaustiva a la empresa Texcol Ltda, con el objetivo principal de encontrar fallos y fortalezas en las instalaciones, con el fin de mejorar el funcionamiento de la empresa generando calidad y eficiencia de comunicación entre las diferentes dependencias que pertenecen a la organización.

En los 15 años que la empresa se encuentra en funcionamiento y después de la implementación de la infraestructura tecnológica en ningún momento de su trayectoria se ha realizado una auditoría informática, encontrando la importancia de desarrollar este trabajo en la empresa de forma prioritaria para salvaguardar el activo más importante que hoy en día poseen las empresas como es el activo de la información generando planes de mejoramiento y planes de contingencia.

El trabajo de auditoría se basó en el estándar COBIT (Objetivos de Control para Información y Tecnologías Relacionadas) que brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, presentando las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos, están enfocadas fuertemente en el control y menos en la ejecución.

ABSTRACT

This paper analyzes, technological infrastructure through a comprehensive audit of the company Texcol Ltda, with the main objective of finding faults and strengths in facilities, in order to improve the functioning of the company generating quality and efficiency of communication between the different units belonging to the organization.

In the 15 years that the company is operating and after implementation of the technological infrastructure at no time in his career has made computer audit, finding the importance of developing this work in the company imminently to safeguard the asset more important that today have companies such as asset information generating improvement plans and contingency plans.

The audit work was based on standard COBIT (Control Objectives for Information and related Technology) that provide good practice through a framework of domains and processes, presenting activities in a manageable and logical structure. COBIT best practices represent the consensus of experts. They are strongly focused on control and less on execution.

TABLA DE CONTENIDO

ANEXOS

LISTA DE FIGURAS

INTRODUCCIÓN

La información en la actualidad juega un papel muy importante en el desarrollo de las empresas y nuestra sociedad, por lo tanto, los desarrolladores de tecnología se han visto en la necesidad de aumentar la velocidad de procesamiento como en la capacidad de almacenamiento de esta, siendo indispensable tener comunicación de buena calidad entre diferentes aéreas y secciones donde se comparten recursos; para la aplicación de una auditoría en la empresa Texcol Ltda. Los problemas de comunicación con falencias viene siendo recurrentes por lo que es indispensable realizar auditoría con el fin de encontrar sus fallos y posibles soluciones, la mejor forma es evaluar la eficiencia y eficacia con que se está operando en la infraestructura física y tecnológica para que por medio de hallazgos se permitan corregir errores existentes y prever de posibles daños a futuro, para que los procesos en la empresa no se vean afectadas por cese de actividades.

IDENTIFICACION DEL PROBLEMA

TITULO DEL PROYECTO

AUDITORIA A LA INFRAESTRUCTURA TECNOLOGICA EN LA EMPRESA TEXCOL LTDA CON SEDE EN SAN JUAN DE PASTO

LINEA DE INVESTIGACION

Este proyecto corresponde a la línea de investigación auditoria en redes.

DESCRIPCION DEL PROBLEMA

Planteamiento del problema: Texcol Ltda., es una empresa que se enfoca al desarrollo de infraestructura en las diferentes ciudades de los departamentos de Nariño y Putumayo aportando con todos los materiales necesarios para desarrollo de vivienda así como forjadora en vías, puentes, túneles, teniendo gran cantidad de clientes en el sector público como privado, contando con proveedores en el interior y exterior del país, por lo cual es de suma importancia hacer una auditoria a la infraestructura física y tecnológica para que la comunicación y almacenamiento de información entre las diferentes áreas de la empresa se realice de forma eficiente y eficaz garantizando veracidad e integridad.

OBJETIVOS

Objetivo general

Aplicar auditoria informática a la infraestructura tecnológica de la empresa Texcol Ltda. Con el fin de identificar fallos, riesgos y amenazas para minimizar el impacto y probabilidad de ocurrencia.

Objetivos específicos

- Identificar el estado actual de la infraestructura del cableado en parte lógica y física de la red de datos, en la empresa Texcol Ltda.

- Identificar el estado actual de la planta tecnológica existente en Texcol Ltda. necesario para el funcionamiento de la red computacional existente en la empresa.
- Definir los riesgos, vulnerabilidades y amenazas existentes en cuanto al mal manejo en la parte lógica y física de la red de datos de la empresa Texcol Ltda.
- Realizar el proceso de análisis y evaluación de riesgos que permitan valorar la probabilidad e impacto que causaría cada uno de los riesgos generando la matriz respectiva.
- Ejecutar las pruebas necesarias que permitan evidenciar las vulnerabilidades, riesgos y amenazas existentes en cuanto a deficiencias en funcionamiento en la parte lógica y física de la red de datos en Texcol Ltda.
- Presentar los resultados de las evaluaciones de la auditoria en el informe final, y elaborar el plan de mejora que será sustentado y entregado a la empresa Texcol Ltda.

JUSTIFICACION

Texcol Ltda. Siendo una empresa que tiene una trayectoria de funcionamiento en la ciudad de Pasto por 15 años ayudando y asesorando en el desarrollo del departamento de Nariño y Putumayo es importante recalcar que a la red de datos existente que actualmente está en funcionamiento en ningún momento se le ha realizado auditoría ni a la parte física, ni a la parte tecnológica, únicamente a la parte financiera.

La ejecución de la auditoría en la empresa Texcol Ltda., se evidencia como necesaria con el fin de mejorar la administración de la red evitando fallos continuos al momento de ejecutar procesos que utilicen la red y trasmisión de datos con el propósito de generar un plan de mejoramiento, plan de contingencia.

En caso de cualquier eventualidad que conlleven a evitar retrasos en el desarrollo de actividades

ALCANCE Y DELIMITACION.

La auditoría se llevó a cabo con el propósito de analizar y evaluar el cumplimiento de las normas de instalación del cableado estructurado según el estándar Cobit, para determinar si este cumple sus funciones de manera eficiente y eficaz, en la empresa Texcol Ltda.

1 MARCO TEORICO

1.1 ANTECEDENTES

A finales del siglo pasado la auditoría se creó únicamente para el sector financiero generando la auditoría contable pero poco a poco se fue incluyendo a la auditoría en diferentes procesos y actividades de las empresas e instituciones en general con el fin de mejorar su eficiencia, eficacia , seguridad , calidad, rentabilidad

La auditoría de los sistemas de información ha surgido cuando las empresas e instituciones han tomado conciencia de que los datos que adquieren, conservan, procesan y emiten, es vital para su propia supervivencia diaria y proyección de eficiencia.

Por tanto, han elevado a la categoría de sistemas críticos prácticamente todos los sistemas internos que manejan información en uno solo, denominado sistema de información. En consecuencia, por su naturaleza crítica el enfoque de auditoría debe anotar una perspectiva que se adecue absolutamente a estos sistemas, sea mediante la transformación de métodos, técnicas y procedimientos de la auditoria tradicional.

Con la introducción de nuevas tecnologías, pronto se detectaron las limitaciones de los métodos tradicionales para realizar la auditoria de sistemas. En su afán de maximizar la eficiencia de los procesos de auditorías, surgen nuevos modelos que se adecuan a las crecientes necesidades del sector de las tecnologías de la información, entre ellos se tienen:

Directrices gerenciales de COBIT, desarrollado por la *Information Systems Audit Control Associatio*n (ISACA):

Las Directrices Gerenciales son un marco internacional de referencias que abordan las mejores prácticas de auditoría y control de sistemas de información. Permiten que la gerencia incluya, comprenda y controle los riesgos relacionados

con la tecnología de información y establezca el enlace entre los procesos de administración, aspectos técnicos, la necesidad de controles y los riesgos asociados.

Este modelo está basado en el concepto de errores que establece responsabilidades relacionadas con la seguridad y los controles correspondientes. Dichos roles están clasificados con base en siete grupos: administración general, gerentes de sistemas, dueños, agentes, usuarios de sistemas de información, así como proveedores de servicios, desarrollo y operaciones de servicios y soporte de sistemas. Además, hace distinción entre los conceptos de autoridad, responsabilidad y respecto a control y riesgo previo al establecimiento del control, en términos de objetivos, estándares y técnicas mínimas a considerar.

Este servicio pretende incrementar la confianza de alta gerencia, clientes y socios, con respecto a la confiabilidad en los sistemas por una empresa o actividad en particular. Este modelo incluye elementos, como: infraestructura, software de cualquier naturaleza, personal especializado y usuarios, procesos manuales y automatizados, y datos. El modelo persigue determinar si el sistema de información es confiable, (i.e. si un sistema funciona sin errores significativos, o fallas durante un periodo de prueba determinado bajo un ambiente dado).

Modelo de evaluación de capacidades de software (CMM), desarrollado por el instituto de ingenieros de software (SEI):

Este modelo hace posible evaluar las capacidades o habilidades para ejecutar, de una organización con respecto al desarrollo y mantenimiento de sistemas de información. Consiste en dieciocho sectores clave, agrupados alrededor de cinco niveles de madurez. Se puede considerar que CMM es la base de los principios de evaluación recomendados por COBIT, así como para algunos de los procesos de administración de COBIT.

Si se revisan los antecedentes de proyectos relacionados auditoría de sistemas en la Universidad de Nariño, se encuentran:

- Auditoria a la infraestructura física de la red de datos de la sede principal y verificación del cumplimiento de las normas de gobierno en línea en la página del centro hospital divino niño, realizado por: Luis Alberto Reynel Araujo.
- Técnicas de auditoria de sistemas aplicadas al proceso de contratación y páginas web en entidades oficiales del departamento de Nariño, realizado por: Luis Carlos Chávez.

1.2 ASPECTOS GENERALES SOBRE AUDITORIA[1]

La auditoría puede definirse como un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados, cuyo fin consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como establecer si dichos informes se han elaborado observando los principios establecidos para el caso.

Por otra parte, la auditoría constituye una herramienta de control y supervisión que contribuye a la creación de una cultura de la disciplina de la organización y permite descubrir fallas en las estructuras o vulnerabilidades existentes en la organización.

La auditoría como función de control debe ser la herramienta a utilizar para ayudar a los funcionarios que tienen responsabilidad administrativa, técnica y operacional a que no incurran en falta. Y es por ello que aquí el control debe ser creativo, inteligente, y constructivo de asesoramiento oportuno a todas las direcciones o gerencias a fin de que la toma de decisiones sea acertada, segura y se logren los objetivos, con la máxima eficiencia.

[1] Piattini, Mario G y del peso, Emilio 2000. “Auditoria Informática: un enfoque práctico”computec RAMA. Madrid, España, Pag 4.

La responsabilidad de un procedimiento de auditoría debe ir más allá de la búsqueda de problemas y de responsables, la visión de la auditoría debe dar la visión de la empresa en su conjunto[2].

1.3 AUDITORIA EN INFORMATICA

La auditoría en informática se desarrolla en función de normas, procedimientos y técnicas definidas por institutos establecidos a nivel nacional e internacional, con unos aspectos básicos se define así:

Fig. 1: fases de auditoría

a. Un proceso formal ejecutado por especialistas del área de auditoria y de informática, se orienta a la verificación y aseguramiento para que las políticas y procedimientos en la organización se realicen de una manera oportuna y eficiente.
b. Las actividades ejecutadas por profesionales del área de informática y de auditoría encaminadas a evaluar el grado de cumplimiento de políticas, controles y procedimientos correspondientes al uso de los recursos de informática por el personal de la empresa, dicha evaluación deberá ser la pauta para la entrega del informe de auditoría, el cual debe contener las observaciones, recomendaciones y áreas de oportunidad para el

[2] http://www.gestiopolis.com/recursos/documentos/fulldocs/fin/auditcontxactual.htm.

mejoramiento y optimización permanente de la tecnología de informática en el negocio.

c. El conjunto de acciones que realiza el personal especializado en las áreas de auditoría y de informática para el aseguramiento continuo de los recursos de informática operen en un ambiente de seguridad y control eficiente con la finalidad de proporcionar a la alta dirección que la información que circula por el área se maneja con los conceptos básicos de integridad, totalidad, exactitud confiabilidad.
d. Proceso metodológico que tiene el propósito principal de evaluar los recursos (humanos, financieros, materiales, tecnológicos, físicos, etc) relacionados con la función de informática para garantizar al negocio que dicho conjunto opere con un criterio de integración y desempeño de niveles altamente satisfactorios para que a su vez apoyen la productividad y rentabilidad de la organización.

1.3.1 Auditoría interna: "es una actividad independiente que realiza la empresa o la entidad y que está encaminada a la revisión de las operaciones contables además de la evaluación y medición de la eficacia de otros controles, con la finalidad de prestar un servicio a la dirección"[3].

Se aplica mejor en empresas medianas que tienden a aumentar en volumen, extensión geográfica y complejidad y se hace imposible el control directo de las operaciones por parte del director.

El objetivo principal es ayudar a la dirección en el cumplimiento de sus funciones y responsabilidades, proporcionándole un análisis objetivo, evaluaciones y recomendaciones pertinentes sobre las operaciones examinadas.

[3] Instituto de Auditores Internos de Estados Unidos.

Otros objetivos que se busca concretar a través de la auditoría interna son: realizar investigaciones especiales solicitadas por la dirección, preparar informes de auditoría acerca de las irregularidades que pudiesen encontrarse como resultado de las investigaciones, expresando igualmente las recomendaciones que se juzguen adecuadas, vigilar el cumplimiento de la recomendaciones contenidas en los informes emitidos con anterioridad.

La auditoría interna posee varias ventajas: facilita una ayuda primordial a la dirección al evaluar de forma relativamente independiente los sistemas de organización y de administración, facilita una evaluación global y objetiva de los problemas de la empresa que generalmente suelen ser interpretados de una manera parcial por los departamentos afectados, pone a disposición de la dirección un profundo conocimiento de las operaciones de la empresa, proporcionado por el trabajo de verificación de los datos contables y financieros, contribuye eficazmente a evitar las actividades rutinarias que generalmente se desarrollan en las grandes empresas, favorece la protección de los intereses y bienes de la empresa frente a terceros.

1.3.2 Auditoria externa: se puede definir como los métodos empleados por una firma externa de profesionales para averiguar la exactitud del contenido de los estados financieros presentados por una empresa. Se trata de dar carácter público, mediante la revisión, a unos estados financieros que en principio eran privados.

Los objetivos de la auditoría externa son: proporcionar a la dirección y a los propietarios de la empresa unos estados financieros certificados por una autoridad independiente e imparcial, proporcionar asesoramiento a la gerencia y a los responsables de las distintas áreas de la empresa en materia de sistemas contables y financieros, procedimientos de organización y otras numerosas fases de la operatoria de una empresa, suministrar información objetiva que sirva de base a las entidades de información y clasificación crediticia, servir de punto de

partida en las negociaciones para la compraventa de las acciones de una empresa, reducir y controlar riesgos accidentales, fraudes y otras actuaciones anormales, liberar implícitamente a la gerencia de sus responsabilidades de gestión.

1.3.3 Diferencias entre auditoría interna y externa

- En la auditoría interna existe un vínculo laboral entre el auditor y la empresa, mientras que en la auditoría externa la relación es de tipo civil.
- En la auditoría interna el diagnóstico del auditor, está destinado para la empresa; en el caso de la auditoría externa este dictamen se destina generalmente para terceras personas o sea ajena a la empresa.
- La auditoría interna está inhabilitada para dar fe pública, debido a su vinculación contractual laboral, mientras la auditoría externa tiene la facultad legal de dar fe pública.

1.3.4 Principios generales de la auditoría externa

- **Exposición:** los estados financieros deben recoger por completo y con claridad todas las transacciones de la empresa.
- **Uniformidad:** la base utilizada en la preparación de los estados financieros de un ejercicio no debe experimentar ninguna variación con respecto al ejercicio precedente.
- **Importancia o materialidad**: este es el criterio que debe presidir el trabajo del auditor es la importancia económica o materialidad de las partidas.
- **Moderación:** de dos o más posibilidades igualmente validas se debe escoger siempre la que dé los resultados más desfavorables.

1.3.5 Normas de trabajo de la auditoría externa: hacen referencia a la preparación y ejecución del trabajo a realizar por el auditor, regulan el conjunto de técnicas de investigación e inspección aplicables a los hechos relativos a los documentos contables sujetos a examen, mediante los cuales el auditor fundamenta su opinión responsable e independiente.

- Programación adecuada.
- Supervisión adecuada.
- Análisis del control interno para fijar el alcance de la pruebas.
- Opinión basada en un material y un trabajo razonablemente suficiente.

1.4 EL AUDITOR

El auditor se refiere a la persona que asume la responsabilidad de realizar un trabajo de este tipo, en todo caso el auditor debe poseer ciertas cualidades para afrontar un trabajo como este:

- Deberá dominar las técnicas y metodologías del proceso auditor.
- Debe ser abierto en sus relaciones personales y que sepa dialogar.
- Debe poseer diversas actitudes como la independencia, la objetividad, la creatividad, el espíritu crítico, la diplomacia, etc.
- El auditor debe mantener un cierto grado de independencia en los asuntos que se encuentra evaluando.
- El auditor tiene la obligación de realizar con esmero y cuidado el dictamen o informe para el que fue contratado.
- Debe poseer una actitud positiva frente a la entidad evaluada.
- Debe tener estabilidad emocional frente la entidad.

- Es su obligación la de respetar las ideas de los demás.
- Debe tener capacidad para la negociación.
- Sera discreto y respetuoso con la información de la empresa.
- Su comportamiento debe ceñirse a la ética profesional.

Dadas estas características el auditor responsablemente deberá cumplir con las siguientes funciones:

- Estudiar la normatividad, misión, objetivos, políticas, estrategias, planes y programas de trabajo.
- Desarrollar el programa de trabajo de una auditoria.
- Definir los objetivos, alcance y metodología para instrumentar una auditoria
- Captar la información necesaria para evaluar la funcionalidad y efectividad de los procesos, funciones y sistemas utilizados.
- Recabar y revisar estadísticas sobre volúmenes y cargas de trabajo.
- Diagnosticar sobre los métodos de operación y los sistemas de información.
- Proponer los sistemas administrativos y/o las modificaciones que permitan elevar la efectividad de la organización.
- Analizar la estructura y funcionamiento de la organización en todos sus ámbitos y niveles.
- Revisar el flujo de datos y formas.
- Considerar las variables ambientales y económicas que inciden en el funcionamiento de la organización.
- Analizar la distribución del espacio y el empleo de equipos de oficina.
- Evaluar los registros contables e información financiera.
- Mantener el nivel de actuación a través de una interacción y revisión continua de avances.
- Proponer los elementos de tecnología de punta requeridos para impulsar el cambio organizacional.

1.5 AUDITORIA DE SISTEMAS COMO OBJETO DE ESTUDIO

Desde que la informática se enfocó hacia el apoyo de la sistematización en las áreas del negocio, se empezaron a implantar aplicaciones administrativas como contabilidad, nómina, etc., lo que originó el proceso conocido como auditoria a sistemas de información.

La auditoría de sistemas, es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. También permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes.

Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos. Los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

La auditoría de sistemas permite además verificar que la información desde su entrada, procedimientos, controles, almacenamientos y salidas, sea integra y verificable y por tanto permita el apoyo a la toma de decisiones dentro de una organización.

Dentro de este procedimiento es necesario evaluar los mecanismos de control implantados en una organización, determinando así, si son adecuados y cumplen

con los objetivos o estrategias, de esta manera, es posible proponer cambios que se deberían realizar para el mejoramiento de los mismos. Estos mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

1.5.1 Alcance de la auditoria de sistemas: el alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoría de sistemas, se complementa con los objetivos de ésta. El alcance ha de figurar expresamente en el Informe final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas. La indefinición de los alcances de la auditoria compromete el éxito o el fracaso de la misma. Así mismo, las personas que realizan la auditoría han de conocer con la mayor exactitud posible los objetivos a los que su tarea debe llegar.

1.6 METODOLOGÍAS DE AUDITORIA DE SISTEMAS

La auditoría de sistemas en el ámbito empresarial, ha sido de gran importancia, puesto que con ella se pretende gestionar la información y sirve como apoyo a la toma de decisiones. Además, se busca disponer de un sistema de información que sea eficiente y eficaz para obtener la mayor productividad y calidad posibles, debido a que la información se ha convertido en el activo más importante de las empresas.

En la actualidad, gran parte de las organizaciones consideran que la información y la tecnología representan activos importantes para la misma, sin dejar de lado otros activos indispensables, como los requerimientos de calidad, controles, seguridad e información. Por tal razón, los directivos deben establecer un adecuado sistema de control interno, para proporcionar seguridad razonable, respecto a si están lográndose los objetivos como: promover la efectividad y eficiencia de las operaciones, proteger y conservar todos los recursos de la

organización, cumplir las leyes y reglamentos internos y externos relacionados con la empresa.

Para esto, se hace necesario aplicar una auditoria de sistemas llevando a cabo una metodología adecuada, que permita evaluar de manera objetiva las vulnerabilidades o falta de controles existentes en la empresa.

Las metodologías desarrolladas y utilizadas en la auditoría y el control informático, se dividen en dos grupos:

- Cuantitativas
- Cualitativas

Las metodologías cuantitativas están basadas en un modelo matemático, diseñadas para producir una lista de riesgos que pueden compararse entre sí con facilidad por tener asignados unos valores numéricos. Estos valores son datos de probabilidad de ocurrencia de un evento que se debe extraer de un riesgo de incidencias donde el número de incidencias tiende al infinito.

Y las metodologías cualitativas están basadas en el criterio humano capaz de definir un proceso de trabajo. Así mismo, esta metodología establece métodos estadísticos y lógica borrosa, que requiere menos recursos humanos y menos tiempo que las metodologías cuantitativas.

Esta metodología presenta un enfoque amplio y logra un plan de trabajo flexible y reactivo. Sin embargo tiene la desventaja de depender mucho de la experiencia, habilidad y calidad del profesional involucrado. Dicha anomalía nace de la dificultad que tiene un profesional sin experiencia que asume la función auditora y busca una fórmula fácil que le permita empezar su trabajo rápidamente. Por lo tanto es necesario que el auditor tenga una gran experiencia y una gran formación tanto auditora como informática. Esta formación debe ser adquirida mediante el estudio y la práctica.

Estas últimas hacen parte de los modelos a seguir dentro del control interno y son necesarias para desarrollar cualquier proyecto de manera ordenada y eficaz, por lo que cada una cumple un papel importante y al optar por una de ellas, el auditor debe cumplirlas a cabalidad.

1.7 **COBIT (*Control Objectives for Information and related Technology*).**

La Organización ISACA *(Information Systems Audit and Control Association*), se formó como una fundación de educación para llevar a cabo los esfuerzos de investigación a gran escala para expandir el conocimiento y el valor de la gobernanza de las Tecnologías de Información (TI) y el campo de control. A través de su fundación, publicó en 1995 el COBIT, como resultado de cuatro años de intensa investigación[4].

El COBIT es una metodología utilizada en las empresas para auditar los sistemas de información, donde se evalúa la gestión y el control, enfocado a los administradores de las TI, los usuarios y los auditores encargados del proceso.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, mini computadoras y ambientes distribuidos, esta basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

La estructura del modelo COBIT, evalúa los criterios de información, como la seguridad y calidad, así como también se verifican los recursos que comprenden la tecnología de información, como el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos implicados en la organización.

Cuando se implementa el COBIT adecuadamente en una organización, se evalúa de manera ágil y consistente el cumplimiento de los objetivos de control, haciendo que los procesos y recursos de información y tecnología contribuyan al logro de los objetivos de la empresa.

[4] www.degerencia.com/articulos/los_cinco_componentes_del_control_interno.

El modelo COBIT, clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro dominios:

1.7.1 Dominio planificación y organización (PO): este dominio cubre la estrategia y las tácticas y 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 de negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

Procesos:

1.7.1.1 PO1 Definición de un plan estratégico

- PO1.1 Administración del valor de TI
- PO1.2 Alineación de TI con el negocio
- PO1.3 Evaluación del desempeño y la capacidad actual
- PO1.4 Plan estratégico de TI
- PO1.5 Planes tácticos de TI
- PO1.6 Administración del portafolio de TI

Objetivo: lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, para asegurar sus logros futuros. Su realización se concreta a través un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo, los que deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo, la definición de objetivos de negocio y necesidades de TI, la alta gerencia será la responsable de desarrollar e implementar planes a largo y corto plazo que satisfagan la misión y las metas generales de la organización.

1.7.1.2 PO2 Definición de la arquitectura de información

- PO2.1 Modelo de arquitectura de información empresarial
- PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos

- PO2.3 Esquema de clasificación de datos
- PO2.4 Administración de integridad

Objetivo: satisfacer los requerimientos de negocio, organizando de la mejor manera posible los sistemas de información, a través de la creación y mantenimiento de un modelo de información de negocio, asegurándose que se definan los sistemas apropiados para optimizar la utilización de esta información, tomando en consideración:

1.7.1.3 PO3 Determinación de la dirección tecnológica

- PO3.1 Planeación de la dirección tecnológica
- PO3.2 Plan de infraestructura tecnológica
- PO3.3 Monitoreo de tendencias y regulaciones futuras
- PO3.4 Estándares tecnológicos
- PO3.5 Consejo de arquitectura de TI

Objetivo: aprovechar al máximo de la tecnología disponible o tecnología emergente, satisfaciendo los requerimientos de negocio, a través de la creación y mantenimiento de un plan de infraestructura tecnológica, tomando en consideración:

1.7.1.4 PO4 Definición de la organización y de las relaciones de TI

- PO4.1 Marco de trabajo de procesos de TI
- PO4.2 Comité estratégico de TI
- PO4.3 Comité directivo de TI
- PO4.4 Ubicación organizacional de la función de TI
- PO4.5 Estructura organizacional
- PO4.6 Establecimiento de roles y responsabilidades
- PO4.7 Responsabilidad de aseguramiento de calidad de TI
- PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento
- PO4.9 Propiedad de datos y de sistemas
- PO4.10 Supervisión

- PO4.11 Segregación de funciones
- PO4.12 Personal de TI
- PO4.13 Personal clave de TI
- PO4.14 Políticas y procedimientos para personal contratado
- PO4.15 Relaciones

Objetivo: prestación de servicios de TI, esto se realiza por medio de una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas

1.7.1.5 PO5 Manejo de la inversión

- PO5.1 Marco de trabajo para la administración financiera
- PO5.2 Prioridades dentro del presupuesto de TI
- PO5.3 Proceso presupuestal
- PO5.4 Administración de costos de TI
- PO5.5 Administración de beneficios

Objetivo: tiene como finalidad la satisfacción de los requerimientos de negocio, asegurando el financiamiento y el control de desembolsos de recursos financieros. Su realización se concreta a través presupuestos periódicos sobre inversiones y operaciones establecidas y aprobados por el negocio.

1.7.1.6 PO6 Comunicación de la dirección y aspiraciones de la gerencia

- PO6.1 Ambiente de políticas y de control
- PO6.2 Riesgo corporativo y marco de referencia de control interno de TI
- PO6.3 Administración de políticas para TI
- PO6.4 Implantación de políticas de TI
- PO6.5 Comunicación de los objetivos y la dirección de TI

Objetivo: asegura el conocimiento y comprensión de los usuarios sobre las aspiraciones del alto nivel (gerencia), se concreta a través de políticas establecidas y transmitidas a la comunidad de usuarios, necesitándose para esto

estándares para traducir las opciones estratégicas en reglas de usuario prácticas y utilizables.

1.7.1.7 PO7 Administración de recursos humanos

- PO7.1 Reclutamiento y retención del personal
- PO7.2 Competencias del personal
- PO7.3 Asignación de roles
- PO7.4 Entrenamiento del personal de TI
- PO7.5 Dependencia sobre los individuos
- PO7.6 Procedimientos de investigación del personal
- PO7.7 Evaluación del desempeño del empleado
- PO7.8 Cambios y terminación de trabajo

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

1.7.1.8 PO8 Asegurar el cumplimiento con los requerimientos externos

- PO8.1 Definición y mantenimiento de procedimientos para la revisión de requerimientos externos,
- PO8.2 Leyes, regulaciones y contratos
- PO8.3 Revisiones regulares en cuanto a cambios
- PO8.4 Búsqueda de asistencia legal y modificaciones
- PO8.5 Seguridad y privacidad
- Propiedad intelectual
- Flujo de datos externos y criptografía

Objetivo: cumplir con obligaciones legales, regulatorias y contractuales. Para ello se realiza una identificación y análisis de los requerimientos externos en cuanto a su impacto en TI, llevando a cabo las medidas apropiadas para cumplir con ellos y se toma en consideración:

1.7.1.9 PO9 Evaluación de riesgos

- PO9.1 Marco de trabajo de administración de riesgos
- PO9.2 Establecimiento del contexto del riesgo
- PO9.3 Identificación de eventos
- PO9.4 Evaluación de riesgos de TI
- PO9.5 Respuesta a los riesgos
- PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos

Objetivo: asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI, para ello se logra la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos.

1.7.1.10 PO10 Administración de proyectos

- PO10.1 Marco de trabajo para la administración de programas
- PO10.2 Marco de trabajo para la administración de proyectos
- PO10.3 Enfoque de administración de proyectos
- PO10.4 Compromiso de los interesados
- PO10.5 Declaración de alcance del proyecto
- PO10.6 Inicio de las fases del proyecto
- PO10.7 Plan Integrado del Proyecto
- PO10.8 Recursos del proyecto
- PO10.9 Administración de riesgos del proyecto
- PO10.10 Plan de calidad del proyecto
- PO10.11 Control de cambios del proyecto
- PO10.12 Planeación del proyecto y métodos de aseguramiento
- PO10.13 Medición del desempeño, reporte y monitoreo del proyecto
- PO10.14 Cierre del proyecto

Objetivo: establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión, para ello se realiza una identificación y priorización de los proyectos en línea con el plan operacional por parte de la misma organización.

Además, la organización deberá adoptar y aplicar sólidas técnicas de administración de proyectos para cada proyecto emprendido.

1.7.1.11 PO11 Administración de calidad

- PO11.1 Sistema de administración de calidad
- PO11.2 Estándares y prácticas de calidad
- PO11.3 Estándares de desarrollo y de adquisición
- PO11.4 Enfoque en el cliente de TI
- PO11.5 Mejora continua
- PO11.6 Medición, monitoreo y revisión de la calidad.

Objetivo: satisfacer los requerimientos del cliente, para ello se realiza una planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización.

1.7.2 **Dominio: adquisición e implementación (AI):** para llevar a cabo la estrategia de TI, las soluciones deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Este dominio cubre cambios y mantenimiento realizado a sistemas existentes.

Procesos:

1.7.2.1 AI1 Identificación de soluciones automatizadas

- AI1.1 Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio
- AI1.2 Reporte de análisis de riesgos
- AI1.3 Estudio de factibilidad y formulación de cursos de acción alternativos
- AI1.4 Requerimientos, decisión de factibilidad y aprobación

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.

1.7.2.2 AI2 Adquisición y mantenimiento del software aplicativo

- AI2.1 Diseño de alto nivel
- AI2.2 Diseño detallado
- AI2.3 Control y posibilidad de auditar las aplicaciones
- AI2.4 Seguridad y disponibilidad de las aplicaciones
- AI2.5 Configuración e implantación de software aplicativo adquirido
- AI2.6 Actualizaciones importantes en sistemas existentes
- AI2.7 Desarrollo de software aplicativo
- AI2.8 Aseguramiento de la calidad del software
- AI2.9 Administración de los requerimientos de aplicaciones
- AI2.10 Mantenimiento de software aplicativo

Objetivo: proporciona funciones automatizadas que soporten efectivamente al negocio, para ello se definen declaraciones específicas sobre requerimientos funcionales y operacionales y una implementación estructurada con entregables claros.

1.7.2.3 AI3 Adquisición y mantenimiento de la infraestructura tecnológica

- AI3.1 Plan de adquisición de infraestructura tecnológica
- AI3.2 Protección y disponibilidad del recurso de infraestructura
- AI3.3 Mantenimiento de la infraestructura
- AI3.4 Ambiente de prueba de factibilidad

Objetivo: proporcionar las plataformas apropiadas para soportar aplicaciones de negocios. Para ello se realizara una evaluación del desempeño del hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema.

1.7.2.4 AI4 Facilitar la operación y el uso

- AI4.1 Plan para soluciones de operación
- AI4.2 Transferencia de conocimiento a la gerencia del negocio

- AI4.3 Transferencia de conocimiento a usuarios finales.
- AI4.4 Transferencia de conocimiento al personal de operaciones y soporte

Objetivo: asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas, para ello se realiza un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento.

1.7.2.5 AI5 Adquirir recursos

- AI5.1Control de adquisición
- AI5.2 Administración de contratos con proveedores
- AI5.3 Selección de proveedores
- AI5.4 Adquisición de recursos de TI

Objetivo: responder a los requerimientos del negocio de acuerdo con la estrategia de negocio, mientras se reducen los defectos y la repetición de trabajos en la prestación del servicio y en la solución

1.7.2.6 AI6 Administración de los cambios

- AI6.1 Estándares y procedimientos para cambios
- AI6.2 Evaluación de impacto, priorización y autorización
- AI6.3 Cambios de emergencia
- AI6.4 Seguimiento y reporte del estatus de cambio
- AI6.5 Cierre y documentación del cambio

Objetivo: minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores. Esto se hace posible a través de un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI.

1.7.2.7 AI7 Instalación y aceptación de los sistemas

- AI7.1 Entrenamiento
- AI7.2 Plan de prueba
- AI7.3 Plan de implantación

- AI7.4 Ambiente de prueba
- AI7.5 Conversión de sistemas y datos
- AI7.6 Pruebas de cambios
- AI7.7 Prueba de aceptación final.
- AI7.8 Promoción a producción
- AI7.9 Revisión posterior a la implantación

Objetivo: verificar y confirmar que la solución sea adecuada para el propósito deseado, para ello se realiza una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas

1.7.3 **Dominio: entregar y dar soporte (DS):** en este dominio se 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. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

Procesos:

1.7.3.1 DS1 Definición de niveles de servicio

- DS1.1 Marco de trabajo de la administración de los niveles de servicio
- DS1.2 Definición de servicios
- DS1.3 Acuerdos de niveles de servicio.
- DS1.4 Acuerdos de niveles de operación
- DS1.5 Monitoreo y reporte del cumplimento de los niveles de servicio
- DS1.6 Revisión de los acuerdos de niveles de servicio y de los contratos

Objetivo: establecer una comprensión común del nivel de servicio requerido, para ello se establecen convenios de niveles de servicio que formalicen los criterios de desempeño contra los cuales se medirá la cantidad y la calidad del servicio.

1.7.3.2 DS2 Administración de servicios prestados por terceros

- DS2.1 Identificación de todas las relaciones con proveedores
- DS2.2 Gestión de relaciones con proveedores
- DS2.3 Administración de riesgos del proveedor
- DS2.4 Monitoreo del desempeño del proveedor

Objetivo: asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos, para ello se establecen medidas de control dirigidas a la revisión y monitoreo de contratos y procedimientos existentes, en cuanto a su efectividad y suficiencia, con respecto a las políticas de la organización y toma en consideración:

1.7.3.3 DS3 Administración de desempeño y capacidad

- DS3.1 Planeación del desempeño y la capacidad
- DS3.2 Capacidad y desempeño actual
- DS3.3 Capacidad y desempeño futuros
- DS3.4 Disponibilidad de recursos de TI
- DS3.5 Monitoreo y reporte

Objetivo: Asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado, para ello se realizan controles de manejo de capacidad y desempeño que recopilen datos y reporten acerca del manejo de cargas de trabajo, tamaño de aplicaciones, manejo y demanda de recursos

1.7.3.4 DS4 Asegurar el servicio continúo

- DS4.1 Marco de trabajo de continuidad de TI
- DS4.2 Planes de continuidad de TI
- DS4.3 Recursos críticos de TI
- DS4.4 Mantenimiento del plan de continuidad de TI
- DS4.5 Pruebas del plan de continuidad de TI
- DS4.6 Entrenamiento del plan de continuidad de TI

- DS4.7 Distribución del plan de continuidad de TI
- DS4.8 Recuperación y reanudación de los servicios de TI
- DS4.9 Almacenamiento de respaldos fuera de las instalaciones
- DS4.10 Revisión post reanudación

Objetivo: mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones, para ello se tiene un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio

1.7.3.5 DS5 Garantizar la seguridad de sistemas

- DS5.1 Administración de la seguridad de TI
- DS5.2 Plan de seguridad de TI
- DS5.3 Administración de identidad
- DS5.4 Administración de cuentas del usuario
- DS5.5 Pruebas, vigilancia y monitoreo de la seguridad
- DS5.6 Definición de incidente de seguridad
- DS5.7 Protección de la tecnología de seguridad
- DS5.8 Administración de llaves criptográficas
- DS5.9 Prevención, detección y corrección de software malicioso
- DS5.10 Seguridad de la red
- DS5.11 Intercambio de datos sensitivos

Objetivo: salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida, para ello se realizan controles de acceso lógico que aseguren que el acceso a

1.7.3.6 DS6 Educación y entrenamiento de usuarios

- DS6.1 Identificación de necesidades de entrenamiento y educación
- DS6.2 Impartición de entrenamiento y educación
- DS6.3 Evaluación del entrenamiento recibido

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

1.7.3.7 DS7 Identificación y asignación de costos

- DS7.1 Definición de servicios
- DS7.2 Contabilización de TI
- DS7.3 Modelación de costos y cargos
- DS7.4 Mantenimiento del modelo de costos

Objetivo: asegurar un conocimiento correcto de los costos atribuibles a los servicios de TI, para ello se realiza un sistema de contabilidad de costos que asegure que éstos sean registrados, calculados y asignados a los niveles de detalle. Los elementos sujetos a cargo deben ser recursos identificables, medibles y predecibles para los usuarios.

1.7.3.8 DS8 Apoyo y asistencia a los clientes de TI

Objetivo: asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente, para ello se realiza un Buró de ayuda que proporcione soporte y asesoría de primera línea, Consultas de usuarios y respuesta a problemas estableciendo un soporte de una función de buró de ayuda

1.7.3.9 DS9 Administración de la configuración

- DS9.1 Repositorio y línea base de configuración
- DS9.2 Identificación y mantenimiento de elementos de configuración
- DS9.3 Revisión de integridad de 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, para ello se realizan controles que identifiquen y registren todos los activos de TI así como su localización física y un programa regular de verificación que confirme su existencia.

1.7.3.10 DS10 Administración de Problemas

- DS10.1 Identificación y clasificación de problemas
- DS10.2 Rastreo y resolución de problemas
- DS10.3 Cierre de problemas
- DS10.4 Integración de las administraciones de cambios, configuración y problemas

Objetivo: asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que vuelvan a suceder, para ello se necesita un sistema de manejo de problemas que registre y dé seguimiento a todos los incidentes, además de un conjunto de procedimientos de escalamiento de problemas para resolver de la manera más eficiente los problemas identificados. Este sistema de administración de problemas deberá también realizar un seguimiento de las causas a partir de un incidente dado.

1.7.3.11 DS11 Administración de datos

- DS11.1 Requerimientos del negocio para administración de datos
- DS11.2 Acuerdos de almacenamiento y conservación
- DS11.3 Sistema de administración de librerías de medios
- DS11.4 Eliminación
- DS11.5 Respaldo y restauración
- DS11.6 Requerimientos de seguridad para la administración de datos

Objetivo: asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento. Lo cual se logra a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI. Para tal fin, la gerencia deberá diseñar formatos de entrada de datos para los usuarios de manera que se minimicen lo errores y las omisiones durante la creación de los datos.

1.7.3.12 DS12 Administración de las instalaciones

- DS12.1 Selección y diseño del centro de datos

- DS12.2 Medidas de seguridad física
- DS12.3 Acceso físico
- DS12.4 Protección contra factores ambientales
- DS12.5 Administración de instalaciones físicas

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.

1.7.3.13 DS13 Administración de la operación

- DS13.1 Procedimientos e instrucciones de operación
- DS13.2 Programación de tareas
- DS13.3 Monitoreo de la infraestructura de TI
- DS13.4 Documentos sensitivos y dispositivos de salida
- DS13.5 Mantenimiento preventivo del hardware

Objetivo: asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada, esto se logra a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades. Para ello, la gerencia deberá establecer y documentar procedimientos para las operaciones de tecnología de información (incluyendo operaciones de red), los cuales deberán ser revisados periódicamente para garantizar su eficiencia y cumplimiento.

1.7.4 **Dominio: monitorear y evaluar (ME):** todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad. Este es, precisamente, el ámbito de este dominio.

Procesos:

1.7.4.1 ME1 Monitoreo del proceso

- ME1.1 Enfoque del monitoreo
- ME1.2 Definición y recolección de datos de monitoreo
- ME1.3 Método de monitoreo
- ME1.4 Evaluación del desempeño
- ME1.5 Reportes al consejo directivo y a ejecutivos
- ME1.6 Acciones correctivas

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., para ello la gerencia podrá definir indicadores claves de desempeño y/o factores críticos de éxito y compararlos con los niveles objetivos propuestos para evaluar el desempeño de los procesos de la organización. La gerencia deberá también medir el grado de satisfacción del los clientes con respecto a los servicios de información proporcionados para identificar deficiencias en los niveles de servicio y establecer objetivos de mejoramiento, confeccionando informes que indiquen el avance de la organización hacia los objetivos propuestos.

1.7.4.2 ME2 Evaluar lo adecuado del control interno

- ME2.1 Monitoreo del marco de trabajo de control interno
- ME2.2 Revisiones de auditoría
- ME2.3 Excepciones de control
- ME2.4 Auto Evaluación del control
- ME2.5 Aseguramiento del control interno
- ME2.6 Control interno para terceros
- ME2.7 Acciones correctivas

Objetivo: asegurar el logro de los objetivos de control interno establecidos para los procesos de TI, para ello la gerencia es la encargada de monitorear la efectividad

de los controles internos a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias., evaluar su efectividad y emitir reportes sobre ellos en forma regular. Estas actividades de monitoreo continuo por parte de la Gerencia deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

1.7.4.3 ME3 Obtención de Aseguramiento Independiente

- ME3.1 Identificar los requerimientos de las leyes, regulaciones y cumplimientos contractuales.
- ME3.2 Optimizar la respuesta a requerimientos externos
- ME3.3 Evaluación del cumplimiento con requerimientos externos
- ME3.4 Aseguramiento positivo del cumplimiento
- ME3.5 Reportes integrados

Objetivo: incrementar los niveles de confianza entre la organización, clientes y proveedores externos. Este proceso se lleva a cabo a intervalos regulares de tiempo, para ello la gerencia deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de implementar nuevos servicios de tecnología de información que resulten críticos, como así también para trabajar con nuevos proveedores de servicios de tecnología de información. Luego la gerencia deberá adoptar como trabajo rutinario tanto hacer evaluaciones periódicas sobre la efectividad de los servicios de tecnología de información y de los proveedores de estos servicios como así también asegurarse el cumplimiento de los compromisos contractuales de los servicios de tecnología de información y de los proveedores de estos servicios.

1.7.4.4 ME4 Proveer auditoría independiente

- ME4.1 Establecimiento de un marco de gobierno de TI
- ME4.2 Alineamiento estratégico
- ME4.3 Entrega de valor
- ME4.4 Administración de recursos

- ME4.5 Administración de riesgos
- ME4.6 Medición del desempeño
- ME4.7 Aseguramiento 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 auditorías independientes desarrolladas a intervalos regulares de tiempo. Para ello la gerencia deberá establecer los estatutos para la función de auditoría, destacando en este documento la responsabilidad, autoridad y obligaciones de la auditoria. El auditor deberá ser independiente del auditado, esto significa que los auditores no deberán estar relacionados con la sección o departamento que esté

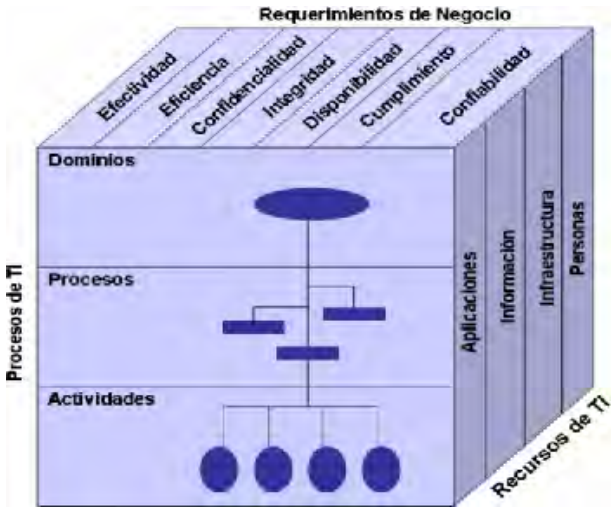
1.8 OBJETIVOS DE CONTROL

Un objetivo de control se define como "la declaración del resultado deseado o propuesto que se ha de alcanzar mediante la aplicación de procedimientos de control en cualquier actividad de TI".

En resumen, la estructura conceptual se puede enfocar desde tres puntos de vista:

- Los recursos de las TI
- Los criterios empresariales que deben satisfacer la información
- Los procesos de TI
- Estos dominios facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.
- Además, se toma en cuenta los recursos que proporciona la tecnología de información, tales como: datos, aplicaciones, plataformas tecnológicas, instalaciones y recurso humano.

Figura 2: Las tres dimensiones conceptuales de COBIT



Fuente: manual del COBIT 4.1

Toda organización, necesita desarrollar una tecnología que le permita rediseñar actividades y procesos para lograr un mejor desempeño en las mismas, es así como el COBIT es fundamental en toda empresa, pues esta metodología reduce posibles vulnerabilidades y riesgos de los recursos de las tecnologías de información y así mismo evalúa el resultado de los objetivos de la empresa.

2. METODOLOGÍA

Para alcanzar los objetivos propuestos, se utilizó la metodología de tipo empírico, porque se realiza recolección y análisis de datos, además se toma como fuente primaria de información la observación directa por parte del auditor, también, se estudian y aplican conceptos y esquemas teóricos, también cabe mencionar que esta metodología clasifica dentro del tipo de investigación aplicada, ya que todas las recomendaciones finales deberán ser aplicadas para tener un funcionamiento de calidad.

De conformidad con lo anterior, se planeó y ejecutó el trabajo de manera que el examen y el resultado de las pruebas proporcionaran una base razonable para fundamentar la opinión y los conceptos expresados en el informe.
La auditoría realizada por el equipo auditor fue dividida en varias etapas así:

- **Etapa I. Familiarización con el entorno:** en esta etapa se realiza el estudio previo al inicio de la Auditoría con el propósito de conocer en detalle la entidad auditada y en si la infraestructura física de la red de datos de la sede principal, además se evalúa el portal web de la entidad, bajo dos diferentes estrategias incluyendo la proporcionada por la estrategia Gobierno en Línea bajo el decreto 1151 de abril de 2008.

  Los resultados de la exploración permiten, además, hacer la selección de las técnicas y metodologías de auditoría a utilizar.

  Se realizaron visitas a la entidad donde se tuvo un contacto directo tanto con personal de la oficina de sistemas como con la documentación solicitada por el auditor y la observación directa de los equipos de cómputo, redes de datos, servidores entre otros.
- **Etapa II. Planeación de la auditoría de sistemas:** en esta etapa se realizó la planificación de todo el proceso que se requiere para la realización de la auditoría.

- Identificar el alcance y los objetivos de la auditoría a realizar.
- Realizar el estudio inicial en la entidad a auditar para recolectar datos sobre la infraestructura física de la red de datos y el cumplimiento del decreto 1151 de 2008 de Gobierno en línea.
- Determinar los recursos necesarios para realizar la auditoría.
- Elaboración del plan de trabajo.

- **Etapa III. Realización de las actividades de la auditoría:** en esta etapa se hicieron efectivos todos los planteamientos de la etapa anterior, con la aplicación de las metodologías y técnicas seleccionadas que garantizaron el cumplimiento de los objetivos planeados. Las actividades que se realizaron dentro de esta etapa, fueron:
- Elaboración del plan de auditoría, para identificar dentro de los dominios del COBIT, los procesos y los objetivos de control que se van a evaluar.
- Elaboración de cuadros de definición de fuentes de conocimiento, análisis, y pruebas de auditoría, para cada uno de los procesos seleccionados dentro de los dominios del COBIT, para ser auditados.
- Realización de pruebas sobre los procesos seleccionados y sobre la infraestructura de la red..
- Elaboración de los cuestionarios cuantitativos para cada uno de los procesos seleccionados dentro de los dominios del COBIT, para ser auditados.
- Identificación de hallazgos dentro del proceso evaluado.
- Asignación de la probabilidad de ocurrencia e impacto para los riesgos detectados mediante la aplicación del formato de hallazgos.

- **Presentación del Informe Final**: se realizó un informe final donde se describen los hallazgos encontrados, junto a las recomendaciones necesarias para subsanar los hallazgos encontrados, además se hace un análisis profundo de los desaciertos del portal web de la entidad.

3. DESARROLLO DEL TRABAJO

3.1 ARCHIVO PERMANENTE

El archivo permanente contiene información tanto constante como variable en el tiempo. Esta información es de vital importancia y se considera necesaria para comprender en forma exacta, rápida y sencilla las características de las áreas objeto de auditoría.

- **Leyes y decretos comunes**: en este apartado se citaran las leyes y decretos que regularon el proceso de auditoría en las dos entidades.

- A los efectos del artículo 12 de la Ley 15/1999, el proveedor únicamente tratará los datos de carácter personal a los que tenga acceso conforme a las instrucciones del cliente y no los aplicará o utilizará con un fin distinto al objeto del contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el caso de que el proveedor destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

- **Misión**

Somos una empresa especializada en el sector ferretero, que trabaja día a día para satisfacer necesidades, deseos y expectativas de nuestros clientes a través de diversos servicios; amplio portafolio de productos con las mejores marcas, excelente calidad y precios competitivos; y a través de un equipo humano altamente capacitado, pugnamos cada día por ser líderes en el mercado y proyectarnos con dinamismo a nuestra comunidad.

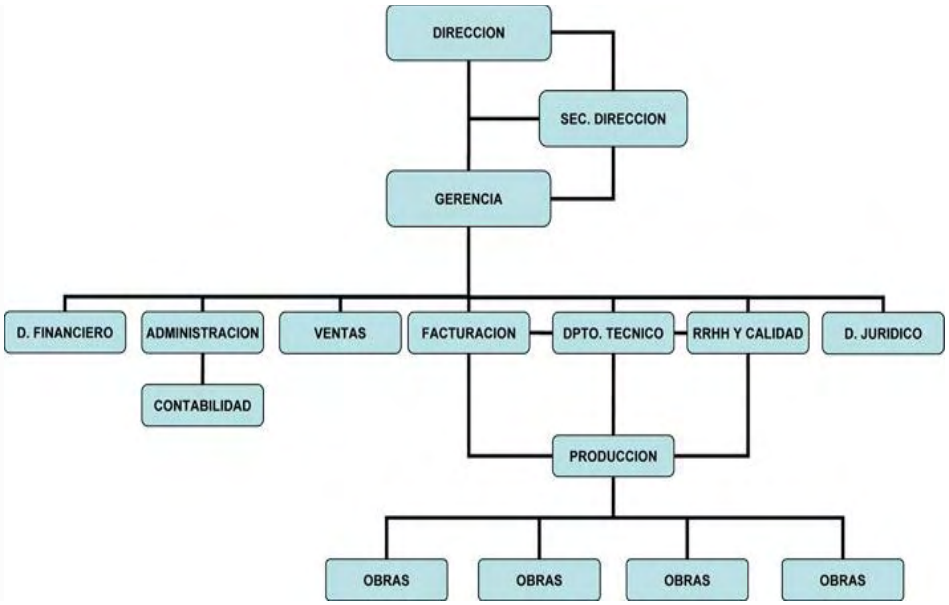
- **Visión**

Ser una empresa líder en el sector ferretero en los departamentos de Nariño y Putumayo, buscando superar las expectativas de nuestros clientes,

proyectándonos como una compañía competitiva que sea de gran aporte para el crecimiento económico de nuestra región.

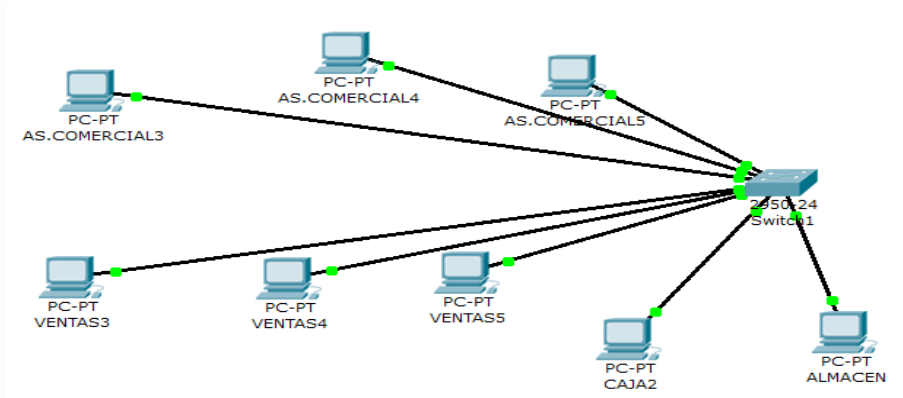
- **Organigrama**

Fig.3 Organigrama



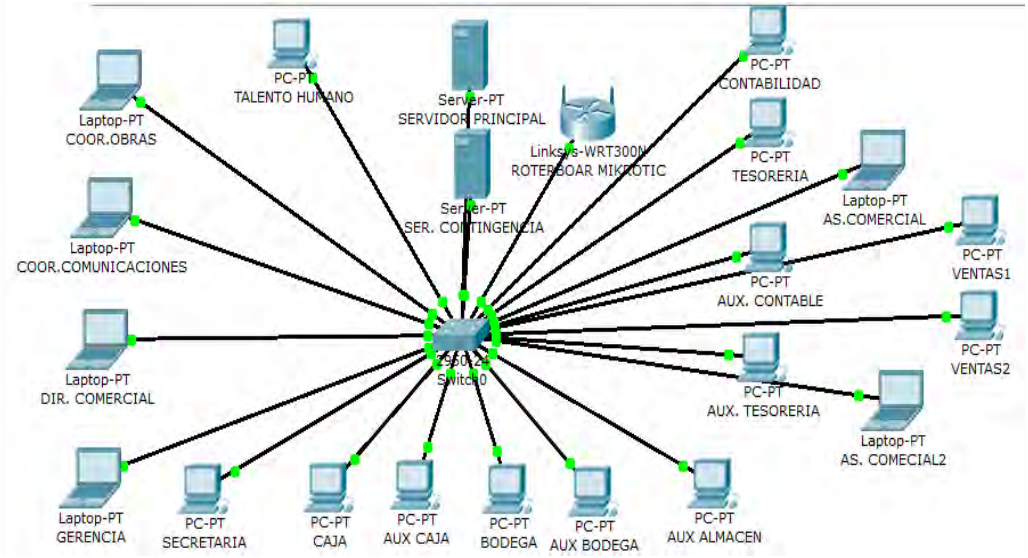
Fuente : recursos humanos Texcol

Fig. 4. Topología red lan piso 1



Fuente : recursos humanos texcol

Fig 5.Topologia red lan piso 2



Fuente: recursos humanos Texcol

3.2. ARCHIVO CORRIENTE

Este archivo está compuesto por documentos directamente relacionados con el desarrollo del trabajo.

3.2.1 Plan de auditoría: las metodologías son necesarias para desarrollar cualquier tipo de proyecto de forma ordenada eficaz, razón por la que la metodología utilizada para la realización de la auditoria de sistemas dentro de **TEXCOL LTDA.** Es de tipo cuantitativo/subjetivo, basado en un modelo matemático numérico, arrojando como resultado una lista de riesgos obtenidos del análisis de cada uno de los procesos a auditar teniendo en cuenta su importancia e impacto dentro del área de sistemas de ahí su calificación y recomendaciones realizadas.

La metodología aplicada en la realización de esta auditoría, se ejecutó de la siguiente manera:

Etapa1. Exploración del entorno: este primer paso se realizó con el fin de familiarizarse con el área de sistemas de la entidad **TEXCOL LTDA**, se hace un estudio previo de los procesos a auditar obteniendo así las herramientas necesarias para una adecuada planeación de la auditoria, también en esta etapa se definen que elementos se utilizaron para elaborar la auditoria. Se realizaron varias visitas con el fin de conocer y observar los diferentes procesos, para identificarlos y auditarlos, a través de entrevistas abiertas se dio inicio a la recolección de información, dando el siguiente paso que fueron la aplicación de cuestionarios cuantificables con los funcionarios de los diferentes departamentos de **TEXCOL LTDA.**

Etapa2. Planeación de las actividades de auditoria: aquí se realizó la planificación de todo el proceso de la auditoría, con las siguientes actividades:

- Se realizó un estudio previo del área de **TEXCOL LTDA.** obteniendo información necesaria respecto al tema.
- Se identificó el alcance y los objetivos de la auditoria a realizar.
- Determinación de los recursos necesarios con los que se realizó la auditoria.
- Se elaboró el plan de trabajo.

Etapa3. Realización las actividades de la auditoria: en esta etapa se realizaron las diferentes actividades implantadas en la etapa anterior, mediante la aplicación de técnicas junto con la aplicación de diferentes herramientas que garantizo el cumplimiento de los objetivos propuestos para la ejecución de la auditoria. En esta etapa se realizaron las siguientes actividades:

- Elaboración del plan de auditoría, a través de COBIT permitiendo así la identificación de los procesos y objetivos de control evaluados. Se elaboran cuadros de definición de fuentes de conocimiento, que facilitan la identificación clara de la fuente de obtención de las pruebas.

- Se aplicaron entrevistas con preguntas abiertas y preguntas cerradas para la obtención de información general de la empresa, para luego elaborar diferentes cuestionarios cuantitativos para cada uno de los procesos seleccionados dentro de los dominios del COBIT a auditar.

- Se realizó la identificación de vulnerabilidades, riesgos y amenazas, y su valoración con respecto a la probabilidad e impacto mediantes la utilización del COBIT (modelo para auditoría y control de sistemas de información).

✓ Identificar las vulnerabilidades, riesgos y amenazas existentes en el sistema.
✓ Valorar los riesgos según la escala definida para la probabilidad e impacto.
✓ Identificación de hallazgos. Mediante el formato de hallazgos, se asigna la probabilidad de ocurrencia e impacto para los riesgos encontrados.

✓ Elaboración de la matriz de probabilidad e impacto, que permitió identificar los riesgos altos que necesitan mitigarse de manera urgente mediante un plan correctivo.

Etapa 4. Presentación del informe final: etapa en la cual se realizó el informe final que contiene todos los procesos evaluados con la descripción del comportamiento que estos tienen dentro de la empresa o los hallazgos encontrados con sus respectivas recomendaciones que permitan mitigarlos al máximo. Este informe se presentó y se entregó al ingeniero de sistemas de **TEXCOL LTDA.** Para que tomen las respectivas correcciones a implantar mediante un plan de mejoramiento.

3.2.2 Instrumentos de recolección de datos

- **Fuentes primarias:** las fuentes primarias en el desarrollo de esta auditoría se poseen las siguientes:

✓ Entrevista, dirigida al ingeniero de sistemas de **TEXCOL LTDA.**
✓ Ejecución de los cuestionarios en todas áreas de la Empresa de **TEXCOL LTDA**.

- ✓ Manuales, que estén relacionados con los procesos que se manejan en el área de sistemas en la Empresa **TEXCOL LTDA.**
- **Fuentes secundarias:** para el desarrollo de este proyecto de auditoría, se cuenta con la vasta gama de libros referenciales y la web, por lo anterior se podrá consultar temas relacionados con auditorías informáticas de seguridad de la red de datos, información relacionada con software para la auditoria de redes, Etc.
- **Plan de pruebas:** el plan de Pruebas permite anotar todas las observaciones durante el proceso de la auditoria de manera secuencial, este contiene lo siguiente: Prueba, Proceso, tipo y acción de la prueba.

3.2.3 Programa de auditoría: para la ejecución de la auditoria física de la infraestructura tecnológica de equipos y de la Red de Datos de la Empresa **TEXCOL LTDA**, se utiliza la metodología COBIT (Control Objetives for Information and related Technology) de ISACA *(Information System Audit and Control Asociation*), que cubre 210 objetivos de control clasificados en 4 dominios y 34 procesos. De los cuales se aplican los siguientes:

3.2.3.1 Dominio planificación y organización (PO): la Planificación y el dominio de Organización cubren el empleo de tecnología y como puede esta ser mejor utilizada en una empresa para ayudar a alcanzar los objetivos de la empresa. Esto también destaca la forma de organización que la infraestructura tecnológica y la TI debe tomar para alcanzar los resultados óptimos.

Procesos de dominio planificación y organización (PO)

- PO1 definir un plan estratégico de TI
- PO3 determinar la dirección tecnológica
- PO4 definir los procesos, organización y relaciones de TI
- PO5 administrar la inversión en TI
- PO9 evaluar y administrar los riesgos de TI

PO1 definir un plan estratégico de TI: la planeación estratégica de TI es necesaria para gestionar y dirigir todos los recursos de TI en línea con la estrategia y prioridades del negocio. La función de TI y los interesados del negocio son responsables de asegurar que el valor óptimo se consigue desde los proyectos y el portafolio de servicios. El plan estratégico mejora la comprensión de los interesados clave de las oportunidades y limitaciones de TI, evalúa el desempeño actual, identifica la capacidad y los requerimientos de recursos humanos, y clarifica el nivel de investigación requerido. La estrategia de negocio y prioridades se reflejarán en portafolios y se ejecutarán por los planes estratégicos de TI, que especifican objetivos concisos, planes de acción y tareas que están comprendidas y aceptadas tanto por negocio como por TI.

- **Que satisface el requerimiento del negocio de:** sostener o extender los requerimientos de gobierno y de la estrategia del negocio, al mismo tiempo que se mantiene la transparencia sobre los beneficios, costos y riesgos
- **Enfocándose en:** la incorporación de TI y de la gerencia del negocio en la traducción de los requerimientos del negocio a ofertas de servicio, y el desarrollo de estrategias para entregar estos servicios de una forma transparente y rentable.

- **Se logra con:**
  - ✓ El compromiso con la alta gerencia y con la gerencia del negocio para alinear la planeación estratégica de TI con las necesidades del negocio actuales y futuras
  - ✓ El entendimiento de las capacidades actuales de TI
  - ✓ La aplicación de un esquema de prioridades para los objetivos del negocio que cuantifique los requerimientos del negocio
- **Objetivos de control:** definir un plan estratégico de TI que satisfaga el requerimiento de negocio de TI de sostener o extender la estrategia de negocio y los requerimientos de gobierno al mismo tiempo que se mantiene la transparencia sobre los beneficios, costos y riesgos.

- **PO1.3 Evaluación del desempeño y la capacidad actual:** el departamento de sistemas debe diseñar e implementar una metodología de evaluación de desempeño de los planes que se encuentran en ejecución en la entidad los cuales servirán para cumplir las metas propuestas.
- **PO1.4 Plan estratégico de TI:** debe realizar planes de evaluación y adquisición de nuevas opciones tecnologías de acuerdo a las necesidades operativas.

PO3 Determinar la dirección tecnológica: aprovechar al máximo la tecnología disponible o tecnología emergente satisfaciendo los requerimientos de negocio, a través de la creación y mantenimiento de un plan de infraestructura tecnológica.

- **Que satisface el requerimiento del negocio de**: contar con sistemas aplicativos estándares, bien integrados, rentables y estables, así como recursos y capacidades que satisfagan requerimientos de negocio, actuales y futuros.

- **Enfocándose en:** la definición e implementación de un plan de infraestructura tecnológica, una arquitectura y estándares que tomen en cuenta y aprovechen las oportunidades tecnológicas

- **Se logra con:** el establecimiento de un foro para dirigir la arquitectura y verificar el cumplimiento

  El establecimiento de un plan de infraestructura tecnológica equilibrado versus costos, riesgos y arquitectura de información.

- **Objetivos de control:** se busca actualizar regularmente aspectos referentes a la arquitectura de sistemas, dirección tecnológica, planes de adquisición, estándares, estrategias de migración y contingencias, con el fin de que la empresa aproveche al máximo sus recursos tecnológicos.

- **PO3.1 Planeación de la dirección:** 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. 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, los aspectos de contingencia de los componentes de la infraestructura.
- **PO3.2 Plan de infraestructura tecnológica:** crear y mantener 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 para inversiones y personal en sistemas de información y la mejora en la interoperabilidad de las plataformas y las aplicaciones.

PO4 Definir los procesos de TI, organización y relaciones de TI: la Prestación de servicios de TI se realiza a través de una organización conveniente en número y habilidades con tareas y responsabilidades definidas y comunicadas.

- **Que satisface el requerimiento del negocio de:** agilizar la respuesta a las estrategias del negocio mientras se cumplen los requerimientos de gobierno y se establece en puntos de contacto definidos y competentes.

- **Enfocándose en:** el establecimiento de estructuras organizacionales de TI transparentes, flexibles y responsables, y en la definición e implementación de procesos de TI con dueños, y en la integración de roles

- **Se logra con:**

  - ✓ La definición de un marco de trabajo de procesos de TI

- ✓ La definición de un cuerpo y una estructura organizacional apropiada.
- ✓ La definición de roles y responsabilidades

- **Objetivos de control:** se busca definir el personal de la tecnología de información, los roles, las funciones y responsabilidades, permitiendo el buen funcionamiento de servicios que satisfagan los objetivos del área de Sistemas que concuerden los de la empresa.

  Teniendo en cuenta los siguientes objetivos de control:

  - **PO4.6 Responsabilidad de aseguramiento de calidad de TI:** el área de sistemas debe definir y dar a conocer a la institución el personal que deberá encargarse del desempeño y funcionamiento de la red de datos. Además sus funciones deberán de quedar guardadas en el manual de funciones interno del área y de la institución.
  - **PO4.13 Políticas y procedimientos para personal contratado**: el área de sistemas deberá identificar la persona clave de TI para la administración de la red de datos y disminuir la dependencia en una sola persona para realizar funciones críticas.

  PO5 Administrar la inversión en TI: los recursos de inversión para implementación de elementos tecnológicos que se utilizan para el buen funcionamiento de la red física de datos necesitan de controles y proyecciones óptimas buscando el beneficio de la entidad.

- **Que satisface el requerimiento del negocio de:** mejorar de forma continua y demostrable la rentabilidad de TI y su contribución a la rentabilidad del negocio con servicios integrados y estandarizados que satisfagan las expectativas del usuario.
- **Enfocándose en:** decisiones de portafolio e inversión de TI y su contribución a la rentabilidad del negocio con servicios integrados y estandarizados que satisfagan las expectativas del usuario.

- **Se logra con:**
    - ✓ El pronóstico y la asignación de presupuesto
    - ✓ La definición de criterios formales de inversión
    - ✓ La medición y evaluación del negocio.
- **Objetivos de control**: administrar la inversión en TI que satisfaga el requerimiento de negocio de TI de mejorar de forma constante y demostrable la rentabilidad de TI y su contribución a la utilidad del negocio con servicios integrados y estándar que satisfagan las expectativas del usuario final
- **PO5.1 Marco de trabajo para la administración financiera:** se deberá designar un equipo de trabajo para encargarse de la administración de la inversión y costos del funcionamiento de la red de datos.
- **PO5.2 Prioridades dentro del presupuesto de TI:** si la entidad quiere que sus recursos que se inviertan en la infraestructura de la red de datos retorne la contribución al portafolio empresarial y sus objetivos, se debe de priorizar los proyectos, mantenimientos y compras de nueva tecnología en el presupuesto.

1. **PO9 Evaluar y administrar los riesgos de TI:** se refiere a crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales acordados. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar.

- **Que satisface el requerimiento del negocio de:** analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y metas del negocio.

- **Enfocándose en:** la elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales de riesgo

operacional, evaluación de riesgos, mitigación del riesgo y comunicación de riesgos residuales.

- **Se logra con:**
    - ✓ La garantía de que la administración de riesgos este incluida completamente en los procesos.
    - ✓ La realización de evaluaciones de riesgo.
    - ✓ La recomendación y comunicación de planes de acción para remediar riesgos.
- **Objetivos de control:** se encargan de identificar, analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y metas de la empresa, con el objetivo de asegurar el logro de los objetivos de TI, con la estabilidad y el funcionamiento de las comunicaciones de la red.

  Se deben adoptar estrategias de mitigación de riesgos para minimizarlos a un nivel aceptable de acuerdo a los siguientes objetivos de control:

    - **PO9.1 Alineación de la administración de riesgos de TI y del negocio**: el área de sistemas debe de iniciar un plan de administración de riesgos que afecte la red de datos de la entidad.
    - **PO9.3 Identificación de eventos**: se debe de realizar autoevaluaciones de manera periódica para identificar los principales elementos de la red de datos que se encuentran predispuestos a todo tipo de riesgo, amenazas, vulnerabilidades de cualquier evento que afecte el funcionamiento de la red de datos, además de determinar su naturaleza.
    - **PO9.4 Evaluación de riesgos IT**: se evaluaran los riegos de forma sistemática de manera cuantitativa y cualitativa, su probabilidad de impacto y sus efectos sobre el funcionamiento de la red de datos.
    - **PO9.5 Respuesta a los riesgos:** teniendo identificados los riesgos se debe de diseñar un plan de procesos en el cual se pueda evitar,

reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia a riesgos.

- **PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos:**

  El plan de riesgos debe de ser apoyado desde la alta dirección para que pueda ser ejecutado en el momento de ser necesario y ser monitoreado con el fin de dar respuestas en cualquier momento ante algún riesgo.

3.2.3.2 Dominio: 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. Además, cubre los cambios y el mantenimiento realizado a los sistemas existentes.

Procesos de dominio adquisición e implementación:

AI2. Adquirir y mantener software aplicativo

AI3. Adquirir y mantener infraestructura tecnológica

AI5. Adquirir recursos de TI

AI2 Adquirir y mantener software aplicativo: es importante contar con software que se utilice para monitorear la red de datos y además darle mantenimiento al software para que el proceso de monitoreo sea correcto y oportuno.

- **Que satisface el requerimiento del negocio de**: construir las aplicaciones de acuerdo con los requerimientos del negocio y haciéndolas a tiempo y a costo razonable.
- **Enfocándose en:** garantizar que exista un proceso de desarrollo oportuno y confiable.

- **Se logra con**:

  - ✓ La traducción de requerimientos de negocio a especificaciones de diseño
  - ✓ La adhesión a los estándares de desarrollo para todas las modificaciones
  - ✓ La separación de las actividades de desarrollo de pruebas y operativas

- **Objetivos de control:** *Adquirir y mantener software aplicativo* que satisfaga el requerimiento de negocio de TI de *hacer* diferentes aplicaciones de acuerdo con los requerimientos del negocio en tiempo y a un costo razonable.

  - **AI2.5 Configuración e implantación de software aplicativo Adquirido:** se debe de tener un software que sea configurado e implementado a las necesidades de la red de datos para ayudar en su monitoreo y buen funcionamiento.
  - **AI2.10 Mantenimiento de software aplicativo:** el software debe de tener un plan de mantenimiento como una guía de actualizaciones que ayuden a mejorar su rendimiento.

AI3 Adquirir y mantener la infraestructura tecnológica: proporcionar las plataformas apropiadas para soportar aplicaciones de negocios debido al costo y a la importancia de los elementos que constituyen la red física de datos es prioritaria tanto la adquisición como el mantenimiento de estos elementos fundamentales para el proceso tecnológico de la entidad.

- **Que satisface el requerimiento del negocio de:** adquirir y dar mantenimiento a una infraestructura integrada y estándar de TI.

- **Enfocándose en:** proporcionar plataformas adecuadas para las aplicaciones del negocio, de acuerdo con la arquitectura definida de TI y los estándares de tecnología.

- **Se logra con:**

  - ✓ El establecimiento de un plan de adquisición de tecnología que se alinea con el plan de infraestructura tecnológica.
  - ✓ La planeación de mantenimiento de la infraestructura.
  - ✓ La implantación de medidas de control interno, seguridad y auditabilidad.

- **Objetivos de control:** se busca satisfacer con los requerimientos de la empresa, el área de sistemas debe contar un plan operativo donde se garantice el buen funcionamiento, mantenimiento y cumplimiento de los estándares de la infraestructura tecnológica para dar soporte a los diferentes procesos dentro de la empresa.

  Toma en consideración los siguientes objetivos de control:

  - **AI3.1 Plan de adquisición de infraestructura tecnológica:** el área de sistemas debe de tener claro cuáles son las necesidades a nivel de infraestructura que necesita la red de datos para así poder diseñar un plan de adquisición, implementación y mantenimiento, además de tener en cuenta futuras ampliaciones en la capacidad de funcionamiento de la red de datos.
  - **AI3.2 Protección y disponibilidad del recurso de infraestructura:** Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad. Se deben definir y comprender claramente las responsabilidades al utilizar componentes de infraestructura sensitivos por todos aquellos que desarrollan e integran los componentes de infraestructura. Se debe monitorear y evaluar su uso.

- **AI3.3 Mantenimiento de la infraestructura:** se analizara si la infraestructura de la red de datos cuenta con lo necesario para responder a los procesos ejecutados por la entidad a través de ella además de diseñar un plan de mantenimiento de los elementos que la conforman.

AI5 Adquirir recursos de TI: se deben suministrar recursos TI, incluyendo personas, hardware, software y servicios; esto requiere de la definición y la ejecución de los procedimientos de adquisición, la selección de proveedores, el ajuste de arreglos contractuales y la adquisición en sí. El hacerlo así garantiza que la organización tenga todos los recursos de TI que se requieran de una manera oportuna y rentable.

- **Que satisface el requerimiento del negocio de:** mejorar la rentabilidad de TI y su contribución a la utilidad del negocio.

- **Enfocándose en:** adquirir y mantener las habilidades de TI que respondan a la estrategia de entrega, en una infraestructura TI, integrada y estandarizada, y reducir el riesgo de adquisición de TI.

- **Se logra con:**

  - ✓ La obtención de asesoría profesional legal y contractual.
  - ✓ La definición de procedimientos y estándares de adquisición.

- **Objetivos de Control:** se busca proveer los recursos TI según lo requiera la empresa de manera oportuna y rentable (Personal, hardware y servicios) teniendo en cuenta la definición de procesos definidos de adquisición..

  Tiene en cuenta los siguientes objetivos de control:

  - **AI5.6 Adquisición de infraestructura, instalaciones y servicios relacionados:** proteger y hacer cumplir los intereses de la organización en todos los contratos incluyendo los derechos y obligaciones para la adquisición de infraestructura.

3.2.3.3 Dominio - entregar y dar soporte (DS)

Administración de instalaciones (DS12): debido a la importancia de información que se maneja en terminales o servidores y la importancia de cada uno de los elementos de la red de datos es de vital importancia darle control y manejo adecuado a cada una de las instalaciones.

- **DS12.1 Selección y diseño del centro de datos:** se debe diseñar e implementar el centro de datos como considera las leyes y regulaciones correspondientes, para que así la comunicación a través de la red de datos sea optima y cumpla con las necesidades del servicio.
- **DS12.2 Medidas de seguridad física:** al no encontrarse ninguna medida de seguridad física la red se encuentra vulnerable a múltiples amenazas tanto de origen ambiental como de origen humano. Se debe de tener claro la persona encargada de aplicar los correctivos y ejecutar las medidas diseñadas para solucionar cualquier riesgo.
- **DS12.3 Acceso físico:** se debe tener claro los roles del personal de sistemas y demás áreas de la entidad, ninguna persona sin autorización o el rol adecuado puede estar en área de los equipos de comunicación de la red de datos.
- **DS12.5 Administración de instalaciones físicas:** las instalaciones físicas de los equipos que conforman la red de datos deben de ser administrados de tal manera que cumplan con los lineamientos de seguridad, leyes, reglamentos y requerimientos por el cual están en funcionamiento.

3.2.3.4 Dominio monitorear y evaluar (ME)

ME2 Supervisar y evaluar el control interno: establecer un programa de control interno efectivo para TI requiere de un proceso bien definido de monitoreo. Este proceso incluye el monitoreo y el

reporte de las excepciones de control, resultados de las auto-Evaluaciones y revisiones por parte de terceros. Un beneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables teniendo en cuenta los siguientes objetivos de control.

- **Que satisface el requerimiento del negocio de:** proteger el logro de los objetivos de TI y cumplir las leyes y reglamentos relacionados con TI
- **Enfocándose en:** el monitoreo de los procesos de control interno para las actividades relacionadas con TI e identificar las acciones de mejoramiento.
- **Se logra con:**
  - ✓ La definición de un sistema de controles internos integrados en el marco de trabajo de los procesos de TI.
  - ✓ Monitorear y reportar actividades de los controles internos sobre TI.
  - ✓ Reportar las excepciones de control a la gerencia para tomar acciones.
- **Objetivos de control:** monitorear y evaluar el control interno que satisfaga el requerimiento de negocio de TI de proteger el logro de los objetivos de TI y cumplir con las leyes y regulaciones relacionadas con TI
- **ME2.1 Monitorear el marco de trabajo de control interno:** El área de sistemas debe de implementar un marco de trabajo de monitorización de la red de datos para que se garantice los procesos en los cuales se ve involucrada y sirva para cumplir las metas de la entidad.
- **ME2.7 Acciones correctivas:** de acuerdo a los controles que se ejecuten sobre la red de datos, el área de sistemas diseñara y ejecutara planes de acciones correctivas.

3.3 CUADROS FUENTES DE CONOCIMIENTO

- Fuentes de conocimiento y plan de pruebas
- Descripción de los cuadros de cuestionarios y entrevistas

Los ítems que se encuentran en este formato son:

REF: identificación del cuadro de Definición.

ENTIDAD AUDITADA: nombre de la entidad a la cual se le está realizando el proceso de auditoría.

OBJETO DE ESTUDIO: identificación de la parte a evaluar

RESPONSABLES: nombres del equipo auditor que está llevando a cabo el proceso de auditoría.

MATERIAL DE SOPORTE: nombre del modelo tomado en la aplicación de la auditoria, en este caso COBIT.

DOMINIO: nombre del dominio de COBIT que se está evaluando.

PROCESO: nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.

Fuentes de Conocimiento: entrevistas y cuestionarios y documentación

Repositorio de pruebas aplicables: posibilidades de respuestas, de análisis de ejecución.

FUENTE: de donde se obtiene la información

Medidas o Indicadores: determina porcentajes

Cuadro de cuestionarios y entrevistas

DOMINIO: Planeación y organización (PO)

PROCESO: PO1 Definir un plan estratégico de TI.

TEXCOL	Empresa Auditora: redes y servicios informáticos	Tipo de Registro: Cuadro de Definición de Fuentes de Conocimiento, Pruebas de Análisis y Auditoria.
Entidad Auditada:	TEXCOL LTDA	
Área Auditada:	**SISTEMAS**	**Ref: PO1-1**
Objeto de Estudio	**Funcionamiento Infraestructura tecnológica equipos de cómputo y red de datos**	
Responsables:	RONALD DARIO CERON ALEX ALBEIRO URBANO	
Material de Soporte:	Manual Cobit 4.0	
DOMINIO: Planeación y Organización (PO)		
PROCESO: PO1 Definir un Plan Estratégico de TI.		
Descripción de la Actividad/Prueba: Determinar Fuentes de Conocimiento, Determinar las Pruebas de Análisis del Sistema y las Pruebas de Auditoria definidas en la Metodología Cobit.		

Fuentes de Conocimiento	Métricas: Medidas o Indicadores	REPOSITORIO DE PRUEBAS APLICABLES	
		De Análisis	De Ejecución
- Entrevista al ingeniero encargado del área de sistemas de TEXCOL LTDA - Entrevista a los diferentes funcionarios de TEXCOL LTDA -plan estratégico de la empresa TEXCOL LTDA. -Arquitectura de Red. -Plan de gestión de TEXCOL LTDA -Presupuesto para infraestructura tecnológica.	% de la organización de la red de datos % de aplicabilidad y factibilidad de los planes de contingencia. % de funcionalidad, y relación costo-beneficio en cuanto al plan de infraestructura tecnológica de la red de datos. % factibilidad, relación costo beneficio de las soluciones tecnológicas en cuanto a la red de datos.	-Analizar la estructura y organización de la empresa. -Analizar plan estratégico de la empresa -Analizar el plan de contingencia para el área de sistemas -Analizar plan de gestión de la empresa -Análisis del plan de infraestructura tecnológica. -Analizar soluciones tecnológicas existentes en la empresa.	-Revisión detallada de plan estratégico de la empresa - Revisión detallada de plan de gestión de la empresa -Revisión detallada de la Arquitectura de red, de las políticas y aplicación de las normas. -Revisión detallada de los planes de contingencia, el cumplimiento de estas, el conocimiento por el personal. -Revisar detalladamente el plan de infraestructura tecnológico de la red de datos. -Revisar soluciones tecnológicas en cuanto a la parte de la red de datos.

Cuadros de Procesos cuestionarios y entrevistas

Ver anexo cuestionarios y entrevistas PO3

Ver anexo cuestionarios y entrevistas PO4

Ver anexo cuestionarios y entrevistas PO5

Ver anexo cuestionarios y entrevistas PO9

Ver anexo cuestionarios y entrevistas AI2

Ver anexo cuestionarios y entrevistas AI3

Ver anexo cuestionarios y entrevistas AI5

Ver anexo cuestionarios y entrevistas DS12

Ver anexo cuestionarios y entrevistas EM2

3.4 RECOLECCIÓN DE INFORMACIÓN.

3.4.1 Cuestionario cuantitativo: permite definir preguntas tomando como base el cuadro de definición de fuente de conocimiento. El cuestionario presenta tres opciones de respuesta (SI, NO, NA (No Aplica)), permitiendo así calificar el proceso entre 1 a 5, teniendo en cuenta el nivel de importancia de la pregunta, bajo criterio de los auditores, la sumatoria del puntaje de las preguntas da el total de la encuesta, se califica las columnas del SI, las del NO y las NA, sumando el puntaje de las preguntas. La fuente permite identificar los responsables bien sea una determinada persona o cualquier medio del cual se tomó la información para calificar.

Con la aplicación del cuestionario cuantitativo se obtuvo el porcentaje de riesgo el cual se obtiene aplicando la siguiente fórmula:

% de Riesgo= $\frac{Sumatoria\ de\ SI * 100}{Total\ Encuesta - Totales\ NA}$

% Total de Riesgo = 100 - % de Riesgo

Para determinar el nivel de riesgo total, se tuvo en cuenta la siguiente categorización:

1% - 30% = Riesgo Bajo

31% - 70% = Riesgo Medio

71% - 100% = Riesgo Alto

Riesgo bajo: Deficiencias bajas en grado de importancia mayor, fáciles de solucionar a largo plazo.

*Riesgo medio: S*e debe tomar medidas de solución o mejora en un determinado periodo de tiempo.

Riesgo alto: se debe establecer soluciones inmediatas para reducir el riesgo sin afectar los objetivos del caso de estudio.

Entonces, se calcula así:

% de Riesgo Total = 100 - % de Riesgo

El resultado obtenido, permitió formular conclusiones acerca de funcionamiento del proceso evaluado, teniendo en cuenta que este toma validez con la obtención de pruebas, que verifique los resultados de la encuesta.

Los ítems que se encuentran en este formato son:

REF: identificación del cuadro de Definición.

ENTIDAD AUDITADA: nombre de la entidad a la cual se le está realizando el proceso de auditoría.

OBJETO DE ESTUDIO: identificación de la parte a evaluar

AREA AUDITADA: área de estudio

RESPONSABLES: nombres del equipo auditor que está llevando a cabo el proceso de auditoría.

MATERIAL DE SOPORTE: nombre del modelo tomado en la aplicación de la auditoria, en este caso COBIT.

DOMINIO: nombre del dominio de COBIT que se está evaluando.

PROCESO: nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.

PREGUNTA: listado de preguntas que serán evaluadas.

SI, NO Y NA: posibilidades de respuestas, Cumple, No cumple o No Aplica para la entidad.

OBSERVACION: si existe alguna recomendación o anexo

TOTAL: se asigna los valores correspondientes a cada columna, la sumatoria de los SI, de los NO y NA.

TOTAL CUESTIONARIO: la suma de los campos de las opciones.

PORCENTAJE DE RIESGO: determina el nivel de riesgo total (Riesgo Bajo, Medio o Alto)

Recolección de información **Dominio planeación y organización**

Cuestionario PO1

TEXCOL	**CUESTIONARIO CUANTITATIVO**	**REF**			
		PLAN PO1			
ENTIDAD AUDITADA		**TEXCOL LTDA**		**PAGINA**	
				1 **DE**	**2**
AREA AUDITADA	Sistemas	**OBJETO DE ESTUDIO**	Funcionamiento Infraestructura tecnológica equipos de cómputo y red de datos		
RESPONSABLES		RONALD DARIO CERON ALEX ALBEIRO URBANO			
MATERIA L DE SOPORTE		COBIT 4.0			
DOMINIO	Planeación y Organización (PO)	**PROCESO**	PO1 Definir un Plan Estratégico de TI.		

PREGUNTA	SI	NO	NA	OBSERVACION
1. ¿Considera que la estrategia de la tecnología de la información está alineada con el desarrollo del negocio?		**4**		**ANEXO2**
2. ¿Existe inventario de la infraestructura tecnológica instalada?		**5**		**ANEXO2**
3¿Se están optimizando el uso de los recursos?		**5**		**ANEXO2**
4¿Las personas de la organización entienden los objetivos de las TI?	**2**			Existe dependencia hacia el ingeniero ya que es el único encargado
5¿Cree que la calidad de los sistemas que se tienen implementados es buena?	**2**			**ANEXO2**
6¿considera que el plan estratégico existente para realizar copias de respaldo es bueno?		**5**		Existe dependencia hacia el ingeniero ya que es el único encargado
7¿Le parece que el mantenimiento preventivo que se está realizando a la infraestructura tecnológica es apropiado?		**5**		Existe dependencia hacia el ingeniero ya que es el único encargado
8 ¿La inversión realizada por gerencia en infraestructura tecnológica es apropiada?	**2**			**ANEXO2**
9 ¿En caso de problema en red, el protocolo para superar el fallo es conveniente?		**4**		**ANEXO2**

10 ¿Existen planes de contingencia adecuados en caso de daño de hardware necesario para administrar la Red de datos?		**5**		Existe dependencia hacia el ingeniero ya que es el único encargado
TOTAL	**6**	**33**		
TOTAL CUESTIONARIO		**39**		

PORCENTAJE DE RIESGO:= $\frac{6*100}{39}$= 15.38%

% de Riesgo Total = 100 – 15.38 = 84.62%

Por lo tanto el porcentaje de riesgo es ALTO.

Cuadros cuantitativos de recolección de información dominios y procesos:

Ver anexo cuadro cuantitativo PO3

Ver anexo cuadro cuantitativo PO4

Ver anexo cuadro cuantitativo PO5

Ver anexo cuadro cuantitativo PO9

Ver anexo cuadro cuantitativo AI2

Ver anexo cuadro cuantitativo AI3

Ver anexo cuadro cuantitativo AI5

Cuadros de cuestionarios de control

ENTIDAD AUDITADA: nombre de la entidad a la cual se le está realizando el proceso de auditoría.

DOMINIO: nombre del dominio de COBIT que se está evaluando.

PROCESO: nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.

Objetivo de Control: punto de auditoria

PREGUNTA: listado de preguntas que serán evaluadas.

SI, NO Y NA: posibilidades de respuestas, Cumple, No cumple o No Aplica para la entidad.

TOTAL: se asigna los valores correspondientes a cada columna, la sumatoria de los SI, de los NO y NA.

TOTAL CUESTIONARIO: la suma de los campos de las opciones.

PORCENTAJE DE RIESGO: determina el nivel de riesgo total (Riesgo Bajo, Medio o Alto)

Entregar y dar soporte (DS)

Cuestionario de control C1

TEXCOL LTDA			**PASTO**
Cuestionario de Control			**C1**
Dominio	Entrega de Servicios y Soportes		
Proceso	DS12: Administración de Instalaciones.		
Objetivo de Control	Escolta de Visitantes		
Cuestionario			
Pregunta	**SI**	**NO**	**N/A**
¿Las instalaciones (cubículos y oficinas) fueron diseñadas o adaptadas específicamente para funcionar como un centro de cómputo?		4	**ANEXO1**
¿Se tiene una distribución del espacio adecuada, de forma tal que facilite el trabajo y no existan distracciones?		4	**ANEXO1**
¿Existe suficiente espacio dentro de las instalaciones de forma que permita una circulación fluida?	3		**ANEXO1**
¿Existen lugares de acceso restringido?		5	**ANEXO1**

¿Se cuenta con sistemas de seguridad para impedir el paso a lugares de acceso restringido?		5	**ANEXO1**
¿Se cuenta con sistemas de emergencia como son detectores de humo, alarmas, u otro tipo de censores?	3		**ANEXO1**
¿Existen señalizaciones adecuadas en las salidas de emergencia y se tienen establecidas rutas de evacuación?		4	**ANEXO1**
¿Se tienen medios adecuados para extinción de fuego en el centro de cómputo?	4		**ANEXO1**
¿Se cuenta con iluminación adecuada y con iluminación de emergencia en casos de contingencia?		3	**ANEXO1**
¿Se tienen sistemas de seguridad para evitar que se sustraiga equipo de las instalaciones?	4		**ANEXO1**
¿Se tiene un lugar asignado para papelería y utensilios de trabajo?	3		**ANEXO1**
¿Son funcionales los muebles instalados dentro del centro de cómputo: archiveros, mesas de trabajo, etc.?		3	**ANEXO1**
¿Existen prohibiciones para fumar, consumir alimentos y bebidas?	4		**ANEXO1**
¿Se cuenta con suficientes carteles en lugares visibles que recuerdan estas prohibiciones?	3		**ANEXO1**
¿Con cuanta frecuencia se limpian las instalaciones? Semanal		3	**ANEXO1**
Mensual			**ANEXO1**
Anual			**ANEXO1**
¿Se cuenta en los cuartos de comunicaciones con piso falso?		4	**ANEXO1**

¿Con cuanta frecuencia se limpian los ductos de aire y la cámara de aire que existe debajo del piso falso (si existe)? Semanal		4	**ANEXO1**
Mensual			
Anual		4	**ANEXO2**
TOTAL	24	43	
TOTAL CUESTIONARIO	67		

PORCENTAJE DE RIESGO:= $\frac{24*100}{67}$= 35.82%

% de Riesgo Total = 100 – 35.82= 64.18

Por lo tanto el porcentaje de riesgo es MEDIO.

Cuadros de cuestionarios de control de procesos:

Ver anexo cuestionario de control DS12 cuadro2

Ver anexo cuestionario de control DS12 cuadro3

Ver anexo cuestionario de control DS12 cuadro4

Ver anexo cuestionario de control ME2 cuadro5

3.5 LISTA DE RIESGOS

- **Riesgos dominio planeación y organización**

PO1 definir un plan estratégico de TI

R1. No existe un grupo encargado de evaluar y estudiar el desempeño de la infraestructura tecnológica

R2. No existen políticas ni procedimientos relacionados con la conformación adecuada de la arquitectura de la infraestructura tecnológica

PO3 Determinar la dirección tecnológica

R3 No existe un plan de infraestructura tecnológica.

R4 No hay un inventario actualizado de la infraestructura tecnológica en la empresa TEXCOL LTDA.

R5 No se lleva un registro documentado de los estudios de nuevas tecnologías y elementos que pueden ser incorporados al sistema de la red de datos

R6 No se realizan simulacros con los planes de contingencia en caso de fallas de software o hardware en la infraestructura tecnológica.

R7. No hay un cronograma de mantenimientos preventivos a. la infraestructura tecnológica.

PO4 Definición de la organización y de las relaciones de TI

R8 El manual de funciones del personal del área de sistemas no se actualiza con frecuencia, con sus respectivas funciones, descripción de cargo y requerimientos, personal responsable.

R9 En caso de falta del personal clave en la parte de Redes de datos no se tiene planes de contingencia para su reemplazo en caso de ausencia o no está documentado.

PO5 Administrar la inversión en TI

R10 No se realiza un proceso de toma de decisiones que de prioridad para la asignación de recursos a la adquisición de elementos tecnológicos que contribuyan con el mejoramiento del sistema de red de datos.

R11 No existen política para elaboración y mantenimiento de un buen presupuesto que sea utilizado en la adquisición de elementos que contribuyan con el sistema de red de datos.

PO9 Evaluación y análisis de riesgos

R12 No existe el plan de evaluación de riesgos del área de sistemas en la infraestructura tecnológica de TEXCOL LTDA

R13 No existe un plan de contingencia ni de seguridad para contrarrestar un evento que afecte la conexión física de la red de datos

Riesgos Dominio adquisición e implementación (AI)

AI2 Adquirir y mantener software aplicativo

R15 No existe software que se utilice para monitorear la conexión de la red de datos en su aspecto físico.

R16 No se tiene ningún tipo de software para el mantenimiento y monitoreo de la conexión física de la red de datos.

AI3 Adquirir y mantener la infraestructura tecnológica

R17 No existe documentación sobre las políticas de mantenimiento que se realiza a la infraestructura tecnológica.

R18 No existe conocimiento por parte de la gran mayoría de funcionarios sobre las políticas de adquisición de hardware.

R19 No existe documentación del proceso de mantenimiento de la infraestructura tecnológica

R20 No existe manual de funciones para el personal encargado de realizar mantenimiento preventivo y correctivo de la infraestructura tecnológica

R21 No se tiene una implementación adecuada de cableado estructurado.

R22 No se tiene planos del cableado estructurado que se extiende por la entidad.

R23 No se realiza seguimiento adecuado de los elementos como: servidores, routers y switches ya que las hojas de vida no recolectan la información necesaria.

AI5 Adquirir infraestructura instalaciones y servicios

R24 No existe un procedimiento específico para instalaciones de la red de datos

Riesgos dominio entregar y dar soporte (DS)

DS12 Administración de instalaciones

R25 No existen políticas adecuadas en el campo de seguridad referente al acceso y salida de las instalaciones donde se encuentran los elementos que conforman el aspecto físico de la red de datos.

R26 Dentro de las políticas de seguridad para el acceso a las instalaciones no se tiene en cuenta la identificación, autenticación y autorización de los individuos que ingresan

R27 la parte de cableado de la red de datos se encuentra con cables sueltos, fuera de canaletas, no sigue un estándar definido.

R28 No existen prohibiciones para fumar, consumir alimentos y bebidas, falta suficientes carteles en lugares visibles.

R29 Con poca frecuencia se revisan y calibran los controles ambientales.

R30 No se tiene un plan de emergencia si falla los controles ambientales.

R31 No se Realizan simulacros con la planta eléctrica.

R32 No se tienen medidas implementadas en caso de falla del sistema de seguridad del área de sistemas

Riesgos dominio monitorear y evaluar (ME)

ME2 Evaluar lo adecuado del control interno

R33 No existen políticas ni procedimientos que se encaminen a monitorear la seguridad de la infraestructura tecnológica.

R34 No existe conocimiento para el personal encargado de administrar la red de datos sobre políticas y procedimientos de monitorear la seguridad del aspecto físico de la red de datos.

R35 No se realizan auditorias de ningún tipo para evaluar el desempeño de la parte eléctrica, ventilación del centro de cómputo y utilización de normas de cableado estructurado.

3.6 VALORACIÓN DE RIESGOS

TEXCOL	VALORACIÓN DE RIESGOS						REF
							VLRN_1
N°	**RIESGOS/VALORACIÓN**	**PROBABILIDAD**			**IMPACTO**			**DOMINIO**
		A	**M**	**B**	**L**	**M**	**C**	
R1	No existe un grupo encargado de evaluar y estudiar el desempeño de la infraestructura tecnológica	X				**X**		PO1 (3)
R2	No existen políticas ni procedimientos relacionados con la conformación adecuada de la arquitectura de la infraestructura tecnológica	X				**X**		PO1(3)
R3	No existe un plan de infraestructura tecnológica	**X**					**X**	PO 3(1)
R4	No hay un inventario actualizado de la infraestructura tecnológica en la empresa TEXCOL LTDA	X				**X**		PO 3(1)
R5	No se lleva un registro documentado de los estudios de nuevas tecnologías y elementos que pueden ser incorporados al sistema de la red de datos	**X**			X			PO 3(1)

R6	No se realizan simulacros con los planes de contingencia en caso de fallas de software o hardware en la infraestructura tecnológica metas organizacionales.	**X**				**X**		PO 3(1)
R7	No hay un cronograma de mantenimientos preventivos a. la infraestructura tecnológica	X				**X**		PO3 (1)
R8	El manual de funciones del personal del área de sistemas no se actualiza con frecuencia, con sus respectivas funciones, descripción de cargo y requerimientos, personal responsable.	**X**				**X**		PO4 (6)
R9	En caso de falta del personal clave en la parte de Redes de datos no se tiene planes de contingencia para su reemplazo en caso de ausencia o no está documentado.	X					**X**	PO4(13)
R10	No se realiza un proceso de toma de decisiones que de prioridad para la asignación de recursos a la adquisición de elementos tecnológicos que contribuyan con el mejoramiento del sistema de red de datos.	**X**			X			PO5 (1)
R11	No existen política para elaboración y mantenimiento de un buen presupuesto que							

	sea utilizado en la adquisición de elementos que contribuyan con el sistema de red de datos.		**X**				**X**	PO5 (2)
R12	No existe el plan de evaluación de riesgos del área de sistemas en la infraestructura tecnológica de TEXCOL LTDA	**X**			**X**			PO9 (1) PO9 (3)
R13	No existe un plan de contingencia ni de seguridad para contrarrestar un evento que afecte la conexión física de la red de datos.	X				**X**		PO9(4) PO9(5)
R14	No se cuenta con pólizas de seguros para el manejo del riesgo	X					**X**	PO9(6)
R15	No existe software que se utilice para monitorear la conexión de la red de datos en su aspecto físico		**X**		**X**			AI2 (5)
R16	No se tiene ningún tipo de software para el mantenimiento y monitoreo de la conexión física de la red de datos.		**X**		X			AI2 (10)
R17	No existe documentación sobre las políticas de mantenimiento que se realiza a la infraestructura tecnológica	X				**X**		AI3 (3)
R18	No existe conocimiento por parte de la gran mayoría de funcionarios sobre las políticas de adquisición de hardware.		X		X			AI3 (1)

R19	No existe documentación del proceso de mantenimiento de la infraestructura tecnológica	**X**				X		AI3 (3)
R20	No existe manual de funciones para el personal encargado de realizar mantenimiento preventivo y correctivo de la infraestructura tecnológica		**X**			X		AI3 (3)
R21	No se tiene una implementación adecuada de cableado estructurado	**X**				X		AI3 (3)
R22	No se tiene planos del cableado estructurado que se extiende por la entidad.			X	X			AI3 (3)
R23	No se realiza seguimiento adecuado de los elementos como: servidores, routers y switches ya que las hojas de vida no recolectan la información necesaria	**X**				X		AI3 (3)
R24	No existe un procedimiento específico para instalaciones de la red de datos.	X			X			AI5 (6)
R25	No existen políticas adecuadas en el campo de seguridad referente al acceso y salida de las instalaciones donde se encuentran los elementos que conforman el aspecto físico de	X				**X**		DS12(2) DS12(3)

	la red de datos							
R26	Dentro de las políticas de seguridad para el acceso a las instalaciones no se tiene en cuenta la identificación, autenticación y autorización de los individuos que ingresan	X				X		DS12(2) DS12(3)
R27	la parte de cableado de la red de datos se encuentra con cables sueltos, fuera de canaletas, no sigue un estándar definido	X				X		DS12(1) DS12(5)
R28	No existen prohibiciones para fumar, consumir alimentos y bebidas, falta suficientes carteles en lugares visibles			X			X	DS12(5)
R29	Con poca frecuencia se revisan y calibran los controles ambientales		X		X			DS12(5)
R30	No se tiene un plan de emergencia si falla los controles ambientales		X		X			DS12(5)
R31	No se Realizan simulacros con la planta eléctrica			X	X			DS12(5)
R32	No se tienen medidas implementadas en caso de falla del sistema de seguridad del área de sistemas		X			X		DS12(1) DS12(5)
R33								

3.7 MATRIZ DE IMPACTO CON RIESGOS ENCONTRADOS EN PROCESO

Matriz de probabilidad e impacto: según el MECI este componentes primordial en el desarrollo de la auditoria ya que permite determinar el nivel de riesgo de cada uno de los hallazgos encontrados, tanto cualitativa como cuantitativamente. Por medio de esta clasificación se puede observar cuál de los riegos es catastrófico, importante, moderado o aceptable y a su vez el respectivo valor del riesgo.

Probabilidad				
	Alto(3)	Riesgo Moderado (15)	Riesgo Importante (30)	Riesgo Inaceptable (60)
	Medio(2)	Riesgo Tolerable (10)	Riesgo Moderado (20)	Riesgo Importante (40)
	Bajo(1)	Riesgo Aceptable (5)	Riesgo Tolerable (10)	Riesgo Moderado (20)
		Bajo(leve)(5)	Medio(moderado)(10)	Alto(catastrófico)(20)
		Impacto		

4. HALLAZGOS

A continuación se describirán los hallazgos encontrados en la TEXCOL LTDA después de un análisis exhaustivo.

Dominios y procesos auditados en la TEXCOL LTDA

Los hallazgos encontrados en TEXCOL LTDA se presentaran en el orden de los dominios y procesos auditados los cuales fueron:

Dominio - planificación y organización (PO)

- Definir un plan estratégico de TI (PO1).
- Determinar la dirección tecnológica (PO3).
- Definición de la organización y de las Relaciones de TI (PO4).
- Administrar la inversión en TI (PO5).
- Evaluación y análisis de riesgos (PO9).

Dominio - adquisición e implementación (AI)

- Adquirir y mantener software aplicativo (AI2).
- Adquirir y mantener la infraestructura tecnológica (AI3)
- Adquirir infraestructura instalación y servicios (AI5)

Dominio - entregar y dar soporte (DS)

- Administración de instalaciones (DS12).

Dominio - monitorear y evaluar (ME)

- Evaluar lo adecuado del control interno (ME2).

4.1 MATRIZ DE PROBABILIDAD DE IMPACTO

Matriz de probabilidad de ocurrencia e impacto según relevancia del proceso

Probabilidad				
	Alto(3)	Riesgo Moderado H5—PO3 H10—PO5 H12—PO9 H24—AI	Riesgo Importante: H1—PO1 H2--PO1 H4—PO3 H13—PO9 H6—PO3 H17—AI3 H7—PO3 H19—AI3 H8—PO4 H21—AI3 H23—AI3 H25—DS12 H26—DS12 H27—DS12	Riesgo Inaceptable H3—PO3 H9—PO4 H14—PO9 H35—ME
	Medio(2)	Riesgo Tolerable H15—AI2 H16—AI2 H18—AI3	Riesgo Moderado H20—AI3 H32—DS12 H34—ME2	Riesgo Importante H11—PO5 H33—ME2
	Bajo(1)	Riesgo Aceptable H22—AI3 H31—DS12	Riesgo Tolerable H29—DS12 H30—DS12	Riesgo Moderado H28—DS12
		Bajo(leve)(5)	Medio(moderado)(10)	Alto(catastrófico)(20)
		Impacto		

Descripción del Formato de Hallazgos

- **ENTIDAD AUDITADA:** hace referencia al nombre de la entidad auditada.
- **REF:** cuestionario que determino el Hallazgo.
- **AREA AUDITADA:** se refiere al área de TI la cual será el objeto de estudio.
- **SISTEMA:** hace referencia al nombre del sistema actual de la entidad auditada.

- **RESPONSABLES:** hace referencia a los nombres del equipo encargado de la auditoría.
- **Probabilidad:** hace referencia a la posibilidad de ocurrencia del riesgo.
- **Impacto:** hace referencia a las consecuencias que puede ocasionar a la entidad la materialización del riesgo.
- **Descripción Hallazgo:** se refiere a los detalles del hallazgo.
- **NIVEL DE RIESGO:** hace referencia al valor cualitativo o cuantitativo del riesgo.
- **CONSECUENCIA:** se refiere al efecto actual o futuro, que tendrá la organización, de no tomar las precauciones oportunas.
- **RECOMENDACIONES:** hace referencia a las descripciones correctivas de carácter preventivo.

Cuadro de hallazgos.

- **Formato de Hallazgos:** teniendo en cuenta la aplicación de los instrumentos para recolección de información, los objetivos planteados con anterioridad y los riesgos definidos en la Matriz se obtiene la siguiente tabla de hallazgos que está definida así:

REF: identificación de la tabla de hallazgos.

ENTIDAD AUDITADA: Nombre de la entidad a la cual se le está realizando el proceso

ÁREA AUDITADA: nombre del área a la cual se aplica la auditoria

OBJETO DE ESTUDIO: identificación de la parte a evaluar.

RESPONSABLES: nombre del equipo auditor que está llevando a cabo el proceso de auditoría.

MATERIA DE SOPORTE: nombre del modelo tomado en la aplicación de la auditoria, en este caso COBIT.

DOMINIO: nombre del dominio de COBIT que se está evaluando.

PROCESO: nombre del proceso en específico que se está auditando dentro de los dominios del COBIT

HALLAZGO: aquí se encontrara la descripción de cada hallazgo encontrado en los diferentes dominios

CONSECUENCIA: en este apartado se encuentra la descripción del efecto actual o futuro que tendrá las dependencias de no tomar las precauciones oportunas..

RECOMENDACIONES: se hace referencia a las descripciones correctivas de carácter preventivo que el equipo auditor ha presentado a las dependencias.

PROBABILIDAD E IMPACTO: hace referencia a la posibilidad de ocurrencia del riesgo y las consecuencias que puede ocasionar la materialización del riesgo

EVIDENCIAS: hace referencia de la descripción de los archivos que dan credibilidad al hallazgo.

Descripción del cuadro de Formato de Hallazgos.

TEXCOL	**HALLAZGOS**			**REF**
ENTIDAD AUDITADA	**TEXCOL LTDA.**			
OBJETO DE ESTUDIO	Funcionamiento Infraestructura tecnológica equipos de cómputo y red de datos			
RESPONSABLES	RONALD DARIO CERON ALEX ALBEIRO URBANO			
MATERIAL DE SOPORTE	COBIT			
DOMINIO		**PROCESO**		
HALLAZGO				
CONSECUENCIAS				
RECOMENDACIONES				
EVIDENCIAS				

Cuadro de Formato de Hallazgos:

Ver cuadro de anexos de hallazgos PO1

Ver cuadro de anexos de hallazgos PO3

Ver cuadro de anexos de hallazgos PO4

Ver cuadro de anexos de hallazgos PO5

Ver cuadro de anexos de hallazgos PO9

Ver cuadro de anexos de hallazgos AI2

Ver cuadro de anexos de hallazgos AI3

Ver cuadro de anexos de hallazgos AI5

Ver cuadro de anexos de hallazgos DS12

Ver cuadro de anexos de hallazgos ME2

5. INFORME EJECUTIVO

.San Juan de Pasto, 26 de febrero del 2016

Doctor:

MAURICIO LEON

Ingeniero Sistemas TEXCOL LTDA

REF: AUDITORIA DE SISTEMAS APLICADA LA INFRAESTRUCTURA TECNOLOGICA DE TEXCOL LTDA.

Cordial Saludo.

Como es de su conocimiento la infraestructura tecnológica de TEXCOL LTDA, fue sometida a una auditoria de sistemas para evaluar su funcionalidad, procesos y salidas de datos, de igual manera en lo referente a seguridad de la información.

Por otro lado, este documento contiene información la cual fue suministrada por los empleados y directivos TEXCOL LTDA.

Los resultados obtenidos fueron los siguientes.

Después de realizar las pruebas y la verificación de procedimientos realizados sobre la infraestructura tecnológica de TEXCOL LTDA se relacionan algunos aspectos favorables generales extraídos del informe de la presente auditoría.

- ✓ La auditoría se realizó con buena disposición por parte del personal encargado del manejo de la infraestructura tecnológica de TEXCOL LTDA
- ✓ La infraestructura tecnológica de TEXCOL LTDA Facilita el proceso intercambio de información y procesos en línea.

- ✓ La infraestructura tecnológica de TEXCOL LTDA Permite llevar de manera automatizada el Inventario.

- ✓ Por lo tanto se podría decir que la infraestructura tecnológica de TEXCOL LTDA tiene un funcionamiento adecuado del 60% y el restante 40% de la infraestructura tecnológica debe ser corregido y mejorado para lograr la optimización en esta área.

Oportunidades de mejoramiento

Administración de información:

- ✓ No existe un planes ni procesos documentados así como manuales de funciones diccionario de datos donde se recolecte, confirme y se especifique procedimientos procesos políticas de la compañía.

- ✓ No existe una debida capacitación del personal para conocer la infraestructura tecnológica de TEXCOL LTDA, su funcionamiento y las diferentes áreas de aplicación.

- ✓ No existen esquemas donde se definan niveles apropiados de seguridad y de controles de protección la infraestructura tecnológica de TEXCOL LTDA.

- ✓ Se hace uso inadecuado de la infraestructura tecnológica de TEXCOL LTDA

- ✓ Pérdida de la confidencialidad de la información la cual solo debe ser conocida por el ingeniero de sistemas y directivos.

Administrar recursos humanos:

- ✓ En la entidad no existe documentación técnica sobre el manejo la infraestructura tecnológica de TEXCOL LTDA, registro de funcionalidades o medidas en caso de errores.

- ✓ La falta de control en la administración de los privilegios de acceso genera fallas en la seguridad de la infraestructura tecnológica de TEXCOL LTDA.

Operación y uso del software:

- ✓ La falta de documentación técnica del software se presenta dependencia hacia el ingeniero de sistemas ya que él es el único que conoce a fondo el funcionamiento del software la infraestructura tecnológica de TEXCOL LTDA, por tal razón al presentarse inconvenientes es la única persona que puede ayudar a restablecer el servicio.

- ✓ La no existencia de manuales de usuario traerá inconsistencias en el manejo de la infraestructura tecnológica de TEXCOL LTDA. Y perjudicara al personal reemplazante o el nuevo personal.

- ✓ El personal encargado del soporte técnico de la infraestructura tecnológica de TEXCOL LTDA, no podrá guiarse ante dudas o inconvenientes con la infraestructura tecnológica de TEXCOL LTDA, ya que no posee las especificaciones de diseño de la red y del funcionamiento en general.

Actualizaciones: la falta de procedimientos para implementación de cambios en la infraestructura tecnológica de TEXCOL LTDA, genera desorden y pérdida de tiempo al no priorizar los cambios a realizar, falta de documentación y capacitación a los empleados lo que ocasiona lentitud a la hora de realizar sus labores ya que no se conoce el cambio realizado.

Planes de continuidad:

- ✓ La falta de un plan de contingencia formal expone a la entidad a fallas o interrupciones que harán que la compañía deje de prestar el servicio de calidad a sus usuarios o desestabilice el buen funcionamiento de la empresa.

- ✓ La ausencia de un plan de contingencia formal genera desinformación en los empleados los cuales no sabrán que decisiones tomar en caso de fallas y que acciones seguir cuando el sistema haya sido restaurado.
- ✓ Debido a la falta de un proceso de reanudación del servicio los operadores de la infraestructura tecnológica de TEXCOL LTDA, se presenta lentitud en el servicio y genera inconsistencias en los datos
- ✓ No existen usuarios y contraseñas para la identificación en el acceso al centro de cómputo del personal de la empresa y del personal exterior.
- ✓ Cualquier operario podría visualizar, modificar o eliminar la información perteneciente a la configuración de la red, generando así falta de integridad en la información.
- ✓ Los operarios de la institución no conocen medidas de prevención que se deben usar sobre los equipos de cómputo para evitar infecciones
- ✓ Perdida de información, daños en el hardware y/o software o mal funcionamiento y lentitud en el procesamiento de datos debido a daños o ataques al sistema informático ocasionado por software malicioso debido a falta de controles en el acceso a páginas no autorizadas de internet y programas de antivirus no instalados o actualizados en los equipos.

Atentamente;

RONALD DARIO CERON

Auditor Egresado Udenar

ALEX ALBEIRO URBANO

Auditor Egresado Udenar

INFORME GENERAL DE LA AUDITORIA

Hallazgos
REF: AUDITORIA INFORMATICA A LA INFRAESTRUCUTURA TECNOLOGICA DE LA EMPRESA TEXCOL LTDA. SEDE EN PASTO

Presente.

De nuestra consideración:

Nosotros, Ronald Darío Cerón y Alex Albeiro Urbano nos dirigimos a ustedes para darles a conocer el dictamen preliminar de la Auditoría practicada A LA INFRAESTRUCUTURA TECNOLOGICA DE LA EMPRESA TEXCOL LTDA. La misma que se ha llevado a cabo desde el 01 de Diciembre del 2015.

De los resultados obtenidos me permito informarle las siguientes observaciones:

1. Red física: en el Proceso de Auditoria Informática a la infraestructura tecnológica se encontró las siguientes falencias con respecto a la seguridad física.

Hallazgos en la seguridad física.

- No existe un grupo encargado de evaluar y estudiar el desempeño de la infraestructura tecnológica.
- No existen políticas ni procedimientos relacionados con la conformación adecuada de la arquitectura y a la infraestructura tecnológica.
- Inadecuada distribución y organización en la instalación de cables de datos y eléctricos en lugares públicos y transitados.
- No existe un plan de infraestructura tecnológica actualizado.
- No se lleva un control y una actualización del plan de infraestructura tecnológico, no está documentada.
- No se realizan simulacros con los planes de contingencia en caso de fallas de software o hardware de la red de datos.

- Existe un inventario del hardware de comunicaciones, pero no se encuentra actualizado ni documentado.
- No existe manual de funciones o procedimientos específico para los trabajadores encargados de la administración y mantenimiento de la infraestructura tecnológica.
- No existe dentro del manual de funciones la definición o descripción de los cargos relacionados con el manejo de la infraestructura tecnológica.
- No existen dentro del manual de funciones especificaciones de requisitos mínimos que deban cumplir las personas para ocupar los cargos relacionados con el manejo la infraestructura tecnológica
- No existe un plan de contingencia que se ejecute cuando se presente ausencia de los funcionarios encargados de manejar la infraestructura tecnológica.
- No existe software que se utilice para monitorear la conexión de la red de datos en su aspecto físico.
- No se tiene ningún tipo de software para monitorear la conexión física de la red de datos.
- No existe mantenimiento para software de monitoreo de la red física de datos
- En caso de falta del personal clave en la parte de Redes de datos TEXCOL LTDA, no se tiene planes de contingencia para su reemplazo en caso de ausencia O no está documentado.
- No se realiza un proceso de toma de decisiones que dé prioridad para la asignación de recursos a la adquisición de elementos tecnológicos que contribuyan con el mejoramiento de la Infraestructura tecnológica.
- No se han hecho simulacros al respecto de funcionarios clave del área de red de datos de TEXCOL LTDA.
- No se tiene actualizado ni documentado el plan de evaluación de riesgos del área de sistemas en Infraestructura tecnológica de TEXCOL LTDA.

- No existe un plan de contingencia para contrarrestar un evento que afecte la Infraestructura tecnológica no se encuentra debidamente documentado.
- No se cuenta con pólizas de seguros para el manejo del riesgo.
- existe la implementación del procedimiento de múltiples cotizaciones a diferentes proveedores dentro de las políticas para adquisición de hardware pero no está completamente documentadas.
- Las deficiencias en los niveles de servicio en cuanto a la red de datos de TEXCOL LTDA. No están identificadas.
- Faltan simulacros, en cuanto al cambio de servicios de red adquiridos con terceros.
- No existe documentación sobre las políticas de mantenimiento que se realiza a los equipos de cómputo.
- Los planes en caso de ataques físicos y lógicos de la red de datos de TEXCOL LTDA, no se encuentran documentados.
- No existe manual de funciones para el personal encargado de realizar mantenimiento preventivo y correctivo de los equipos de cómputo.
- No se tiene una implementación adecuada del centro de cómputo.
- No existe un diagrama o planos del cableado estructurado que se extiende por la entidad de la red de datos de TEXCOL LTDA.
- No se realiza seguimiento adecuado de los elementos como: servidores, routers y switches ya que las hojas de vida no recolectan la información necesaria.
- Existen políticas para el uso de los computadores conectados a la red de TEXCOL LTDA, pero no están documentadas
- No existe la instalación de dispositivos en el lugar donde se ubican los servidores (detectores humo, supresores de fuego) que permitan detectar y prevenir incendios.
- existe la instalación de cámaras que permitan monitorear el interior de las instalaciones de la entidad. Pero no están documentadas las políticas y sus operarios.

- Existe una parte de cableado de la red de datos que se encuentra con cables sueltos, fuera de canaletas, no sigue un estándar definido.
- Existen prohibiciones para fumar, consumir alimentos y bebidas, pero falta suficientes carteles en lugares visibles cerca a los switch y routers y falta documentarlas.
- No se tiene un plan de emergencia si falla los controles ambientales.
- No se Realizan simulacros con la planta eléctrica.
- No se tienen medidas implementadas en caso de falla del sistema de seguridad del área de sistemas de TEXCOL LTDA.
- No se compara periódicamente el desempeño de las metas en el área de Sistemas de TEXCOL LTDA.
- No se tienen políticas, estándares, procedimientos y metodologías de TI con requerimientos legales y regulatorios en TEXCOL LTDA.

Recomendaciones:

Hardware: de acuerdo a las falencias encontradas con respecto al Hardware, se

Expone las siguientes recomendaciones:

- Conformar un grupo determinado de funcionarios que evalúen y estudien el desempeño de la infraestructura tecnológica para que con ello tomen decisiones oportunas y adecuadas en la eventualidad de no cumplir objetivos planteados.
- Elaborar e implementar políticas y procedimientos relacionados con la conformación de la arquitectura y la infraestructura tecnológica para ajustar los servicios de red a las necesidades propias que necesite la entidad.
- Documentar el plan de infraestructura tecnológica, ya que de esta forma se lleva un registro del avance del mismo.
- Crear políticas que estén relacionadas con la búsqueda de nuevas tecnologías y elementos que mejoren el desempeño de la infraestructura tecnológica.

- Documentar los estudios que se realicen de nuevas tecnologías y elementos que mejoren el desempeño de la infraestructura tecnológica para lograr implementarlas en el futuro con mayor facilidad.
- Realizar simulacros de posibles fallas de software y hardware de la red de datos de TEXCOL LTDA, para estar preparados en caso de una falla real y saber si los procesos de contingencia planeados, son óptimos y eficaces en su desarrollo.
- Llevar un inventario documentado y actualizado de la infraestructura tecnológica de TEXCOL LTDA, ya que de esta forma se puede tener un control sobre los recursos con los que se cuenta y lo que se necesita a futuro, y manejar de la mejor manera los recursos con los que se cuenta dentro de la empresa.
- Documentar los cambios o mejoras al plan de infraestructura tecnológica, para así tener una mejor visión del logro de los mismos facilitar su difusión entre las partes interesadas, en cuanto a lo referente a estos procesos de mejoramiento tecnológico que desarrolla TEXCOL LTDA.
- Elaborar el manual de funciones o procedimientos específico para los trabajadores encargados del manejo y administración de la infraestructura tecnológica y con esto se oriente al personal para un óptimo funcionamiento y desempeño de las tareas que se deben realizar en este campo.
- Implementar dentro del manual de funciones o procedimientos para los trabajadores encargados del manejo y administración de la infraestructura tecnológica las descripciones o definiciones adecuadas, para no perder una guía concreta para la ejecución de tareas fundamentales.
- Ajustar los requerimientos mínimos para ocupar los cargos relacionados con el manejo de la infraestructura tecnológica, para cumplir con esto con el cumplimiento de perfiles ajustándose a la normatividad y lograr desempeño adecuado de los funcionarios.
- Elaborar un plan de contingencia que subsane la ausencia del personal encargado del manejo de la infraestructura tecnológica para evitar que los

procesos sean afectados y se asigne la responsabilidad de estas funciones a personas idóneas.

- Documentar y llevar registro de las prácticas para supervisar que los roles y responsabilidades de las funciones del personal se ejerzan de forma apropiada, para así evaluar el desempeño y las mejoras que se puedan presentar en caso de fallas, o debilidades encontradas, dentro de la Empresa TEXCOL LTDA.
- Tener planes de contingencia para el reemplazo del personal clave en la parte de Redes de datos en TEXCOL LTDA, para así evitar contratiempos, en cuanto al reemplazo y demoras en el sistema de la red de datos.
- Implementar un proceso de toma de decisiones donde se brinde la prioridad necesaria a la asignación de recursos para adquirir elementos tecnológicos que ayuden al mejoramiento de la infraestructura tecnológica y con ello optimizar los procesos informáticos de la entidad.
- Estudiar e implementar políticas donde se permita elaborar y administrar un buen presupuesto que sea utilizado para adquirir aquellos elementos tecnológicos necesarios para optimizar los procesos donde se involucre la infraestructura tecnológica.
- Elaborar políticas y procedimientos para el análisis y evaluación de riesgos del área de sistemas en la infraestructura tecnológica, ya que de esta manera se garantiza que los activos de la empresa estén correctamente valorados, protegidos y salvaguardados de acuerdo a su importancia y de acuerdo con los riesgos a los que se ven expuestos.
- Documentar el plan de seguridad informática, para evitar retrasos en el tiempo de respuestas, tener en claro el costo, tiempo y recursos necesarios en caso de pérdida o intrusión de agentes externos a la empresa TEXCOL LTDA y así lograr evitar tomar riesgos y retrasos innecesarios.
- Elaborar un plan de contingencia que ayude a dar soporte a la infraestructura tecnológica para obtener mecanismos que ayuden a la

recomponer y reactivar los procesos que se vean afectados para el sistema de red de datos.

- Obtener pólizas de seguros para el manejo del riesgo, tanto para personal como para la infraestructura tecnológica, para así tener un respaldo en caso de accidentes fortuitos que se puedan presentar dentro de la empresa TEXCOL LTDA.
- Adquirir software adecuado para monitorear la conexión física de la red de datos y con ello tener visión clara de la actividad de la red de datos.
- Llevar el proceso de mantenimiento periódico del software para monitoreo de la red física de datos y con ello asegurar el óptimo funcionamiento de esta herramienta.
- Documentar las políticas de adquisición de infraestructura tecnológica, para de esta manera poder controlar los riesgos que se puedan presentar en este proceso de adquisición.
- Llevar un registro de las fallas o anomalías para mantener un control de los servicio.
- Mantener registro documentado que ayuda a controlar mejor los servicios ya que se pueden tomar medidas correctivas de manera más exhaustiva si el problema persiste o se presenta continuamente.
- Llevar un plan de contingencia documentado en caso de ataques físicos o lógicos a la red de datos.
- Socializar entre los usuarios dicho plan de contingencia.
- Mantener una evaluación constante del plan de contingencia.
- Realizar capacitaciones para los usuarios de la red, para enseñar la manera de utilizar el plan de contingencia.
- Realizar un plan documentado de simulacro de ataques físicos y lógicos a la red teniendo en cuenta el tipo de ataque que se realiza, el software que utilizara y el área evaluada.

- Hacer una evaluación de los simulacros realizando una comparación, de manera que se compare si los posibles hallazgos encontrados fueron reparados o no sean realizadas las correcciones pertinentes.
- Documentar las políticas de mantenimiento de los equipos de cómputo para consolidar la guía del proceso a seguir y con ello agilizar las actividades correspondientes.
- Implementar el diligenciamiento de un acta o documento adecuado para facilitar el mantenimiento de los elementos de cómputo y así facilitar el trabajo a la persona encargada del proceso para la respectiva revisión y reparación.
- Implementar la documentación sobre el mantenimiento de los equipos de cómputo se permite actuar más rápido ante este tipo de eventos ya que se facilita por la recolección de antecedentes.
- Incorporar dentro del manual de funciones las actividades pertinentes para lo que concierne al mantenimiento de equipos de cómputo ya que así se optimizara este proceso debido a que se asigna responsabilidad directa.
- Implementar el centro de cómputo con características adecuadas y normatividad correspondiente para lograr optimización de procesos y seguridad de la información que es vital para la entidad.
- Implementar el proceso de mantenimiento de los elementos como: swiches, routers y servidores para garantizar su óptimo funcionamiento y cuidado ya que son elementos fundamentales en la constitución de la red de datos.
- Implementar el proceso específico para el mantenimiento de la red de datos y así se prevengan los sucesos que puedan perjudicar procesos que se relacionen con el sistema de red de datos.
- Implementar y ajustar la entidad a un correcto esquema de cableado estructurado para que no se atente contra la normatividad para alcanzar los objetivos de calidad que debe poseer la entidad por la importancia de la información que se maneja.

- Elaborar y Documentar los planos del cableado estructurado que se extiende por la entidad para tener facilidad de análisis al momento de una eventual toma de decisiones para mejorar el sistema de red de datos con incorporación de nuevos elementos en su aspecto físico.
- Elaborar hojas de vida adecuadas para recolectar información que sirva para el óptimo seguimiento de los equipos como: servidores, routers y switches y con ello prevenir y corregir inconvenientes a futuro.
- Documentar las políticas para el uso de los equipos de cómputo en el cual se debe detallar que tipo de software puede ser utilizado, además de una clara normatividad que evite que los usuarios instalen software no autorizado o desconocido.
- Además en este documento de debe incluir las políticas de cómo se deben utilizar los discos extraíbles como memorias USB para evitar que la red sea puesta en riesgo por atacantes externos, ya que las memorias pueden ser portadoras de virus que no están en la red y de esta manera infectar el equipo y poner en riesgo la red.
- Realizar la conexión y tendido del cableado en las sedes de acuerdo a los norma estándares **TIA/EIA 568-B-2, TIA/EIA 569-B, TIA/EIA 606A, TIA/EIA**
- **607 y TIA/EIA/TSB-67** para los ductos, pasos y espacios necesarios para la instalación de sistemas estandarizados de telecomunicaciones.
- Mantener una revisión constante del cableado, canaletas y puntos de conexión en las sedes para evitar cableado fuera de la norma estándar.
- Documentar los puntos de cableado donde se está encontrando daños, para saber el motivo que lo provoca y verificar si en ese punto se está realizando un posible sabotaje de la red.
- Crear políticas adecuadas en el campo de seguridad referente a la identificación, autenticación y autorización de los individuos que ingresan a las instalaciones para impedir que se atente contra los elementos de la entidad incluyendo los elementos que hacen parte del aspecto físico de la red de datos

- Implementar en la entidad políticas para dar mayor seguridad a las instalaciones ante cualquier evento natural o ambiental para disminuir los riesgos de desastres que atenten contra el óptimo desempeño y el aspecto físico en general de la red de datos.
- Aumentar el número de carteles en los lugares visibles, además de ser estrictos en cuanto al consumo de comida y bebidas cerca de los equipos.
- También se debe educar al personal para que no consuma comida cerca de los equipos y así prevenir deterioro de los mismos.
- Aumentar la señalización y seguridad cerca de los router y switch especialmente aquellos que se encuentran con acceso cercano a los usuarios de TEXCOL LTDA.
- Realizar un plan de simulacro de las plantas eléctricas UPS en el cual se tenga en cuenta, tiempo de carga de las baterías configuración y cantidad de equipos que debería respaldar.
- Documentar los posibles hallazgos, fallas o debilidades que se encuentren en el simulacro.
- Elaborar e implementar políticas y procedimientos adecuados para el monitoreo de la seguridad del aspecto físico de la red de datos para tener un seguimiento que ayude a generar procesos preventivos y correctivos.
- Implementar dentro de las políticas de monitoreo del aspecto físico de la red datos una descripción detallada de los procesos a trabajar, con ello se elaborara seguimientos óptimos y precisos que optimicen el funcionamiento de la infraestructura tecnológica.
- Contemplar el periodo en el que se deba realizar el monitoreo dentro de las políticas de la seguridad de la infraestructura tecnológica, para que el tiempo empleado sea el adecuado y se pueda realizar las respectivas prevenciones y correcciones.
- Asignar las funciones de monitorear la seguridad de la infraestructura tecnológica a personal específico, con ello se priorizara la ejecución de estas tareas y se sabrá quién responderá ante estas actividades.

- Documentar las políticas para seguridad de la red física de datos y con ello utilizar esta información como herramienta ágil para ejecutar este proceso.
- Dar a conocer a los funcionarios encargados de la administración de de la infraestructura tecnológica las políticas de monitoreo para el seguimiento de la seguridad del aspecto físico de la red de datos, para lograr ejecución dentro de lo correctivo y preventivo dentro de lo que atente al sistema de red de datos.

- Realizar auditorías de la infraestructura tecnológica para así lograr tener la visión más clara de la situación que presenta la red de datos y mejorar los aspectos que sean necesarios

Seguridad lógica

Hallazgos en la seguridad lógica:

- En el Proceso de Auditoria Informática a la infraestructura tecnológica de TEXCOL LTDA. se encontró las siguientes falencias con respecto a la seguridad lógica.
- El sistema operativo instalado en el servidor se encuentra desactualizado.
- El sistemas operativos instalados en equipos de cómputo no están debidamente licenciados así como los paquetes ofimáticos y de seguridad antivirus se encuentra desactualizados.
- No existe una correcta segmentación de la red de datos.
- El software contable de TEXCOL LTDA. no está protegido.

Recomendaciones:

- Actualizar el sistema operativo WINDOWS SERVER instalado en el servidor de TEXCOL LTDA migrar a una la versión más reciente.
- Segmentar la red de datos de TEXCOL LTDA para aumentar la seguridad de la red, dividiéndola por departamentos, de manera que un intruso en caso de ataque solo pueda tener acceso a una sola área de la empresa y no a toda la red de datos.

- Legalizar la compra de licencias de sistemas operativos paquetes ofimáticos y de seguridad antivirus.

CONCLUSIONES

Con el desarrollo de este trabajo de grado, se logró auditar la infraestructura tecnológica de TEXCOL LTDA, identificando los riesgos y amenazas que presenta la empresa en cuanto a este aspecto, y dando las correspondientes recomendaciones pertinentes, para de esta manera hacer que la empresa brinde su servicio de una manera óptima y eficiente en cuanto a la parte de la red de datos que maneja.

El presente trabajo realizado en la empresa TEXCOL LTDA reveló la situación actual en la que se encuentra.

Una vez aplicado el análisis de riesgos a los recursos TEXCOL LTDA se pudo conocer las amenazas, vulnerabilidades, que probabilidades hay de que ocurra, el nivel de riesgo al que está sujeto los recursos informáticos y nivel de impacto que ocasionaría cumpliendo con los objetivos impuestos en el inicio del trabajo.

Los hallazgos de auditoria, cuestionarios de control interno, entrevistas y pruebas han sido herramientas apropiadas para la obtención de resultados que muestran las falencias a ser consideradas dentro del mejoramiento constante de la empresa TEXCOL LTDA.

El trabajo aportó una visión clara sobre la importancia de la AUDITORIA Y SEGURIDAD EN SISTEMAS centrado en la infraestructura tecnología de la empresa TEXCOL LTDA. Respecto al tiempo dedicado para realizar este trabajo no podemos estimar con precisión las horas invertidas puesto que ha habido meses en los que hemos dedicado gran cantidad de horas y otros que por diversos motivos, no han sido tantas como hubiésemos querido.

Se invirtió una gran cantidad de horas en el comienzo de este trabajo para hacernos una idea de qué se iba a plasmar en este documento y en leer abundante documentación para que la información fuera lo más rigurosa posible. Para concluir, solamente destacar que se hizo una valoración positiva de los

conocimientos aprendidos y puestos en práctica a través de este duradero y arduo trabajo, que ha hecho que su propia finalización supusiera un verdadero reto personal, estas son nuestras conclusiones:

- La auditoría de sistemas es una herramienta la cual permite conocer de manera profunda el funcionamiento de cualquier empresa o área la cual se objetó de nuestro estudio por medio de evaluación de los procesos, técnicas, política, normas con el fin de encontrar vulnerabilidades de seguridad tanto a nivel físico como lógico, para poder realizar recomendaciones y planes de mejoramiento para cubrir estas falencias.
- La empresa TEXCOL LTDA desde la gerencia hasta los funcionarios del área de sistemas son conscientes de que existen falencias las cuales quedan demostradas en este estudio..
- La empresa TEXCOL LTDA debe de dar mayor prioridad al área de sistemas por ser esta un pilar fundamental en todos los procesos que se realizan en la entidad, ya que como queda descrito en este documento ni siquiera aparece en el organigrama institucional.
- Se deja a disposición de La empresa TEXCOL LTDA los hallazgos y recomendaciones, las cuales son necesarias para continuar con el proceso de mejoramiento.
- Se debe buscar el mejoramiento continuo de la entidad por medio de nuevas auditorías a otras áreas.

RECOMENDACIONES

La información de la empresa, se ha convertido en un Activo Real de la misma, como sus Stocks o materias primas si las hay. Por ende, han de realizarse inversiones informáticas con planificación y estrategias.
Generalmente una empresa que presenta problemas en alguno de sus desarrollos de procesos presenta síntomas de necesidad de una auditoría informática, las empresas acuden a las auditorías externas cuando existen síntomas bien perceptibles de debilidad. Estos síntomas pueden agruparse en clases:

- **Síntomas de descoordinación y desorganización**:
    - ✓ No coinciden los objetivos de la Informática de la Compañía y de la propia Compañía.
    - ✓ No se atienden las peticiones de cambios de los usuarios.
    - ✓ No se reparan las averías de Hardware ni se resuelven incidencias en plazos razonables.
    - ✓ El usuario percibe que está abandonado y desatendido.
    - ✓ No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de Aplicaciones críticas y sensibles.
- **Síntomas de debilidades económico-financiero**:
    - ✓ Incremento desmesurado de costes.
    - ✓ Necesidad de justificación de Inversiones Informáticas (la empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).
    - ✓ Desviaciones Presupuestarias significativas.
    - ✓ Costes y plazos de nuevos proyectos (deben auditarse simultáneamente a Desarrollo de Proyectos y al órgano que realizó la petición).
- **Síntomas de Inseguridad: Evaluación de nivel de riesgos:** continuidad del Servicio. Es un concepto aún más importante que la Seguridad. Establece las estrategias de continuidad entre fallos mediante Planes de Contingencia* Totales y Locales.

BIBLIOGRAFIA

- ECHENIQUE GARCIA José A., Auditoria en informática, 2ª Ed., Mc GRAW-HILL, Mexico D.F., 2005.

- GUSTIN Enith, SOLARTE Francisco Javier, HERNANDEZ Ricardo. Manual De Procedimientos para Llevar a la Práctica La Auditoría Informática y de Sistemas, Copyright © 2011.

- INGENIERO FRANCISCO NICOLAS SOLARTE SOLARTE. (Septiembre de 2010) Auditoria Informática y de Sistemas. Retrieved from http://auditordesistemas.blogspot.com/

- Murillo, Enrique (26 de marzo de 2013). «La Función del Auditor» (en español). AOB News. Consultado el 26 de marzo de 2013. Retrieved from. http://es.wikipedia.org/wiki/Auditor

- PIATTINI Mario, DEL PESO Emilio, Auditoría en informática: un enfoque práctico, 2ª Ed., Alfaomega/RA-MA, México D.F., 2001.

- PINILLA F. José D., Auditoría informática: un enfoque operacional, ECOE, Bogotá, 1995

- ROBERTO GÓMEZ LÓPEZ. Doctor en Economía (Dirección y Administración de Empresas). Retrieved from
- http://ucapanama.org/wp-content/uploads/2011/12/Generalidades-en-la-Auditoria.pdf.

BIBLIOWEB

- ISACA, COBIT 4.1 Castellano (En línea). En: ISACA Colombia (Bogotá). Disponible en la dirección electrónica: http://www.isaca-bogota.net/metodologias/cobit.aspx 281

- PARRA GALVIS, Andrés Felipe. Auditoria de sistemas de información (en línea). En: Guía Laboral Gerencie 2009: Agosto 27, 2008. Disponible en la dirección electrónica: http://www.gerencie.com/auditoria-de-sistemas-de-informacion.html

- WIKIPEDIA. Objetivos de control para la información y tecnologías relacionadas (En línea). En: Wikipedia La enciclopedia Libre. Disponible en la dirección electrónica: http://es.wikipedia.org/wiki/COBIT

- http://www.monografias.com/trabajos39/la-auditoria/la-auditoria.shtml

- http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica

ANEXOS

La información presentada en los diferentes anexos se encuentra debidamente clasificada en el dispositivo magnético y en la memoria USB presentada.

- ANEXO 1 FOTOGRAFICO
- ANEXO 2 ENTREVISTAS
- ANEXO CUESTIONARIOS Y ENTREVISTAS
- ANEXO CUADRO CUANTITATIVO
- ANEXO CUADRO DE HALLAZGOS
- ANEXO CUADRO CUESTIONARIOS DE CONTROL

GLOSARIO

Amenaza: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: Según [ISO/IEC Guía 73:2002]: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Auditoría: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

COBIT (Objetivos de Control de las Tecnologías de la Información y Tecnologías Relacionadas) Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información, actualizados, internacionales y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida.

Conexión física: Permiten a las computadoras transmitir y recibir señales directamente. Las conexiones físicas están definidas por el medio empleado (pueden ser cables hasta satélites) para transmitir la señal, por la disposición geométrica de las computadoras (topología) y por el método usado para compartir información, desde textos, imágenes y hasta videos y sonidos.

Factibilidad: Es la disponibilidad de los recursos necesarios para llevar a cabo los objetivos o metas señaladas, sirve para recopilar datos relevantes sobre el desarrollo de un proyecto y en base a ello tomar la mejor decisión.

Infraestructura tecnológica: Es el conjunto de hardware y software sobre el que se asientan los diferentes servicios que una empresa necesita tener en funcionamiento para poder llevar a cabo todas sus actividades.

ISACA: Information Systems Audit and Control Association. Publica COBIT y emite diversas acreditaciones en el ámbito de la seguridad de la información.

Plan de contingencia: Es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudara a controlar una situación de emergencia y minimizar sus consecuencias negativas.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.