AUDITORIA A LOS PROCESOS DEL SISTEMA INFORMÁTICO Y DE INFORMACIÓN DE LA EMPRESA DE TRANSPORTE TRANSANDES S.A.S DE LA CIUDAD DE IPIALES – NARIÑO.

EDWARD CAMILO MUÑOZ ORDOÑEZ
EDWIN ROBERT VELASCO MEJIA

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

AUDITORIA A LOS PROCESOS DEL SISTEMA INFORMÁTICO Y DE INFORMACIÓN DE LA EMPRESA DE TRANSPORTE TRANSANDES S.A.S DE LA CIUDAD DE IPIALES – NARIÑO.

EDWARD CAMILO MUÑOZ ORDOÑEZ
EDWIN ROBERT VELASCO MEJIA

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

Asesor:
MANUEL BOLAÑOS GONZALEZ
Ingeniero de Sistemas

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERIA
PROGRAMA INGENIERIA 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 por el Honorable Concejo 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 priman las normas sobre el derecho de autor”.

Artículo 13, Acuerdo N. 005 de 2010 emanado del Honorable Consejo Académico.

NOTA DE ACEPTACIÒN

_____

_____

_____

_____
Jurado

_____
Jurado

San Juan de Pasto, marzo 7 de 2016

AGRADECIMIENTOS

Agradezco en primer lugar a Dios y a mi Virgencita de Las Lajas, por bendecirme para llegar hasta donde he llegado, porque mis oraciones hicieron realidad este sueño tan anhelado.

A mi esposa, Patricia Almeida y a mis hijos Sol Ángela y Cristian Camilo, por motivarme a que continúe con mis estudios y de esta manera ser parte de los profesionales de la Universidad de Nariño, sin la ayuda de ellos este logro no tendría valor.

A la Universidad de Nariño, por darme nuevamente la oportunidad de terminar mis estudios y formarme como un profesional, gracias al Acuerdo de Titulación Exitosa.

A mi Asesor del trabajo de grado, Ingeniero Manuel Bolaños, por su esfuerzo y dedicación, quien con sus conocimientos, su experiencia, su paciencia y su motivación ha logrado en mí que pueda terminar mis estudios con éxito.

También me gustaría agradecer a mis maestros durante toda mi carrera profesional porque todos han aportado con un granito de arena a mi formación, en especial a los Ingenieros: Ing. Delio Gómez, Ing. Ricardo Timarán, Ing. Manuel Dolores (Q.E.P.D.), Ing. Nelson Jaramillo, Ing. Manuel Bolaños, Ing. Francisco Solarte, Ing. Edgar Dulce, Ing. Juan Carlos Castillo.

A todos los familiares, compañeros, amigos, conocidos que me animaron a que terminara mis estudios como Ingeniero de Sistemas, a todos ellos muchas gracias y que Dios los bendiga.

Edward Camilo Muñoz Ordoñez

AGRADECIMIENTOS

Primero doy gracias a Dios, por regalarme la oportunidad de tener tan buena experiencia dentro de la Universidad de Nariño, gracias a mi Universidad por darme la posibilidad de convertirme en el profesional que tanto me apasiona, gracias a cada maestro que hizo parte de este proceso integral de formación.

A mi hermosa familia. Hasta ahora no ha sido sencillo el camino, pero gracias a sus aportes y amor, a su inmensa bondad y apoyo, lo complicado de lograr esta meta se ha notado menos. Les agradezco, y hago presente mi gran afecto hacia ustedes.

Finalmente, un sincero agradecimiento a la Empresa de Transporte TRANSANDES S.A.S por permitirnos desarrollar esta investigación en sus instalaciones y por brindarnos toda la información y recursos necesarios para llevar a cabo esta auditoría.

Edwin Robert Velasco Mejía

DEDICATORIA

A Dios,
por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

A mi Esposa e Hijos,
por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.

A mis padres,
por haberme ayudado a iniciar mis estudios de ingeniería de sistemas.

A mis maestros,
Ing. Francisco Solarte, Ing. Juan Carlos Castillo, Ing. Edgar Dulce, Ing. Ricardo Timarán, Ing. Manuel Bolaños e Ing. Nelson Jaramillo, por su gran apoyo y motivación para la culminación de nuestros estudios profesionales.

A mí Asesor,
Ing. Manuel Bolaños, por su apoyo ofrecido en este trabajo, por su tiempo compartido y por impulsar el desarrollo de nuestra formación profesional.

Edward Camilo Muñoz Ordoñez

DEDICATORIA

A mis padres, que han sabido formarme con buenos sentimientos, hábitos y valores, lo cual me ha ayudado a salir adelante en los momentos más difíciles.

A mi hermano Fidernando, quien siempre ha estado junto a mí brindándome su apoyo, muchas veces desempeñando el papel de padre.

A mi esposa Yesenia, quien me ha dado la fortaleza para levantarme y continuar cuando he estado a punto de caer, por motivarme con su constante amor a alcanzar mis anhelos.

A mis amados hijos: Luisa, José, Santiago, por ser mi fuente de motivación e inspiración para poder superarme cada día más y así poder luchar para que la vida nos depare un futuro mejor.

Edwin Robert Velasco Mejía

RESUMEN

Este trabajo de grado trato sobre la auditoría a los procesos del sistema de información de la empresa de transporte TransAndes S.A.S de la ciudad de Ipiales – Nariño, utilizando el estándar COBIT, para poder identificar posibles vulnerabilidades, amenazas y riesgos dentro del sistema de información de la empresa, tanto en la seguridad física, seguridad lógica, implementando las buenas prácticas en los procesos del sistema, además de proponer controles para el manejo óptimo de la información correspondiente a las tecnologías de la información y de esta manera cumplir de manera efectiva con los objetivos de la empresa.

Después de realizar un conocimiento de la empresa, y teniendo en cuenta las herramientas para la recolección de información como son las encuestas, entrevistas, listas de chequeo entre otras, se determinaron o seleccionaron los dominios y procesos que involucran al sistema de información de la empresa de transporte TransAndes S.A.S., evidenciando unos hallazgos y determinando de esta manera unas recomendaciones.

Los resultados obtenidos se presentaron en un informe final y ejecutivo con las recomendaciones de cada uno de los hallazgos.

ABSTRACT

This degree work dealt with the audit processes of the information system of the transport company TransAndes S.A.S. of Ipiales-Nariño, using the COBIT standard, to identify potential vulnerabilities, threats and risks within the system of company information, both in physical and logical security, implementing good practices in system processes, and proposing controls for optimal management of the information technology and thus effectively fulfill with company goals.

After performing knowledge of the company, and having into account the tools for collecting information such as surveys, interviews, checklists among other, were determined and selected domains and processes involving the information system of the transport company TransAndes S.A.S., highlighting some findings and determining some recommendations.

The resulted obtained were presented in a final report and executive with recommendations for each of the findings.

TABLA DE CONTENIDO

Pág.

LISTADO DE FIGURAS

Pág.

LISTADO DE TABLAS

Pág.

GLOSARIO

- **Acción correctiva:** es aquella que llevamos a cabo para eliminar la causa de un problema.

- **Acción preventiva:** se anticipan a la causa, y pretenden eliminarla antes de su existencia. Evitan los problemas identificando los riesgos. Cualquier acción que disminuya un riesgo es una acción preventiva.

- **Activo:** en relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Según [ISO/IEC 13335-1:2004]: Cualquier cosa que tiene valor para la organización.

- **Alerta:** una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

- **Amenaza:** según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

- **Análisis de riesgos cualitativo:** análisis de riesgos en el que se usa una escala de puntuaciones para situar la gravedad del impacto.

- **Análisis de riesgos cuantitativo:** análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

- **Análisis de riesgos:** según [ISO/IEC Guía 73:2002]: uso sistemático de la información para identificar fuentes y estimar el riesgo.

- **Aplicación:** aunque se suele utilizar indistintamente como sinónimo genérico de 'programa' es necesario subrayar que se trata de un tipo de programa específicamente dedicado al proceso de una función concreta dentro de la empresa.

- **Archivo de datos:** cualquier archivo creado dentro de una aplicación: por ejemplo, un documento creado por un procesador de textos, una hoja de cálculo, una base de datos o un gráfico. También denominado documento.

- **Archivo de programa:** archivo ejecutable que inicia una aplicación o programa. Los archivos de programa tienen las extensiones EXE, PIF, COM o BAT.

- **Auditor:** persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

- **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.

- **Autenticación:** proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

- **Backup:** acción de copiar archivos o datos de forma que estén disponibles en caso de que un fallo produzca la perdida de los originales. Esta sencilla acción evita numerosos, y a veces irremediables problemas si se realiza de forma habitual y periódica.

- **Bases de Datos:** colección de datos organizada de tal modo que el ordenador pueda acceder rápidamente a ella. Una base de datos relacionar es aquella en la que las conexiones entre los distintos elementos que forman la base de datos están almacenadas explícitamente con el fin de ayudar a la manipulación y el acceso a éstos.

- **Bitácoras:** es como el "diario" de algunos programas donde se graban todas las operaciones que realizan, para posteriormente abrirlos y ver qué es lo que ha sucedido en cada momento.

- **Centro de cómputo:** es un área de trabajo cuya función es la de concentrar, almacenar y procesar los datos y funciones operativas de una empresa de manera sistematizada.

- **Checklist:** lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

- **Cliente:** cliente o 'programa cliente' es aquel programa que permite conectarse a un determinado sistema, servicio o red.

- **Cliente-Servidor:** se denomina así al binomio consistente en un programa cliente que consigue datos de otro llamado servidor sin tener que estar obligatoriamente ubicados en el mismo ordenador. Esta técnica de consulta 'remota' se utiliza frecuentemente en redes como 'Internet'.

- **COBIT:** (control objetives for information and related technology) objetivos de control para la información y tecnología relacionadas. Publicados y mantenidos

por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de tecnología de información, aceptados para ser empleados por gerentes de empresas y auditores.

- **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.

- **Confidencialidad:** acceso a la información por parte únicamente de quienes estén autorizados. Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

- **Control correctivo:** control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

- **Control preventivo:** control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

- **Control Interno:** las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una garantía razonable de que los objetivos del negocio se alcanzarán y de que los eventos indeseables serán prevenidos o detectados y corregidos.

- **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.

- **COSO:** el modelo COSO define el control interno como un conjunto de procesos, realizado por los directivos de una organización, y creado para garantizar el logro de los objetivos.

- **Criptografía:** ciencia dedicada al estudio de técnicas capaces de conferir seguridad a los datos. El cifrado es fundamental a la hora de enviar datos a través de las redes de telecomunicaciones con el fin de conservar su privacidad.

- **Datos:** término general para la información procesada por un ordenador.

- **Desastre:** cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante

el tiempo suficiente como para verse la misma afectada de manera significativa.

- **Disponibilidad:** acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Según [ISO/IEC 13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

- **Dominio:** agrupación de objetivos de control en etapas lógicas en el ciclo de vida de inversión de TI.

- **Equipo auditor:** grupo de personas encargadas de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

- **Evaluación de riesgos:** según [ISO/IEC guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

- **Evento:** según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad.

- **Evidencia objetiva:** información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

- **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.

- **Gestión de riesgos:** proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

- **Gestión de claves:** controles referidos a la gestión de claves criptográficas.

- **Hardware:** Conjunto de dispositivos de los que consiste un sistema. Comprende componentes tales como el teclado, el mouse, las unidades de disco y el monitor.

- **Impacto:** el coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros ej., pérdida de reputación, implicaciones legales, etc.

- **Incidente:** según [ISO/IEC TR 18044:2004]: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Información:** en sentido general, es todo lo que reduce la incertidumbre y sirve para realizar acciones y tomar decisiones.

- **Infraestructura:** la tecnología, los recursos humanos y las instalaciones que permiten el procesamiento de las aplicaciones.

- **Institución:** un grupo de individuos que trabajan para un fin común, por lo general dentro del contexto de una forma organizacional, como una corporación agencia pública, institución de caridad o fondo.

- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

- **Internet:** interconexión de redes informáticas que permite a las computadoras conectadas comunicarse directamente.

- **Inventario de activos:** lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

- **IP:** acrónimo de internet. Es el protocolo que facilita la comunicación entre ordenadores conectados a la red internet. Cada ordenador en internet tiene una dirección IP única, que le identifica dentro de la red y permite su localización para posibilitar la comunicación.

- **ISACA:** (information systems audit and control association) asociación de auditoría y control de los sistemas de información. Publica COBIT y emite diversas acreditaciones en el ámbito de la seguridad de la información.

- **ISO 17799:** código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su

vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de julio de 2007. No es certificable.

- **ISO 19011:** "guidelines for quality and/or environmental management systems auditing". Guía de utilidad para el desarrollo de las funciones de auditor interno para un SGSI.

- **ISO 27001:** estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005.

- **ISO 27002:** código de buenas prácticas en gestión de la seguridad de la información (trascripción de ISO 17799). No es certificable. Cambio de oficial de nomenclatura de ISO 17799:2005 a ISO 27002:2005 el 1 de julio de 2007.

- **ISO 9000:** normas de gestión y garantía de calidad definidas por la ISO.

- **ISO:** (international organization for standardization) organización internacional para la normalización. Organización de carácter voluntario fundada en 1946 que es responsable de la creación de estándares internacionales en muchas áreas, incluyendo la informática y las comunicaciones.

- **LAN (local área network - red de area local):** interconexión de computadoras y periféricos para formar una red dentro de una empresa u hogar, limitada generalmente a un edificio.

- **Lenguaje:** en informática, conjunto de caracteres e instrucciones utilizadas para escribir programas de ordenador.

- **Magerit:** estándar para el análisis y gestión de riesgos de los sistemas de la información.

- **Mantenimiento Correctivo:** medida de tipo reactivo orientada a eliminar la causa de una no-conformidad, con el fin de prevenir su repetición.

- **Mantenimiento Preventivo:** medida de tipo pro-activo orientada a prevenir potenciales no-conformidades.

- **MECI:** modelo estándar de control interno.

- **Metodología:** conjunto de métodos utilizados en la investigación científica

- **Norma:** principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

- **Objetivo de control:** un estatuto del resultado o propósito que se desea alcanzar al implantar procedimientos de control en un proceso en particular.

- **Objetivo:** declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad de TI determinada.

- **Organización:** conjunto de personas e instalaciones con una disposición de responsabilidades, autoridades y relaciones. Una organización puede ser pública o privada.

- **Papeles de trabajo:** registra el planeamiento, naturaleza, oportunidad y alcance de los procedimientos de auditoría aplicados por el auditor y los resultados y conclusiones extraídas a la evidencia obtenida. Se utilizan para controlar el progreso del trabajo realizado para respaldar la opinión del auditor. Los papeles de trabajo pueden estar constituidos por datos conservados en papel, película, medios electrónicos u otros medios.

- **Password:** conocida también como 'clave de acceso'. Palabra o clave privada utilizada para confirmar una identidad en un sistema remoto que se utiliza para que una persona no pueda usurpar la identidad de otra.

- **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.

- **Plan estratégico de TI:** un plan a largo plazo, describe de forma cooperativa como los recursos de TI contribuirán a los objetivos estratégicos empresariales (metas).

- **Política de seguridad:** documento que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:2005]: intención y dirección general expresada formalmente por la dirección.

- **Procedimiento:** forma especificada para llevar a cabo una actividad o un proceso. Método o sistema estructurado para la ejecución de actividades. En computación, una subrutina o subprograma, como idea general, se presenta como un algoritmo separado del algoritmo principal, el cual permite resolver una tarea específica.

- **Proceso:** conjunto de operaciones lógicas y aritméticas ordenadas, cuyo fin es la obtención de resultados. Por lo general, un conjunto de procedimientos influenciados por las políticas y estándares de la organización, que toman las entradas provenientes de un número de fuentes, incluyendo otros procesos,

manipula las entradas, y genera salidas, incluyendo a otros procesos, para los clientes de los procesos. Los procesos tienen razones claras de negocio para existir, propietarios responsables, rol claro y responsabilidades alrededor de la ejecución del proceso, así como los medios para medir el desempeño.

- **Programa:** secuencia de instrucciones que obliga al ordenador a realizar una tarea determinada.

- **Red:** servicio de comunicación de datos entre ordenadores. Conocido también por su denominación inglesa: 'network'. Se dice que una red está débilmente conectada cuando la red no mantiene conexiones permanentes entre los ordenadores que la forman. Esta estructura es propia de redes no profesionales con el fin de abaratar su mantenimiento.

- **Repositorio:** donde se almacenan los elementos definidos o creados por la herramienta, y cuya gestión se realiza mediante el apoyo de un sistema de gestión de base de datos (SGBD) o de un sistema de gestión de ficheros.

- **Riesgo residual:** según [ISO/IEC guía 73:2002] El riesgo que permanece tras el tratamiento del riesgo.

- **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.

- **Router:** es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un router (mediante bridges), y que por tanto tienen prefijos de red distintos.

- **Segregación de tareas:** reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

- **Seguridad de la información:** según [ISO/IEC 27002:2005]: preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

- **Selección de controles:** proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

- **Servidor:** ordenador que ejecuta uno o más programas simultáneamente con el fin de distribuir información a los ordenadores que se conecten con él para dicho fin. Vocablo más conocido bajo su denominación inglesa 'server'.

- **Sistema de información:** se denomina Sistema de Información al conjunto de procedimientos manuales y/o automatizados que están orientados a proporcionar información para la toma de decisiones.

- **Software:** componentes inmateriales del ordenador: programas, sistemas operativos, etc.

- **Switch:** dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

- **Técnica:** la técnica es el procedimiento o el conjunto de procedimientos que tienen como objetivo obtener un resultado determinado, ya sea en el campo de la ciencia, de la tecnología, de las artesanías o en otra actividad

- **TI:** tecnologías de información

- **Tratamiento de riesgos:** según [ISO/IEC guía 73:2002]: proceso de selección e implementación de medidas para modificar el riesgo.

- **Usuario:** una persona o una entidad externa o interna que recibe los servicios empresariales de TI.

- **Valoración de riesgos:** según [ISO/IEC Guía 73:2002]: proceso completo de análisis y evaluación de riesgos.

- **Virus:** programa que se duplica así mismo en un sistema informático incorporándose a otros programas que son usados por varios sistemas.

- **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.

INTRODUCCIÓN

Actualmente los sistemas de información son la base de las organizaciones, instituciones, entidades y empresas, el grado de responsabilidad reposa en los sistemas, datos e información encaminados al logro de los objetivos internos, estos se pueden mejorar y mantener teniendo una adecuada sistematización y documentación.

El manejo de la información abarca aspectos que van desde el tratamiento de documentos en medio físico como el proceso de almacenamiento y recuperación, hasta los sistemas de información que tenga la organización o sistemas externos a los que esté obligada a reportar información, pasando por aspectos tan importantes como la forma de almacenamiento de los datos digitales, modelos de respaldo de información y planes de contingencia o de continuidad del negocio, incluyendo además los sistemas físicos de seguridad y accesibilidad a sitios o áreas restringidas.

Se tiene la falsa percepción de que la seguridad de la información es una tarea imposible de aplicar, pero se debe tener muy claro que no existen sistemas cien por ciento seguros, porque el costo de la seguridad total es muy alto y las organizaciones no están preparadas para hacer este tipo de inversión.

Es por esto que los activos de información han pasado a formar parte de la actividad cotidiana de organizaciones e individuos, con esfuerzo, el conocimiento necesario y el apoyo constante de las directivas se puede alcanzar un nivel de seguridad razonable.

La empresa de transportes TransAndes S.A.S. de la ciudad de Ipiales, es una entidad en crecimiento que debe involucrar dentro de sus procesos buenas prácticas encaminadas a la protección de la información, por lo cual es necesario el desarrollo del análisis de riesgos de la seguridad de la información aplicado a cada uno de los activos de la información, que permite conocer las debilidades y fortalezas internas encaminadas en la generación de los controles adecuados y normalizados dentro de las políticas de seguridad informática que hacen parte de un sistema de gestión de seguridad de la información (SGSI).

IDENTIFICACION DEL PROBLEMA

TITULO DEL PROYECTO

AUDITORIA A LOS PROCESOS DEL SISTEMA INFORMÁTICO Y DE INFORMACIÓN DE LA EMPRESA DE TRANSPORTE TRANSANDES S.A.S DE LA CIUDAD DE IPIALES – NARIÑO.

TEMA

Auditoria aplicada al área de sistemas, en los procesos del sistema informático y de información de la empresa de transportes TransAndes S.A.S. de la ciudad de Ipiales – Nariño.

MODALIDAD

Este trabajo de grado, corresponde a la modalidad de TRABAJO DE APLICACION, a realizarse en la empresa de transportes TransAndes S.A.S. de la ciudad de Ipiales – Nariño. Trabajo que permitirá acrecentar conocimiento y generar diferentes alternativas de desarrollo empresarial por medio de la aplicación de métodos organizacionales, de funcionamiento, aplicación y cumplimiento de políticas, leyes y normas, necesarias para el funcionamiento de una empresa.

LINEA DE INVESTIGACION

Según las líneas de investigación aprobadas y definidas en el Programa de Ingeniería de Sistemas de la Universidad de Nariño, como Acuerdo de Facultad No. 045 de octubre 10 de 2002, dado por el Concejo de Facultad, el proyecto corresponde a la línea de investigación de sistemas computacionales, ya que esta línea tiene como objetivo planificar, diseñar, implantar, administrar y evaluar sistemas computacionales y servicios basados en estos sistemas complejos de información, la cual soporta la temática de auditoria de sistemas.

DEFINICION DEL PROBLEMA

PLANTEAMIENTO DEL PROBLEMA

La empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales no posee un sistema de seguridad de la información que permita la gestión de vulnerabilidades, amenazas y riesgos a las que se ve expuesto cada uno de los procesos internos, no se cuenta con un estándar de controles que lleven a contrarrestar delitos informáticos sobre los datos, comprometiendo la integridad, confidencialidad y disponibilidad de la información.

Los procedimientos existentes en la empresa de transporte TransAndes S.A.S. son ejecutados por iniciativa propia de cada uno de los usuarios del sistema, no existe una documentación específica de las funciones del personal en los procedimientos administrativos y del sistema de gestión seguridad de la información (SGSI).

Dentro de la empresa de transporte TransAndes S.A.S, se pueden evidenciar problemas como: la mala instalación eléctrica, hardware que ha cumplido su vida útil, instalación de software no permitido en los equipos, desorganización en al archivo físico de reportes, entre otros.

La empresa de transporte TransAndes S.A.S. tiene muchos inconvenientes dentro del manejo de la información, debido a que ha ido creciendo paulatinamente y no se ha tomado conciencia de la importancia de asegurar la información existente; en este rápido y cambiante mundo de los negocios, la tecnología de información juega un papel imprescindible, en casi todas las organizaciones, se ha convertido en la base de mejor productividad, mayor calidad, menos tiempo de respuesta, que sin lugar a duda son piezas clave para el éxito de toda organización.

OBJETIVOS

OBJETIVO GENERAL

Desarrollar procesos de evaluación al sistema informático y de información de la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales, Nariño con el propósito de identificar las vulnerabilidades, amenazas y riesgos.

OBJETIVOS ESPECÍFICOS

- Conocer los procesos que afectan la seguridad informática y de la información con vulnerabilidades, amenazas y riesgos en la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales, Nariño.

- Planificar una auditoria, en la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales, Nariño para establecer los controles de seguridad informática y de la información.

- Proponer acciones y estrategias para la ejecución de los controles de seguridad informática y de la información en la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales, Nariño

- Presentar informe final de resultados donde se establecerán los controles, hallazgos y recomendaciones para la empresa de trasporte TransAndes S.A.S. de la ciudad de Ipiales

JUSTIFICACIÓN

La empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales, tiene una infraestructura tecnológica en crecimiento, de la cual dependen muchos de los procesos, dependencias y el funcionamiento administrativo. Gran parte de la información de la empresa, se encontró en los equipos del personal administrativo, otra parte en los buzones de correo, también se evidenció la existencia de información en formato físico y por último la que se encuentra almacenada en sistemas de información, pero se halló que no hay políticas de control que puedan proveer un adecuado tratamiento de este valioso activo como es la información sensible de la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales.

En la actualidad la empresa debe considerar dentro de sus planes el aseguramiento de la información generando políticas y controles en busca de garantizar la continuidad del negocio, la empresa debe tomar conciencia de la necesidad de asegurar el flujo de información, optimizar recursos y garantizar la confidencialidad, disponibilidad e integridad de la misma.

Este es uno de los retos que debe asumir la empresa para estar acorde a los modelos y estándares actuales, para ello fue necesario empezar con la ejecución análisis de riesgos de la seguridad de la información que en un futuro será la base para implementar el sistema de gestión de seguridad de la información (SGSI).

Se debe tener un análisis de riesgos con el fin de garantizar mayor efectividad y eficiencia dentro de cada uno de los procesos, teniendo en cuenta que al conocer las fortalezas y debilidades se mejora el control y administración de recursos tecnológicos, que buscan proporcionar mecanismos y herramientas para adoptar buenas prácticas de seguridad de la información.

La empresa de transporte TransAndes S.A.S, ha mostrado su preocupación ante este vertiginoso y cambiante ambiente tecnológico. De no integrar dentro de sus sistemas, buenas prácticas y recomendaciones de seguridad informática, resultado del análisis de riesgos, buscando tomar total ventaja de su información, reduciendo el riesgo, maximizando beneficios, y ganando competitividad, muy seguramente en un futuro cercano podría ser víctima de delitos informáticos que obstaculicen su normal funcionamiento como pueden ser intrusiones, modificación y/o robo de información, denegación de servicios, entre otros.

ALCANCE Y DELIMITACION DEL PROYECTO

En la empresa de transporte TransAndes S.A.S de la ciudad de Ipiales, se analizó los procesos que tienen que ver con la seguridad informática y de la información, evaluando lo siguiente:

Seguridad lógica, seguridad física, infraestructura tecnológica, hardware y software.

Con respecto a la seguridad lógica de la información, los objetivos que se evaluaron y que se pueden identificar riesgos tiene que ver con:

- Restricciones de acceso a los programas y archivos.
- Controlar la manipulación de la información por parte de los usuarios, verificando la accesibilidad y de acuerdo con el procedimiento adecuado.
- Establecer el mejor canal de transmisión de la información para que los datos lleguen al destino y no exista replica de información.
- Que exista integralidad en la información emitida y recibida.

En la seguridad física, se realizó un análisis de los procedimientos llevados a cabo en la empresa como medidas de prevención ante las amenazas a la información. Se tuvo en cuenta la infraestructura física, las instalaciones, entre otros con el fin de evaluar aspectos externos como desastres naturales, incendios, tormentas, inundaciones, o amenazas humanas, disturbios, sabotajes intencionales o no.

De acuerdo con la infraestructura tecnológica se tuvo en cuenta la red de datos, ya que está muy involucrada en los procesos del sistema de información de la empresa TransAndes. En este ítem se analizó cómo se encuentra distribuida la red de datos, las áreas de acceso a los servicios, la forma en que se encuentran comunicados los equipos, topología, contraseñas de acceso, entre otras.

Los equipos de cómputo de la empresa de transporte TransAndes S.A.S. se evaluaron, verificando las características de los mismos para de esta manera determinar si son funcionales de acuerdo con capacidad y de acuerdo con el uso que se está prestando.

Con respecto al software considerado como activo de la empresa, se evaluó si cuenta con licencias de funcionamiento, analizó las vulnerabilidades, amenazas y riesgos en la adquisición e instalación del software en los equipos. Si existe software no legalizado instalado, si el software es el adecuado para el manejo de la información de la empresa de transporte TransAndes S.A.S.

1. MARCO REFERENCIAL

1.1. ANTECEDENTES

La auditoría de los sistemas de información ha surgido cuando las empresas e instituciones han tomado conciencia sobre 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 adecúe absolutamente a estos sistemas, sea mediante la transformación de métodos, técnicas y procedimientos de la auditoria tradicional, o sea mediante la creación de unos nuevos.

A principios de los años 80's, se empiezan a utilizar técnicas de tratamiento de la información por medio de computadores, como apoyo a la labor de los auditores. El auditor de sistemas de información empieza a ser también experto en el uso de lenguajes informáticos que le sirven para escribir, compilar y ejecutar programas para la consecución de pruebas y obtención de evidencia.

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 adecúan a las crecientes necesidades del sector de las tecnologías de la información, entre ellos se tiene:

Directrices gerenciales de COBIT, desarrollado por la information systems audit control association (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.

The management of the control of data Information technology, desarrollado por el Instituto Canadiense de Contadores Certificados (CICA):

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.

SysTrust - principios y criterios de confiabilidad de sistemas, desarrollados por la Asociación de Contadores Públicos (AlCPA) y el CICA:

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, 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.

ISO/IEC 27000. (information technology – security techniques – information security management system - requirements):

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI). Según el conocido "ciclo de Deming": PDCA - acrónimo de plan. do check, act (planificar, hacer, verificar, actuar). Es consistente con las mejores prácticas descritas en ISO/17799 (actual ISO ICE 27002) y tiene su origen en la revisión de la norma Británica British Standard BS 7799 - 2: 2002.

Al realizar la investigación sobre auditorías dirigidas al área de transporte no se encontraron antecedentes.

1.2. MARCO TEÓRICO

1.2.1. Aspectos generales de la auditoria.

Uno de los avances más importante de los últimos años es la tecnología y con ello el cambio drástico que el mundo ha tenido con el paso del tiempo, el competitivo campo laboral ha adaptado de forma muy positiva el manejo de la tecnología, teniendo como resultado que la información de una empresa este bien organizada, de esta manera se hace necesario tener un control de las herramientas como equipos de cómputo, equipos de comunicación, bases de datos, redes y sistemas de información, para saber así con que herramientas se cuenta y que tan actualizados están, lo anterior combinado con la necesidad de obtener un plan estratégico y corporativo que permita a la empresa conocer las fortalezas y debilidades que genere a la parte administrativa: seguridad, confiabilidad, efectividad y eficacia de su entorno, a partir de esto se hace necesario que se lleve a cabo una auditoría de acuerdo con las necesidades que existan en la empresa.

Por lo general el área de sistemas de una empresa, es un espacio dotado de recursos tecnológicos como equipos de cómputo, impresoras, equipos de comunicaciones, donde prácticamente se realiza todo el procesamiento de la información, que por razones de organización se hace necesaria la auditoria[1].

Existen algunas funciones del área de sistemas, que son:

Administración de sistemas y soporte centralizados. Gran parte de la actividad que se desarrolló en el área de sistemas corresponde a la administración de los sistemas operativos y al soporte a los usuarios de los computadores centrales o corporativos, con los objetivos de garantizar la continuidad del funcionamiento de las máquinas y del software al máximo rendimiento, y facilitar su utilización a todos los sectores de la comunidad de la empresa. Se desarrollaron las siguientes tareas:

- Mantenimiento de los equipos.
- Sintonía del sistema operativo y optimización del rendimiento.
- Gestión de cuentas de usuario y asignación de recursos a las mismas.
- Preservación de la seguridad de los sistemas y de la privacidad de los datos de usuario, incluyendo copias de seguridad periódicas.
- Evaluación de necesidades de recursos (memoria, discos, unidad central) y provisión de los mismos en su caso.
- Instalación y actualización de utilidades de software.
- Atención a usuarios (consultas, preguntas frecuentes, información general, resolución de problemas, asesoramiento, etc.).

[1] http://benmp82.galeon.com/funsis.htm

- Organización de otros servicios como copia de ficheros (backups), impresión desde otros ordenadores en impresoras dependientes de estos equipos.

Funciones del área de sistemas y comunicaciones[2]. La misión fundamental del área, es el diseño, implementación y mantenimiento de los elementos que constituyen la infraestructura informática de la empresa, como los elementos físicos, lógicos, configuraciones y procedimientos necesarios para proporcionar a toda la comunidad los servicios informáticos necesarios para desarrollar sus actividades. También se encarga de:

- La red informática, de los ordenadores centrales que están a disposición de los usuarios y/o que prestan servicios a los ordenadores personales, así como de las aplicaciones instaladas en ellos y los servicios de uso general, como por ejemplo el correo electrónico.
- Instalación y configuración de los ordenadores centrales.
- Altas y bajas de usuarios.
- Instalación y configuración de aplicaciones en los servidores.
- Mantenimiento de los discos de usuarios.
- Administración de las listas de correo.
- Copias de seguridad de los datos de los usuarios y recuperación de los mismos en caso de pérdida.
- Instalación, configuración y mantenimiento de servicios como correo electrónico, proxy web, FTP anónimo.
- Diseño y configuración de la red.

Existen diferentes tipos de auditoría que se aplican de acuerdo a la necesidad, donde se busca encontrar y evaluar diferentes procesos y evidencias[3]. Generalmente, es realizada por una persona independiente y competente acerca de la información que se maneja en una empresa, de igual manera detecta los puntos exactos de control en las distintas dependencias, permitiendo:

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

[2] http://benmp82.galeon.com/funsis.htm

[3] Arens, Alvin A. Auditoria un Enfoque Integral. 6 Edición. Méjico: Prentice Hall, 1996.

- Capacitar y educar sobre controles en los sistemas de información.

La auditoría informática es la evaluación de los recursos tecnológicos, deberá comprender no sólo la evaluación de los equipos de cómputo de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información, según sea la necesidad planteada en el proyecto, además, es importante para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad.

Definición de auditoria.

Auditoria es un examen complejo que se realiza a una empresa, evaluando cumplimiento de normas, proyectos, la parte financiera, el cumplimiento de objetivos, en general evalúa la eficiencia y eficacia de todos los procesos que tienen que ver con el mejoramiento y desarrollo empresarial, determinando diferentes alternativas de soluciones para garantizar organización y logro de objetivos.

Objetivo general de la auditoria.

El objetivo de la auditoria consiste en apoyar a los miembros de la empresa (directorio y las gerencias) en el desempeño de sus actividades, que le permitan la buena y oportuna toma de decisiones. Para ello la auditoria proporciona análisis, evaluaciones, recomendaciones, asesoría e información concerniente a las actividades revisadas.

Funciones principales.

- Evaluar la gestión de la empresa, para emitir sugerencias orientadas a mejorar la gestión administrativa, y asegurar la vigencia de una estructura de control interno sólida y efectiva.
- Verificar el debido cumplimiento de las funciones y responsabilidades asignadas a cada funcionario de la empresa.
- Evaluar el logro de los objetivos y metas, fijadas en los planes y programas, trazados por la empresa.
- Identificar y comunicar a las autoridades competentes, las desviaciones importantes en la ejecución de las actividades, que impiden lograr los objetivos y las metas previamente establecidas; recomendar las medidas correctivas para subsanar dichas desviaciones y cumplir la finalidad para que fue creada la empresa.
- Garantizar la calidad de la información financiera, administrativa o de cualquier otro tipo, de modo que permita a todos los niveles jerárquicos, tomar decisiones acertadas sobre una base firme y segura.

- Establecer el grado en que la prestación de servicios ofrecidos a la colectividad, se han logrado en forma eficiente, efectiva y económica.
- Verificar el cumplimiento de las disposiciones legales, reglamentarias, contractuales y normativas aplicables.
- Ejercer revisión en forma preventiva a los egresos ejecutados por la empresa.
- Evaluar los procesos informáticos de la empresa.

1.2.2. Auditoria informática como objeto de estudio.

La auditoría en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática, de los equipos de cómputo, su utilización, eficiencia y seguridad de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

Los factores que pueden influir en una organización a través del control y la auditoría en informática, son:
- Necesidad de controlar el uso evolucionado de las computadoras.
- Controlar el uso de la computadora, que cada día se vuelve más importante y costosa.
- Altos costos que producen los errores en una organización.
- Abuso en las computadoras.
- Posibilidad de pérdida de capacidades de procesamiento de datos.
- Posibilidad de decisiones incorrectas.
- Valor del hardware, software y personal.
- Necesidad de mantener la privacidad individual.
- Posibilidad de pérdida de información o de mal uso de la misma.
- Necesidad de mantener la privacidad de la organización.

Características de la auditoría informática.

La información de la empresa y para la empresa, siempre importante, 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, materia de la que se ocupa la auditoría de inversión informática.

Del mismo modo, los sistemas informáticos han de protegerse de modo global y particular, a ello se debe la existencia de la auditoría de seguridad informática en general, o, a la auditoría de seguridad de alguna de sus áreas, como pudieran ser desarrollo o técnica de sistemas.

Teniendo en cuenta lo anterior y partiendo de las diferentes actividades de sistemas que cada empresa tiene dentro de su organización dentro de las áreas generales, se establecen las siguientes divisiones de auditoría informática: de

explotación, de sistemas, de comunicaciones y de desarrollo de proyectos. Estas son las áreas específicas de la auditoría informática más importantes. Cada área específica puede ser auditada desde los siguientes criterios generales, que pueden modificarse según sea el tipo de empresa a auditar:

- Desde su propio funcionamiento interno.
- Desde el apoyo que recibe de la dirección y, en sentido ascendente, del grado de cumplimiento de las directrices de ésta.
- Desde la perspectiva de los usuarios, destinatarios reales de la informática.
- Desde el punto de vista de la seguridad que ofrece la Informática en general o la rama auditada.

1.2.3. Clasificación de la auditoria informática.

Auditoría informática de explotación.

Explotación informática se encarga de obtener resultados informáticos, como son: listados impresos, ficheros soportados magnéticamente, órdenes automatizadas para lanzar o modificar procesos industriales, entre otras. Los datos es la materia prima que hay que transformar por medio del proceso informático (gobernado por programas), bajo el criterio de integridad y control de calidad y así lleguen finalmente al usuario. Para auditar explotación hay que auditar las sesiones que la componen y sus interrelaciones.

Auditoría informática de sistemas.

Encargada de analizar todo lo concerniente a técnica de sistemas en todas sus facetas, teniendo como resultado en la actualidad que todo lo que forme el entorno general de sistemas, como son las comunicaciones, líneas y redes de las instalaciones informáticas, se auditen por separado. Dentro de la auditoria informática de sistemas se evalúo lo siguiente:

- Sistemas operativos.
- Software básico.
- Tunning.
- Optimización de los sistemas y subsistemas.
- Administración de base de datos.
- Investigación y desarrollo.

Auditoría informática de comunicaciones y redes.

Para el informático y para el auditor informático, el entramado conceptual que constituyen las redes nodales, líneas, concentradores, multiplexores, redes locales, etc., no son sino el soporte físico-lógico del tiempo real. El auditor tropieza con la dificultad técnica del entorno, pues ha de analizar situaciones y hechos alejados entre sí, y está condicionado a la participación del monopolio telefónico que presta el soporte. Como en otros casos, la auditoría de este sector requiere un

equipo de especialistas, expertos simultáneamente en comunicaciones y en redes locales (no hay que olvidarse que en entornos geográficos reducidos, algunas empresas optan por el uso interno de redes locales, diseñadas y cableadas con recursos propios). El auditor de comunicaciones deberá inquirir sobre los índices de utilización de las líneas contratadas con información abundante sobre tiempos de falta de uso. Deberá proveerse de la topología de la red de comunicaciones, actualizada, ya que la desactualización de esta documentación significaría una grave debilidad. La inexistencia de datos sobre cuantas líneas existen, cómo son y donde están instaladas, supondría que se bordea la inoperatividad informática. Sin embargo, las debilidades más frecuentes o importantes se encuentran en las disfunciones organizativas.

Auditoría informática de desarrollo de proyectos o aplicaciones.

El desarrollo es una evolución del llamado análisis y programación de sistemas y aplicaciones, que a su vez, engloba muchas áreas que tiene la empresa. Una aplicación recorre las siguientes fases:

- Pre-requisitos del usuario (único o plural) y del entorno
- Análisis funcional
- Diseño
- Análisis orgánico (pre-programación y programación)
- Pruebas
- Entrega a explotación y alta para el proceso.

Estas fases deben estar sometidas a un exigente control interno, caso contrario, además del disparo de los costos, podrá producirse la insatisfacción del usuario.

Finalmente, la auditoría deberá comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la maquina sean exactamente los previstos y no otros.

Auditoría de la seguridad informática.

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También pueden ocurrir robos, fraudes o sabotajes, virus, etc., que provoquen la destrucción total o parcial de la actividad computacional. Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos.

1.2.4. Metodología de auditoría informática.

Como auditor se debe recolectar toda la información general, que permita así mismo definir un juicio global objetivo siempre amparadas en pruebas o hechos

demostrables. Dar como resultado un informe claro, conciso y a la vez preciso depende del análisis y experiencia del auditor, frente a diferentes entornos a evaluar, dependiendo de las debilidades y fortalezas encontradas en dicha empresa auditada. La recolección de información, el análisis, la aplicación de diferentes normas de acuerdo con el tipo de auditoría, los hallazgos encontrados y pruebas que avalen estos resultados son indispensables en la realización de una auditoria. Para llegar al resultado hay que seguir una serie de pasos que permiten tener claridad y orden de la auditoria a aplicar.

Alcance y objetivos de la auditoría informática.

El alcance de la auditoría expresa los límites de la misma. Debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones, las materias y las organizaciones a auditar. A los efectos de acotar el trabajo, resulta muy beneficioso para ambas partes expresar las excepciones de alcance de la auditoría, es decir cuales materias, funciones u organizaciones no van a ser auditadas. Tanto los alcances como las excepciones deben figurar al comienzo del informe final.

Estudio inicial del entorno auditable.

Esta etapa es una de las más importantes en el desarrollo de la auditoria, ya que el auditor debe conocer todos los procesos desarrollados, relacionado con el área tomada como caso de estudio. Para realizar dicho estudio ha de examinarse las funciones y actividades generales de la informática. Para su realización el auditor debe conocer lo siguiente:
Organización: para el auditor, el conocimiento de quién ordena, quién diseña y quién ejecuta es fundamental. Para realizar esto el auditor deberá fijarse en:

- Organigrama.
- Departamentos.
- Relaciones jerárquicas y funcionales entre órganos de la organización.
- Flujos de información.
- Número de puestos de trabajo.
- Número de personas por puesto de trabajo.
- Entorno operacional.
- Situación geográfica de los sistemas.
- Arquitectura y configuración de hardware y software.
- Inventario de hardware y software.
- Comunicación y redes de comunicación.

Elaboración del plan y de los programas de trabajo.

Una vez asignados los recursos, el responsable de la auditoría y sus colaboradores establecen un plan de trabajo y así, se procede con la

programación del mismo. El plan se elabora teniendo en cuenta, entre otros criterios, los siguientes:

- Si la revisión debe realizarse por áreas generales o áreas específicas.
- Si la auditoría es global, de toda la Informática, o parcial. El volumen determina no solamente el número de auditores necesarios, sino las especialidades necesarias del personal.
- En el plan no se consideran calendarios, porque se manejan recursos genéricos y no específicos.
- En el plan se establecen los recursos y esfuerzos globales que van a ser necesarios.
- En el plan se establecen las prioridades de materias auditables, de acuerdo siempre con las prioridades del cliente.
- El plan establece disponibilidad futura de los recursos durante la revisión.
- El plan estructura las tareas a realizar por cada integrante del grupo.
- En el Plan se expresan todas las ayudas que el auditor ha de recibir del auditado.

Una vez elaborado el plan, se procede a la programación de actividades. Esta ha de ser lo suficientemente flexible como para permitir modificaciones a lo largo del proyecto.

Actividades propiamente dichas de la auditoría informática.

La auditoría informática general se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos. Cuando la auditoría se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a la misma, de forma que el resultado se obtiene más rápidamente y con menor calidad. Existen técnicas que hacen que el auditor las aplique de acuerdo con su juicio y con el tipo de auditoría a ejecutar y son:

Técnicas de trabajo:

- Análisis de la información obtenida del auditado
- Análisis de la información propia cruzamiento de las informaciones anteriores
- Entrevistas
- Simulación
- Muestreos
- Inspección
- Confirmación
- Investigación
- Certificación
- Observación

Herramientas:

- Cuestionario cuantitativos

- Estándares
- Cuadros de definición de fuentes de conocimiento.
- Encuestas
- Entrevistas

Confección y redacción del informe final.

La función de la auditoría se materializa exclusivamente por escrito. Por lo tanto, la elaboración final es el exponente de su calidad. Resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.

Redacción de la carta de introducción o carta de presentación del informe final.

La carta de introducción tiene especial importancia porque en ella ha de resumirse la auditoría realizada. Se destina exclusivamente al responsable máximo de la empresa, o a la persona concreta que encargó o contrató la auditoría.

Estructura del informe final: el informe comienza con la fecha de comienzo de la auditoría y la fecha de redacción del mismo. Se incluyen los nombres del equipo auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo que ostente. Siguiendo los siguientes pasos:

- Definición de objetivos y alcance de la auditoría:
- Enumeración de temas considerados:
- Cuerpo expositivo

Modelo conceptual de la exposición del informe final:

- El informe debe incluir solamente hechos importantes. La inclusión de hechos poco relevantes o accesorios desvía la atención del lector.
- El informe debe consolidar los hechos que se describen en el mismo.
- El término de "hechos consolidados" adquiere un especial significado de verificación objetiva y de estar documentalmente probados y soportados. La consolidación de los hechos debe satisfacer, al menos los siguientes criterios:
  1. El hecho debe poder ser sometido a cambios.
  2. Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.
  3. No deben existir alternativas viables que superen al cambio propuesto.
  4. La recomendación del auditor sobre el hecho, debe mantener o mejorar las normas y estándares existentes en la instalación.

La aparición de un hecho en un informe de auditoría implica necesariamente la existencia de una debilidad que ha de ser corregida.
Flujo del hecho o debilidad:

Hecho encontrado.
- Ha de ser relevante para el auditor y para el cliente
- Ha de ser exacto, y además convincente.
- No deben existir hechos repetidos.

Consecuencias del hecho: las consecuencias deben redactarse de modo que sean directamente deducibles del hecho.

Repercusión del hecho: se redactará las influencias directas que el hecho pueda tener sobre otros aspectos informáticos u otros ámbitos de la empresa.

Conclusión del hecho: no deben redactarse conclusiones más que en los casos en que la exposición haya sido muy extensa o compleja.
Recomendación del auditor informático:
- Deberá entenderse por sí sola, por simple lectura.
- Deberá estar suficientemente soportada en el propio texto.
- Deberá ser concreta y exacta en el tiempo, para que pueda ser verificada su implementación.
- La recomendación se redactará de forma que vaya dirigida expresamente a la persona o personas que puedan implementarla.

1.2.5. Herramientas y técnicas para la auditoría informática[4].

Cuestionarios.

Las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Entrevistas.

La entrevista es una de las actividades personales más importante del auditor, en ellas, se recoge más información y mejor matizada que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios. Aparte de algunas cuestiones menos importantes, la entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo. El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud a una serie de

[4] http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

preguntas variadas, también sencillas. Sin embargo, esta sencillez es solo aparente. Tras ella debe existir una preparación muy elaborada y sistematizada, y que es diferente para cada caso particular.

Checklist.

El conjunto de estas preguntas recibe el nombre de checklist. Salvo excepciones, las checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma. Según la claridad de las preguntas y el talante del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable.

El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer. Por ello, aun siendo importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía lo es más el modo y el orden de su formulación. Las empresas externas de auditoría Informática guardan sus checklists, pero de poco sirven si el auditor no las utiliza adecuada y oportunamente. No debe olvidarse que la función auditora se ejerce sobre bases de autoridad, prestigio y ética.

El auditor deberá aplicar la checklist de modo que el auditado responda clara y concisamente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta. En algunas ocasiones, se hará necesario invitar a aquél a que exponga con mayor amplitud un tema concreto, y en cualquier caso, se deberá evitar absolutamente la presión sobre el mismo.

Algunas de las preguntas de las checklists utilizadas para cada sector, deben ser repetidas. En efecto, bajo apariencia distinta, el auditor formulará preguntas equivalentes a las mismas o a distintas personas, en las mismas fechas, o en fechas diferentes. De este modo, se podrán descubrir con mayor facilidad los puntos contradictorios; el auditor deberá analizar los matices de las respuestas y reelaborar preguntas complementarias cuando hayan existido contradicciones, hasta conseguir la homogeneidad. El entrevistado no debe percibir un excesivo formalismo en las preguntas. El auditor, por su parte, tomará las notas imprescindibles en presencia del auditado, y nunca escribirá cruces ni marcará cuestionarios en su presencia.

Trazas y/o huellas.

Con frecuencia, el auditor informático debe verificar que los programas, tanto de los Sistemas como de usuario, realizan exactamente las funciones previstas, y no otras. Para ello se apoya en productos software muy potentes y modulares que,

entre otras funciones, rastrean los caminos que siguen los datos a través del programa. Muy especialmente, estas "trazas" se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las mencionadas trazas no deben modificar en absoluto el sistema. Si la herramienta auditora produce incrementos apreciables de carga, se convendrá de antemano las fechas y horas más adecuadas para su empleo. Por lo que se refiere al análisis del sistema, los auditores informáticos emplean productos que comprueban los valores asignados por técnica de sistemas a cada uno de los parámetros variables de las librerías más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado por el fabricante. A modo de ejemplo, algunas instalaciones descompensan el número de iniciadores de trabajos de determinados entornos o toman criterios especialmente restrictivos o permisivos en la asignación de unidades de servicio para según cuales tipos carga. Estas actuaciones, en principio útiles, pueden resultar contraproducentes si se traspasan los límites.

Observación.

La observación es una de las técnicas más utilizadas en la recolección de información para aplicación de una auditoria, ya que a través de diferentes técnicas y métodos de observación permite recolectar directamente la información necesaria sobre el comportamiento del sistema, del área de sistemas, de las funciones, actividades y operaciones del equipo procesador o de cualquier otro hecho, acción o fenómeno del ámbito de sistemas. Existen diferentes tipos de observación

- Observación directa
- Observación indirecta
- Observación oculta
- Observación participativa
- Observación no participativa
- Introspección
- Estrospección
- Observación histórica, entre las cuales están:
  - Observación controlada
  - Observación natural

Inventarios.

Esta forma de recopilación de información consiste en hacer un recuento físico de lo que se está auditando, consiste propiamente en comparar las cantidades reales existentes con las que debería haber para comprobar que sean iguales o, en caso contrario, para resaltar las posibles diferencias e investigar sus causas.
Los principales tipos de inventarios aplicables en el ambiente de sistemas computacionales, son:

- Inventario de software
- Inventario de hardware

- Inventario de documentos
  - Inventario de documentos administrativos
- Manuales de la organización
- Manuales de procedimientos administrativos
- Manuales de perfil de puestos •
  - Otros manuales administrativos
  - Inventario de documentos técnicos para el sistema
- Manuales e instructivos técnico del hardware, periféricos y componentes del sistema.
- Manuales e instructivos de mantenimiento físico del sistema (hardware), entre otros.

1.2.6. Estándares de auditoria.

Para la realización y ejecución de una auditoría se hace necesario aplicar normas o estándares bajo los cuales las empresas deben regirse, de allí la importancia identificar los estándares internacionales que en este caso son[5]:

Directrices gerenciales de COBIT, desarrollado por la information systems audit and control association (ISACA), asociación de auditoría y control de los sistemas de información: 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 administre 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. Uno de los objetivos de ISACA es promover estándares aplicables internacionalmente para cumplir con su visión. La estructura para los estándares de auditoría de SI brinda múltiples niveles de asesoría, como:

- Los auditores de SI respecto al nivel mínimo de desempeño aceptable requerido para cumplir con las responsabilidades profesionales indicadas en el código de ética profesional de ISACA.
- La dirección y otras partes interesadas en las expectativas de la profesión con respecto al trabajo de sus profesionales.
- Los poseedores de la designación de auditor certificado de sistemas de información (certified information systems auditor, CISA) respecto a los requisitos que deben cumplir. El incumplimiento de estos estándares puede resultar en una investigación de la conducta del poseedor del certificado CISA por parte de la junta de directores de ISACA o del comité apropiado de ISACA y, en última instancia, en sanciones disciplinarias, así:

1. The management of the control of data information technology, desarrollado por el Instituto Canadiense de Contadores Certificados (CICA): Este modelo está basado en el concepto de roles y establece responsabilidades relacionadas con seguridad y los controles correspondientes. Dichos roles

[5] www.adacsi.org.ar/files/es/content/146/Standards.doc

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 responsabilidad respecto a control y riesgo previo al establecimiento del control, en términos de objetivos, estándares y técnicas mínimas a considerar.

2. Administración de la inversión de tecnología de inversión: un marco para la evaluación y mejora del proceso de madurez, desarrollado por la Oficina de Contabilidad General de los Estados Unidos (GAO): este modelo identifica los procesos críticos, asegurando el éxito de las inversiones en tecnología de información y comunicación electrónicas. Además los organiza en cinco niveles de madurez, similar al modelo CMM.
3. Estándares de administración de calidad y aseguramiento de calidad ISO 9000, desarrollados por la Organización Internacional de Estándares (ISO): la colección ISO 9000 es un conjunto de estándares y directrices que apoyan a las organizaciones a implementar sistemas de calidad efectivos, para el tipo de trabajo que ellos realizan.
4. SysTrust – principios y criterios de confiabilidad de sistemas, desarrollados por la Asociación de Contadores Públicos (AICPA) y el CICA: Este servicio pretende incrementar la confianza de la 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 un sistema de información es confiable, (si un sistema funciona sin errores significativos, o fallas durante un periodo de tiempo determinado bajo un ambiente dado).
5. Modelo de evolución de capacidades de software (CMM), desarrollado por el Instituto de Ingeniería 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.
6. Administración de sistemas de información: Una herramienta de evaluación práctica, desarrollado por la Directiva de Recursos de Tecnología de Información (ITRB): este es una herramienta de evaluación que permite a entidades gubernamentales, comprender la implementación estratégica de tecnología de información y comunicación electrónica que puede apoyar su misión e incrementar sus productos y servicios.
7. Guía para el cuerpo de conocimientos de administración de proyectos, desarrollado por el comité de estándares del instituto de administración de proyectos: esta guía está enfocada en las mejores prácticas sobre administración de proyectos. Se refiere a aspectos sobre los diferentes

elementos necesarios para una administración exitosa de proyectos de cualquier naturaleza. En forma precisa, este documento identifica y describe las prácticas generalmente aceptadas de administración de proyectos que pueden ser implementadas en las organizaciones.

8. Ingeniería de seguridad de sistemas – modelo de madurez de capacidades (SSE – CMM), desarrollado por la agencia de seguridad nacional (NSA) con el apoyo de la Universidad de Carnegie Mellon: este modelo describe las características esenciales de una arquitectura de seguridad organizacional para tecnología de información y comunicación electrónica, de acuerdo con las prácticas generalmente aceptadas observadas en las organizaciones.
9. Administración de seguridad de información: aprendiendo de organizaciones líderes, desarrollado por la Oficina de Contabilidad General de los Estados Unidos (GAO): este modelo considera ocho organizaciones privadas reconocidas como líderes respecto a seguridad en cómputo. Este trabajo hace posible la identificación de dieciséis prácticas necesarias para asegurar una adecuada administración de la seguridad de cómputo, las cuáles deben ser suficientes para incrementar significativamente el nivel de administración de seguridad en tecnología de información y comunicación electrónica.

El modelo COBIT para auditoría y control de sistemas de información[6].

La evaluación de los requerimientos del negocio, los recursos y procesos IT, son puntos bastante importantes para el buen funcionamiento de una compañía y para el aseguramiento de su supervivencia en el mercado. COBIT es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso. Las siglas COBIT significan objetivos de control para tecnología de información (control objectives for information systems and related technology). El modelo es el resultado de una investigación con expertos de varios países, desarrollado por ISACA (Information Systems Audit and Control Association). COBIT, lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de tecnología. Vinculando tecnología informática y prácticas de control, el modelo COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores. La estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización. “La adecuada implementación de COBIT en una organización, provee una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados,

[6] http://www.channelplanet.com/index.php?idcategoria=13932

que aseguran que los procesos y recursos de información y tecnología contribuyen al logro de los objetivos del negocio en un mercado cada vez más exigente, complejo y diversificado. Cualquier tipo de empresa puede adoptar una metodología COBIT, como parte de un proceso de reingeniería en aras de reducir los índices de incertidumbre sobre vulnerabilidades y riesgos de los recursos IT y consecuentemente, sobre la posibilidad de evaluar el logro de los objetivos del negocio apalancado en procesos tecnológicos", Señaló un informe de ETEK. COBIT se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales y las redes. Está basado en la filosofía de que los recursos 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.

Criterios de Información de COBIT.

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos más amplios de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

- La efectividad tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.
- La eficiencia consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.
- La confidencialidad se refiere a la protección de información sensitiva contra revelación no autorizada.
- La integridad está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
- La disponibilidad se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.
- El cumplimiento tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.
- La confiabilidad se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

COBIT da soporte al gobierno de TI al brindar un marco de trabajo que garantiza que[7]:

[7] http://www.auditool.org/blog/auditoria-de-ti/831-evaluacion-en-los-procesos-de-gobierno-de-ti

- TI está alineada con el negocio.
- TI habilita al negocio y maximiza los beneficios.
- Los recursos de TI se usan de manera responsable.
- Los riesgos de TI se administran apropiadamente. Ver figura 1.

Figura 1. Áreas de enfoque del Gobierno de TI

- **Alineación estratégica.** Se enfoca en garantizar el vínculo entre los planes de negocio y de TI; en definir, mantener y validar la propuesta de valor de TI, y en alinear las operaciones de TI con las operaciones de la empresa.
- **Entrega de valor.** Se refiere a ejecutar la propuesta de valor a lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de la TI.
- **Administración de riesgos.** Requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa, un claro entendimiento del deseo de riesgo que tiene la empresa, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la empresa y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.
- **Administración de recursos.** Se trata de la inversión óptima, así como de la administración adecuada de los recursos críticos de TI:
  - Aplicaciones
  - Información
  - Infraestructura
  - Personas
- **Medición del desempeño.** Rastrea y monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio, con el uso de Balanced Scorecard (BSC) que traduce la estrategia en acción, para

La medición del desempeño es esencial para el gobierno de TI. COBIT le da soporte e incluye el establecimiento y el monitoreo de objetivos que se puedan medir, referentes a lo que los procesos de TI requieren generar (resultado del proceso) y cómo lo generan (capacidad y desempeño del proceso). Muchos estudios han identificado que la falta de transparencia en los costos, valor y riesgos de TI, es uno de los más importantes impulsores para el gobierno de TI. Mientras las otras áreas consideradas contribuyen, la transparencia se logra de forma principal por medio de la medición del desempeño.

Los productos COBIT se han organizado en tres niveles diseñados para dar soporte a lo siguiente[8]:
- Administración y consejos ejecutivos.
- Administración del negocio y de TI.
- Profesionales en gobierno, aseguramiento, control y seguridad.

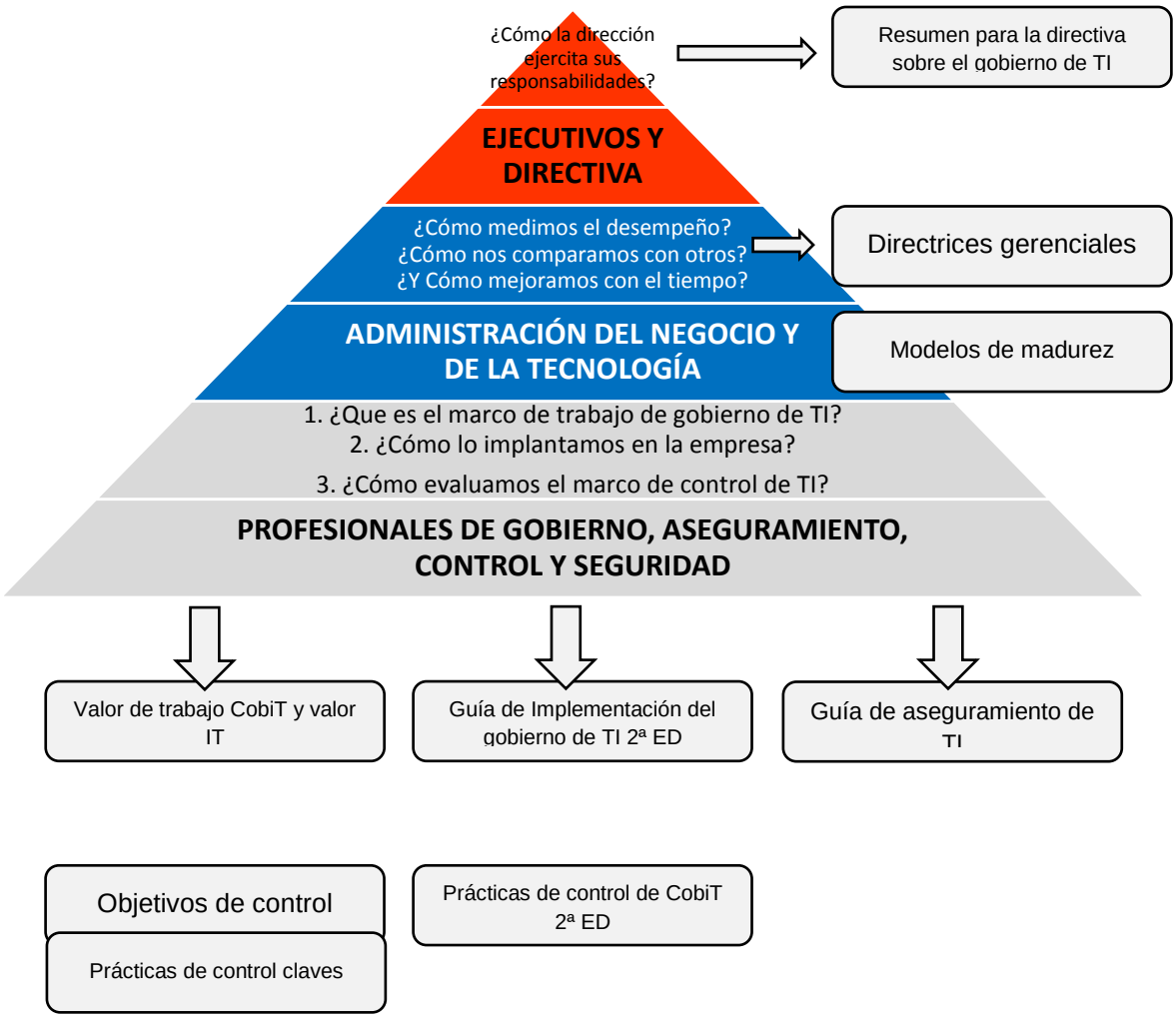
[8] http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf

El diagrama de contenido de COBIT mostrado en la anterior figura presenta las audiencias principales, sus preguntas sobre gobierno TI y los productos que generalmente les aplican para proporcionar las respuestas. También hay productos derivados para propósitos específicos, para dominios tales como seguridad o empresas específicas.

Brevemente, los productos COBIT, incluyen:

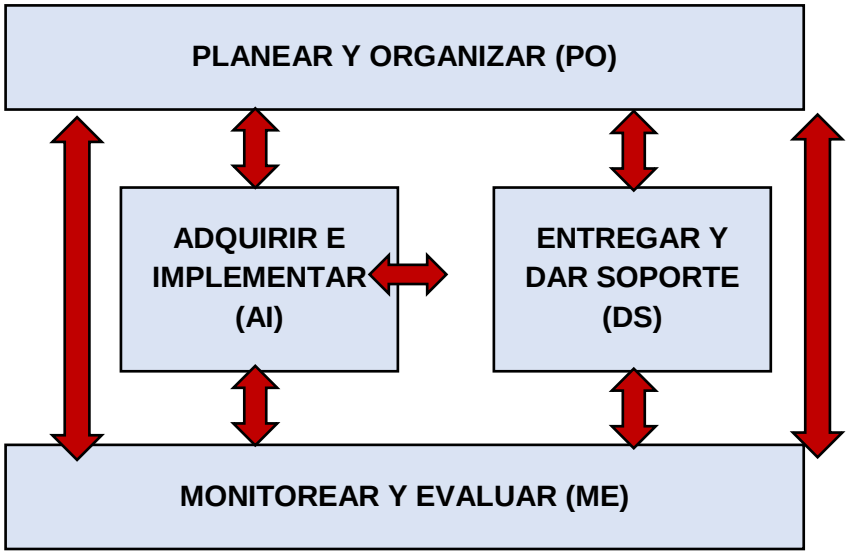
- El resumen informativo al concejo sobre el gobierno de TI, 2ª edición: diseñado para ayudar a los ejecutivos a entender por qué el gobierno de TI es importante, cuáles son sus intereses y cuáles son sus responsabilidades para administrarlo.
- Directrices gerenciales / modelos de madurez: ayudan a asignar responsabilidades, medir el desempeño, llevar a cabo benchmarks y manejar brechas en la capacidad.
- Marco de referencia: explica cómo COBIT organiza los objetivos de gobierno y las mejores prácticas de TI con base en dominios y procesos de TI, y los alinea a los requerimientos del negocio.
- Objetivos de control: brindan objetivos a la dirección basados en las mejores prácticas genéricas para todos los procesos de TI
- Guía de implementación de gobierno de TI: usando COBIT y Val TI 2ª edición. Proporciona un mapa de ruta para implementar gobierno TI utilizando los recursos COBIT y Val TI.
- Prácticas de control de COBIT: guía para conseguir los objetivos de control para el éxito del gobierno de TI 2ª edición: proporciona una guía de por qué vale la pena implementar controles y cómo implementarlos. Ver figura 2.

Figura 2. Diagrama de contenido del COBIT



- Guía de aseguramiento de TI: usando COBIT, proporciona una guía de cómo COBIT puede utilizarse para soportar una variedad de actividades de aseguramiento junto con los pasos de prueba sugeridos para todos los procesos de TI y objetivos de control. El conjunto de lineamientos y estándares internacionales conocidos como COBIT, define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro “dominios” principales, a saber. Ver figura 3.

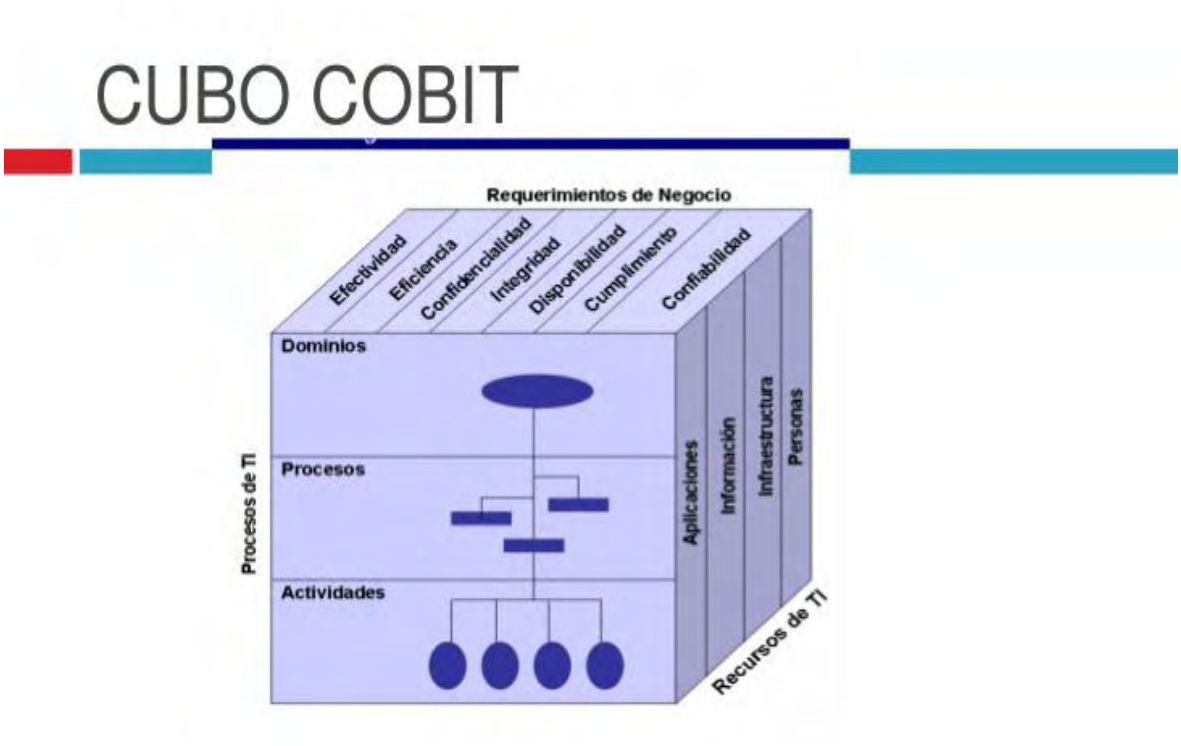
Figura 3. Cuadro de los dominios interrelacionados de COBIT



- **Planear y organizar (PO):** proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).
- **Adquirir e implementar (AI):** proporciona las soluciones y las pasa para convertirlas en servicios.
- **Entregar y dar soporte (DS):** recibe las soluciones y las hace utilizables por los usuarios finales.
- **Monitorear y evaluar (ME):** monitorear todos los procesos para asegurar que se sigue la dirección provista.

Estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de información, como de la tecnología que la respalda. Estos dominios y objetivos de control facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. Ver figura 4.

Figura 4. El cubo de COBIT



Así mismo, se deben tomar en cuenta los recursos que proporciona la tecnología de información, tales como: datos, aplicaciones, plataformas tecnológicas, instalaciones y recurso humano.

Dominios de COBIT.

Entendiéndose como dominio, la agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional, los procesos a su vez son conjuntos o series de actividades unidas con delimitación o cortes de control y las actividades son acciones requeridas para lograr un resultado medible.

COBIT, proporciona una lista completa de procesos que puede ser utilizada para verificar que se completan las actividades y responsabilidades, sin embargo, no es necesario que apliquen todas, y, aún más, se pueden combinar como se necesite por cada empresa.

Dominio. Planificación y organización (PO).

Este dominio cubre la estrategia y 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:

PO1 Definición de un plan estratégico.

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 de 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.

PO2 Definición de la arquitectura de información.

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.

PO3 Determinación de la dirección tecnológica.

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.

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

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.

PO5 Administrar la inversión en TI.

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 de presupuestos periódicos sobre inversiones y operaciones establecidas y aprobados por el negocio.

PO6 Comunicación de la dirección y aspiraciones de la gerencia.

Objetivo: asegurar 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.

PO7 Administración de recursos humanos de TI.
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.

PO8 Administración de 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.

PO9 Evaluación 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.

PO10 Administración de proyectos.
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.

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, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

Procesos:
AI1 Identificación de soluciones automatizadas.
Objetivo: asegurar el mejor enfoque para cumplir con los requerimientos del usuario. Para ello se realiza un análisis claro de las oportunidades alternativas comparadas contra los requerimientos de los usuarios.

AI2 Adquisición y mantenimiento del 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.

AI3 Adquisición y mantenimiento de la infraestructura tecnológica.

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.

AI4 Facilitar la operación y el uso.
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.

AI5 Adquirir recursos de TI.
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.

AI6 Administración de los cambios
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 actual.

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:
DS1 Definir y administrar los niveles de servicio.
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.

DS2 Administración de servicios prestados por terceros.
Objetivo: asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos. 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.

DS3 Administración de desempeño y capacidad.
Objetivo: asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado. 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.

DS4 Garantizar la continuidad del servicio.
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.

DS5 Garantizar la seguridad de sistemas.
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 sistemas, datos y programas está restringido a usuarios autorizados.

DS6 Identificación y asignación 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.

DS7 Educación y entrenamiento de usuarios.
Objetivo: asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados. Para ello se realiza un plan completo de entrenamiento y desarrollo.

DS8 Administrar la mesa de servicio y los incidentes.
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.

DS9 Administración 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.

DS10 Administración de 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.

DS11 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.

DS12 Administrar el ambiente físico.
Objetivo: proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

DS13 Administración de la operación.
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.

Dominio. Monitoreo y evaluación (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:
ME1 Monitoreo del proceso.
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 de 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.

ME2 Monitorear y evaluar el control interno.
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.

ME3 Garantizar el cumplimiento con requerimientos.
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.

ME4 Proporcionar gobierno de TI.
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 siendo auditado y en lo posible deberá ser independiente de la propia empresa. Esta auditoría deberá respetar la ética y los estándares profesionales, seleccionando para ello auditores que sean técnicamente competentes, es decir que cuenten con habilidades y conocimientos que aseguren tareas efectivas y eficientes de auditoría. La función de auditoría deberá proporcionar un reporte que muestre los objetivos de la auditoria, período de cobertura, naturaleza y trabajo de auditoría realizado, así como también la organización, conclusión y recomendaciones relacionadas con el trabajo de auditoría llevado a cabo.

ISO 27000. Sistemas de gestión de la seguridad de la información.

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).

La serie contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los sistemas de gestión de la seguridad de la información (SGSI). La mayoría de estas normas se encuentran en preparación.

¿Qué es ISO 27000?.

Es una familia de estándares internacionales para sistemas de gestión de la seguridad de la información (SGSI).

Requisitos para la especificación de sistemas de gestión de la seguridad de la información:

1. Proceso del análisis y gestión del riesgo.
2. Métricas y medidas de protección.
3. Guías de implantación.
4. Vocabulario claramente definido para evitar distintas interpretaciones de conceptos técnicos y de gestión y mejora continua.

Alcance IS027000.

General: cubre todos los tipos de organizaciones. También especifica los requerimientos a establecer, poniendo en ejecución, funcionando, supervisando, repasando, manteniendo y mejorando la documentación del sistema de administración en la seguridad de la información (ISMS), dentro del contexto de la totalidad de los riesgos del negocio.

Aplicación: el conjunto de requerimientos precisados en este estándar internacional son genéricos y se piensa sean aplicables a todas las organizaciones, sin importar su tipo, tamaño y naturaleza.

ISO 27001.

Esta norma muestra cómo aplicar los controles propuestos en la ISO 17799, estableciendo los requisitos para construir un SGSI, "auditable" y "certificable".

La información tiene una importancia fundamental para el funcionamiento y quizá incluso sea decisiva para la supervivencia de la organización. El hecho de disponer de la certificación según ISO/IEC 27001 ayuda a gestionar y proteger sus valiosos activos de información.

ISO/IEC 27001 es la única norma internacional auditable que define los requisitos para un sistema de gestión de la seguridad de la información (SGSI). La norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales.

Ello ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

Riesgo informático.

Los riesgos, en términos de seguridad, se caracterizan por lo general, mediante la siguiente ecuación.

$$\text{Riesgo} = \frac{\text{Amenaza} + \text{Vulnerabilidad}}{\text{Contramedida}}$$

La amenaza representa el tipo de acción que tiende a ser dañina, mientras que la vulnerabilidad (conocida a veces como falencias (flaws) o brechas (breaches)) representa el grado de exposición a las amenazas en un contexto particular. Finalmente, la contramedida representa todas las acciones que se implementan para prevenir la amenaza.

Las contramedidas que deben implementarse no sólo son soluciones técnicas, sino también reflejan la capacitación y la toma de conciencia por parte del usuario, además de reglas claramente definidas.

Para que un sistema sea seguro, deben identificarse las posibles amenazas y por lo tanto, conocer y prever el curso de acción del enemigo.

Los sistemas de información computarizados son vulnerables a una diversidad de amenazas y atentados por parte de:

1. Personas tanto internas como externas de la organización.
2. Desastres naturales.
3. Por servicios, suministros y trabajos no confiables e imperfectos.
4. Por la incompetencia y las deficiencias cotidianas.
5. Por el abuso en el manejo de los sistemas informáticos.
6. Por el desastre a causa de intromisión, robo, fraude, sabotaje o interrupción de las actividades de cómputos.

Controles.

Es el conjunto de disposiciones metódicas, cuyo fin es vigilar las funciones y actitudes de las empresas y para ello permite verificar si todo se realiza conforme a los programas adoptados, órdenes impartidas y principios admitidos.

MAGERIT. Análisis y gestión de riesgos de los sistemas de la información.

El concejo superior de informática ha elaborado la metodología de análisis y gestión de riesgos de los sistemas de información, MAGERIT. La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes, pero que también dan lugar a ciertos riesgos que deben minimizarse con medidas que garanticen la seguridad y generen confianza en la utilización de estos medios.

El ciclo de gestión de la seguridad siempre establece como primera etapa el análisis y la gestión de los riesgos del sistema que tratamos de proteger. Para una correcta definición e implantación de la seguridad, es necesario identificar y determinar los diferentes elementos significativos dentro del entorno de la seguridad de los sistemas de información.

Elementos de MAGERIT.

A continuación, se define brevemente los elementos considerados significativos por MAGERIT para el estudio de la seguridad en sistemas de información.

- **Activos:** recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección.
- **Amenazas:** eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- **Vulnerabilidad de un activo:** potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.
- **Impacto en un activo:** consecuencia sobre éste de la materialización de una amenaza.
- **Riesgo:** posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización
- **Servicio de salvaguarda:** acción que reduce el riesgo.
- **Mecanismo de salvaguarda:** procedimiento, dispositivo, físico o lógico, que reduce el riesgo.

Descripción del proceso de análisis y gestión de riesgos.

En el proceso de análisis y gestión de riesgos de la seguridad en los sistemas de información se puede identificar las siguientes etapas:

- Planificación.
- Análisis de riesgos.
- Gestión de riesgos.
- Selección de mecanismos de salvaguarda.

COSO (Sponsoring Organizations of the Treadway Commission).

COSO inicio en 1985, recomendando que las organizaciones patrocinadoras de la comisión trabajen juntas para desarrollar sistemas integrados de orientación sobre el control interno.

El modelo COSO define el control interno como un conjunto de procesos, realizado por los directivos de una organización, y creado para garantizar el logro de los objetivos.

COSO consta de cinco elementos, estos elementos proporcionan un marco eficaz para describir y analizar el sistema de control interno, los cuales son;

Entorno de control.

Sirve como base para los demás componentes del control interno, proporcionando disciplina y estructura. El entorno de control tiene una incidencia generalizada en las actividades de la organización, influye sobre las actividades de control, los sistemas de información y comunicación y en la supervisión[9].

Evaluación del riesgo.

Cada empresa se enfrenta a una variedad de riesgos de fuentes externas e internas que deben ser evaluados. Una condición previa para la evaluación de riesgos es el establecimiento de objetivos y por lo tanto la evaluación de riesgos es la caracterización y análisis de los riesgos relevantes para la consecución de los objetivos asignados. "La evaluación de riesgos es un requisito previo para establecer cómo los riesgos deberían ser manejados, dado que estos afectan a la supervivencia y éxito de la empresa. Es imposible reducir el riesgo a cero, es por ello que la dirección determina cual es el nivel de riesgo aceptable"[10].

Las actividades de control.

[9] http://www.mercadotendencias.com/informe-coso-entorno-de-control/
[10] http://www.mercadotendencias.com/informe-coso-evaluacion-de-los-riesgos/

Las actividades de control son las políticas y procedimientos que ayudan a asegurar el cumplimiento de las directrices establecidas por la dirección para controlar los riesgos que pueden obstaculizar el logro de los objetivos de la institución. Las actividades de control se originan en toda la organización, en todos los niveles y en todas las funciones. Estos incluyen una amplia gama de actividades tan diversas como aprobaciones, autorizaciones, verificaciones, conciliaciones, revisiones de desempeño operativo, la seguridad de los activos y la separación de funciones[11].

Información y comunicación.

"Actualmente dada la facilidad y la disponibilidad, las organizaciones tienen acceso a un gran caudal de datos, existen algunos que son útiles y relevantes para la empresa y para la realización de los objetivos propuestos por ésta. Esa gran base de datos, al ser útil para la organización pasa a ser información necesaria para la consecución de sus actividades y fines. La información recogida debe ser relevante para la gestión del negocio, además de ser clara y oportuna" [12].

MECI. Modelo estándar de control interno.

Es una herramienta de gestión que busca unificar criterios en materia de control interno para el sector público, estableciendo una estructura para el control a la estrategia, la gestión y la evaluación.

Proporciona una estructura para el control de la estrategia, la gestión y la evaluación en las entidades, con el fin de orientarlas hacia el cumplimiento de los objetivos institucionales y la contribución de estos a los fines esenciales del Estado.

Principios:

1. Autorregulación: establecer de manera participativa las normas, procesos y procedimientos bajo un entorno de integridad, eficiencia y transparencia en la actuación pública.

2. Autogestión: interpretar, coordinar y aplicar de manera efectiva, eficiente y eficaz la función administrativa que le ha sido asignada.

3. Autocontrol: es la capacidad de cada servidor público, independientemente de su nivel jerárquico, para controlar su trabajo, detectar desviaciones, efectuar correctivos y garantizar los resultados que se esperan en el desarrollo de su función.

[11] http://www.mercadotendencias.com/informe-coso-actividades-de-control/

[12] littp://www.mercadotendencias.com/informe-coso-informacion-y-comunicacion/

2. METODOLOGÍA

Se hizo necesario contar con una metodología para llevar un orden en la auditoría de sistemas de la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales - Nariño, esta metodología es de tipo investigativa, cuantitativa y subjetiva, sirvió como apoyo a la toma de decisiones, con unos objetivos que fueron cumplidos a cabalidad para lograr satisfacer el proceso de la auditoria donde se reunió evidencia por parte del auditor para posteriormente analizarla y sacar unas conclusiones para fortalecer el sistema de información.

Es responsabilidad de la dirección el contenido de la información suministrada por la empresa y analizada por el equipo auditor conformado por los estudiantes Edward Camilo Muñoz Ordoñez y Edwin Robert Velasco Mejía.

Para alcanzar los objetivos propuestos, se utilizó la metodología de tipo empírico, porque se realizó recolección y análisis de datos, además se tomó como fuente primaria de información la observación directa por parte del equipo auditor, también, se estudiaron y aplicaron 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.

Con lo anterior, se planteó la auditoría donde se comenzó a recolectar evidencias para hacer pruebas que proporcionaron unos datos para su posterior análisis, para la recolección de información se utilizó cuestionarios cuantificables con los funcionarios de los diferentes departamentos para hacer la pertinente toma de decisiones.

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

Etapa I. Exploración y familiarización con el entorno.

En esta etapa se realizó una verificación de la empresa, conociendo sus diferentes procesos familiarizándose con las instalaciones de la empresa auditada. Esta exploración le permitió al auditor analizar los objetivos a los que se debe llegar, también se realizaron visitas a los diferentes departamentos donde se utiliza el sistema de información mirando el manejo de los usuarios para lograr una mejor percepción de la información.

Una vez familiarizado con la empresa a ser auditada explorando sus diferentes procesos se procedió a realizar la auditoria de sistemas que permita conocer la vulnerabilidades de la empresa como también sus posibles soluciones.

Etapa II. Planeación de la auditoría de sistemas.

En esta etapa se realizó la planificación de la auditoría:

- Identificar el alcance y los objetivos de la auditoria a realizar.
- Realizar el estudio inicial en la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales - Nariño, para recolectar datos sobre el funcionamiento del sistema.
- Determinar los recursos necesarios para realizar la auditoria.
- Elaboración del plan de auditoria.

Etapa III. Realización de las actividades de la auditoría.

En esta etapa del proyecto se hicieron efectivas las actividades planificadas en la fase anterior, aplicando distintas técnicas y utilizando herramientas que garanticen el cumplimiento de los objetivos planteados. 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 a evaluar.
- Realizar pruebas a los dominios y procesos seleccionados.
- Elaboración cuadros de definición de fuentes de conocimiento de los procesos seleccionados.
- Elaboración de cuestionarios cuantitativos para cada uno de los dominios seleccionados en cuanto al sistema de información.
- Identificación de hallazgos.
- Asignación de la probabilidad de ocurrencia e impacto para los riesgos detectados mediante la aplicación del formato de hallazgos.
- 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 IV. Presentación del informe final.

En esta etapa del proceso de auditoría se presentó ante directivas de la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales - Nariño, sustentando y presentando el informe donde se dan a conocer los problemas encontrados y se sugieren posibles soluciones.

3. DESARROLLO DEL TRABAJO

3.1. ARCHIVO PERMANENTE

El archivo permanente contiene información constante. 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. Se incluye en este punto información permanente que sirve de consulta guía para la evaluación de políticas y procedimientos de la empresa, en este caso de la empresa de transportes TransAndes S.A.S. de la ciudad de Ipiales – Nariño.

3.1.1. Ambiente general de la empresa.

Nombre de la empresa.

Empresa de transportes TransAndes S.A.S. de la ciudad de Ipiales – Nariño.

Reseña histórica.

Transportamos sus mercancías con los más altos estándares de calidad y en tiempos de entrega muy cortos, con servicio puerta a puerta tanto en recogida como en entrega, contamos con una completa red de comunicaciones y dispositivos de seguridad GPS en nuestros vehículos lo que garantiza un seguimiento minuto a minuto y personalizado a cada vehículo brindándonos la seguridad e información inmediata, Además respaldamos sus mercancías ya que estamos amparados con amplias pólizas de transporte[13].

Nuestro compromiso es garantizar la calidad y la generación de valor en cada proceso, es por esto que desde el mes de mayo de 2010 hemos iniciado con éxito la implementación del sistema de la calidad bajo la norma ISO 9001:2000, con el fin de fortalecer nuestras bases comerciales y de servicio y alcanzar así la certificación por parte de la ICONTEC.

Misión.

TRANSANDES S.A.S., es una empresa dedicada a la prestación del servicio de transporte y distribución de mercancías a nivel nacional e internacional (República

[13] Plan estratégico empresa de transportes TransAndes S.A.S.

del Ecuador), nos enfocamos en la satisfacción de la necesidad de envío de bienes, de nuestros clientes, apoyándonos en nuestros valores corporativos, que permitan el crecimiento empresarial, garantizando la rentabilidad de los socios, motivando el desarrollo personal y profesional, de cada uno de nuestros colaboradores y del medio ambiente[14].

Visión.

Ser en el 2011, una empresa certificada bajo la norma N.T.C ISO 9001-2000, con apoyo tecnológico acorde a las necesidades del mercado, que garanticen la calidad del servicio que se ofrece, obteniendo clientes altamente satisfechos, asegurando su fidelidad, ampliando cobertura a nivel nacional y en la República del Ecuador. Desarrollando estrategias de posicionamiento de la imagen corporativa[15].

Valores Corporativos[16].

- **COMPROMISO:** el desarrollo de nuestra actividad diaria exige compromiso con nuestra empresa, con nuestros clientes y con nuestro país.

- **CUMPLIMIENTO:** nuestro crecimiento empresarial depende de la puntualidad y eficiencia con que sirvamos a nuestros clientes.

- **CONFIANZA:** por nuestro cumplimiento y puntualidad la empresa genera la confianza de todos aquellos que se relacionan con nuestra empresa.

- **FLEXIBILIDAD Y ADAPTACION AL CAMBIO:** motivarnos a desarrollar estrategias de talento humano que reflejen el cambio en nuestros colaboradores, y sea percibido por nuestros clientes.

- **LEALTAD Y HONESTIDAD:** para la empresa es vital concienciar al personal de que no hay nada tan valioso como poder mirar a nuestros semejantes, todos los días con la frente en alto, la mirada clara y el honor intacto.

- **TRABAJO EN EQUIPO:** practicar relaciones humanas significa mucho más que establecer o mantener contactos con otros individuos, significa estar condicionados en nuestras relaciones por una actitud, un estado de espíritu, o una manera de ver las cosas, que nos permitan comprender a las otras personas y respetar su personalidad cuya estructura es sin duda diferente de la nuestra.

[14] Plan estratégico empresa de transportes TransAndes S.A.S.
[15] Plan estratégico empresa de transportes TransAndes S.A.S.
[16] Plan estratégico empresa de transportes TransAndes S.A.S.

- **CUIDADO DEL MEDIO AMBIENTE:** nuestra labor se centrara en que en cada kilómetro recorrido, consideremos siempre al mundo como si fuera nuestro propio hogar.

- **SENTIDO DE PERTENENCIA:** nuestros colaboradores deben siempre estar con la camisa puesta.

Servicios.

Transportamos sus mercancías con los más altos estándares de calidad y en tiempos de entrega muy cortos, con servicio puerta a puerta tanto en recogida como en entrega, contamos con una completa red de comunicaciones y dispositivos de seguridad GPS en nuestros vehículos lo que garantiza un seguimiento minuto a minuto y personalizado a cada vehículo brindándonos la seguridad e información inmediata, además respaldamos sus mercancías ya que estamos amparados con amplias pólizas de transporte[17].

Nuestro compromiso es garantizar la calidad y la generación de valor en cada proceso, es por esto que desde el mes de mayo de 2010 hemos iniciado con éxito la implementación del sistema de la calidad bajo la norma ISO 9001:2000, con el fin de fortalecer nuestras bases comerciales y de servicio y alcanzar así la certificación por parte de la ICONTEC.

Servicios Adicionales: contamos con servicio especial de transporte internacional desde nuestras oficinas al Ecuador, habilitados legalmente en Colombia mediante el certificado de idoneidad No. C.I. No. CO- 211-0004 y en Ecuador mediante permiso de prestación de servicios PPS No. EC- 0090-05. Principalmente llegamos a las ciudades de Tulcán, Ibarra, Quito, Guayaquil, Manta, Cuenca. Cualquiera sea su mercancía a transportar.

Naturaleza jurídica.

Toda la información de la naturaleza jurídica de la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales – Nariño se encuentra en Anexos como archivo en formato word, con el nombre de: Anexo 1 NATURALEZA JURIDICA TRANSANDES SAS MANUAL DE FUNCIONES.docx, ubicado dentro de la carpeta ANEXOS TRANSANDES SAS. (Ver anexo 1)

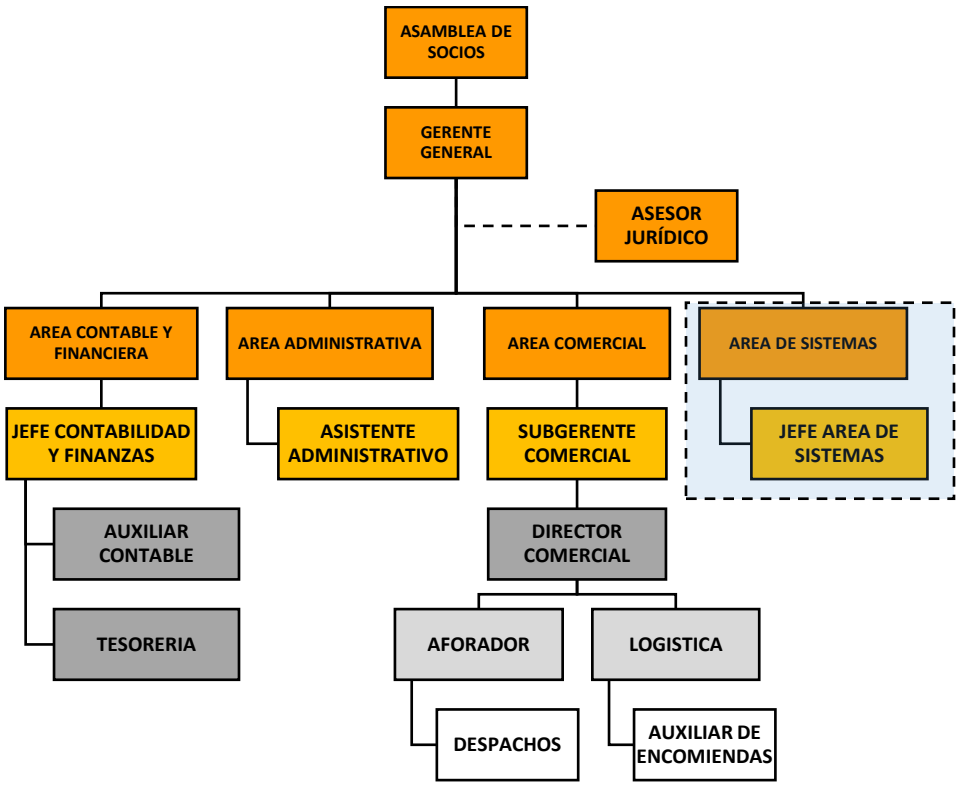
[17] Plan estratégico empresa de transportes TransAndes S.A.S.

Logo de la empresa de transportes TransAndes S.A.S. de la ciudad de Ipiales – Nariño. Ver figura 5.

Figura 5. Logo TransAndes S.A.S.

Estructura organizacional. Ver figura 6.

Figura 6: Estructura organizacional TransAndes S.A.S.



3.2. ARCHIVO CORRIENTE

Para hacer la auditoria es necesario acumular información que será utilizada por el grupo auditor que tendrá que ver con el desarrollo de los diferentes dominios de COBIT.

3.2.1. Plan de auditoría.

Objetivos.

Objetivo general: identificar las vulnerabilidades, amenazas y riesgos en los procesos que afectan la seguridad informática y de la información, empleando la planificación de una auditoria, de acuerdo al estándar COBIT en la empresa de Transporte TransAndes S.A.S. de la ciudad de Ipiales, Nariño,

Objetivos Específicos:

- Conocer el área de informática y los procesos internos de la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales – Nariño.

- Identificar y analizar las diferentes vulnerabilidades, amenazas y riesgos que afectan la seguridad informática y de la información.

- Diseñar los instrumentos para la recolección de la información como pruebas o evidencias de los hallazgos encontrados.

- Aplicar los instrumentos diseñados, realizar las pruebas, ejecutar el proceso de análisis y evaluación de riesgos para su valoración.

- Elaborar y entregar el informe final con los riesgos confirmados y controles propuestos.

Alcance.

Para desarrollar este trabajo en primer lugar se identificó e investigó las diferentes técnicas de auditoría de sistemas, es decir los estándares utilizados para realizar una auditoría de seguridad informática como el COBIT, Magerit, ISO 27000, COSO, MECI, con el fin de determinar cuáles van a ser utilizadas. En este caso utilizamos el estándar COBIT 4.0. Dentro de las técnicas que se investigó se encuentran técnicas para obtener información como cuestionarios cuantitativos, encuestas y entrevistas, todas estas a través de cuadros de fuentes de conocimiento.

La aplicación de técnicas de auditoría se realizó a la empresa de transporte TransAndes S.A.S de la ciudad de Ipiales – Nariño, con el propósito de efectuar

una revisión y evaluación de los controles físicos y lógicos, procedimientos de informática, observar su utilización, y evaluar la seguridad, con el fin de detectar problemas y plantear recomendaciones alternativas para que se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

Los puntos que se evaluaron fueron los siguientes:

De las instalaciones físicas se evaluó:

- Protección física de datos.
- Personal de las dependencias.
- Medidas de evacuación, alarmas, salidas alternativas.
- Estructura, diseño y distribución de las instalaciones eléctricas, de cableado de la red de datos.
- Sustituciones o sustracción de equipos, componentes, soportes magnéticos, documentación u otros activos.
- Seguridad de oficinas, recintos e instalaciones, protección eléctrica, contra incendios.
- Áreas de acceso público.
- Ubicación y protección de hardware.
- Mantenimiento de los equipos.
- Desastres naturales, incendios accidentales tormentas e inundaciones.
- Amenazas ocasionadas por el hombre.

De equipos o hardware se evaluó:

- Seguridad física de los medios.
- Actas e informes técnicos.
- Inventarios.
- La existencia de hojas de vida de los equipos de cómputo.
- La elaboración correcta de bitácoras de los mantenimientos realizados.

De seguridad lógica se evaluó:

- Que cada usuario solo pueda acceder a los recursos que se le autorice el propietario.
- Autenticación.
- Quien asigna la contraseña inicial y sucesivas.
- Controles existentes para evitar y detectar virus.
- Que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Que la información transmitida sea recibida por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.

- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Justificación.

Se realizó una auditoría de sistemas al sistema de información de la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales - Nariño, evaluado cada uno de los ítems anteriormente nombrados para verificar, evaluar y analizar los diferentes hallazgos así como sus posibles soluciones para que se realicen mejoras, esto con el fin de mejorar en los diferentes aspectos para un buen funcionamiento y mejoramiento del servicio de sus asociados.

Metodología.

Para el cumplimiento de los objetivos planteados en la auditoría, se realizaran las siguientes actividades:

Investigación preliminar:

- Determinar la estructura organizacional de la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales - Nariño para determinar responsables en la vigilancia del sistema de información instalado.
- Evaluar la importancia de la seguridad física, lógica, infraestructura tecnológica y software dan a los procesos de la empresa.
- Conocer de manera global el sistema de información instalado y configurado para el manejo de los servicios, identificando los elementos que apoyan la seguridad y administración de la misma.

Identificación y agrupación de riesgos:

- Identificar y clasificar los riesgos a los que está expuesto el sistema informático y de información, ya sean propios o generados por entidades externas (personas, procedimientos, bases de datos, redes, virus etc.) esto se hace por medio de las visitas que se realizan para la familiarización del auditor con el sistema de información.

Diseño del programa de auditoría:

- Definir los dominios, procesos y objetivos de control de COBIT, que tienen relación con el proceso de auditoría.
- Realizar los procedimientos que permitan recolectar la evidencia que apoye los hallazgos y recomendaciones.

Ejecución de las pruebas de auditoría:

- Obtener evidencia sobre los procesos establecidos, su utilización, y el entendimiento y ejecución de los mismos por parte de las personas involucradas.
- Identificar las causas de las debilidades.

- Determinar la probabilidad y el impacto que tendrá cada debilidad en el sistema de información.
- Identificar los hallazgos de tipo preventivo, defectivo y correctivo de las debilidades encontradas.
- Identificar los recursos afectados por las debilidades encontradas.

Elaboración y envío del informe de auditoría:

- Comunicar a las personas o entes involucrados en la vigilancia y administración del sistema de información de la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales - Nariño, los resultados de la auditoria, para que ellos hagan la gestión necesaria para implementar los controles que cubran aquellas situaciones de riesgo de mayor relevancia, y mantengan y optimicen la red.
- Hacer parte de la documentación para futuras auditorías.

Herramientas de estudio:

- Evidencia fotográfica.
- Cuestionarios cuantitativos de análisis de riesgo.
- Encuestas.
- Entrevistas.

Recursos:

- Humanos:
  - Edward Camilo Muñoz Ordoñez
  - Edwin Robert Velasco Mejía
- Técnicos.
  - Computador.
  - Impresora.
  - Cámara Digital.
  - Grabadora de voz.

Cronograma de actividades. Ver tabla 1.

Tabla 1. Cronograma de actividades.

ETAPAS	ACTIVIDADES	2015				2016	
		SEP	OCT	NOV	DIC	ENE	FEB
I ETAPA	Recolección, clasificación y análisis de la información sobre técnicas de auditoría de sistemas.						
II ETAPA	Identificar el alcance y los objetivos de la auditoría.						
	Realizar el estudio inicial en la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales – Nariño.						
	Determinar los recursos necesarios para realizar la auditoria.						
	Elaboración del plan de trabajo.						
III ETAPA	Elección de los procesos a auditar.						
	Ejecución de la auditoría.						
	Elaboración de un análisis de hallazgos y riesgos.						
	Elaboración del informe con los hallazgos encontrados, detectando las causas y su efecto.						
	Elaboración del modelo de madurez en el cual se encuentra el sistema auditado.						
	Elaboración de un informe final.						
IV ETAPA	Sustentación y presentación del informe final						

Programa de auditoría.

Para la realización de la auditoria de sistema a la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales - Nariño, se utilizó la metodología COBIT (objetivos de control para la información y tecnologías relacionadas) donde existen cuatro dominios de los cuales se evaluaron los siguientes:

Objetivos de control para la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales - Nariño:

DOMINIO DE PLANEACION Y ORGANIZACIÓN (PO)

Este dominio se refiere a la identificación de la tecnología de información de la empresa TransAndes y en cómo esta puede contribuir a cumplir los objetivos de la misma. Los procesos que se aplican son los siguientes:

PO4 Definir los procesos, la organización y las relaciones de TI.

Prestación de servicios de TI esto se realiza a través de una organización conveniente en número y habilidades con tareas y responsabilidades definidas y comunicadas, teniendo en cuenta los siguientes objetivos de control:

PO4.1 Marco del trabajo del comité estratégico.
PO4.2 Comité directivo.
PO4.3 Ubicación organizacional de la función de la TI.
PO4.4 Estructura organizacional.
PO4.5 Roles y responsabilidades.
PO4.6 Responsabilidad de aseguramiento de calidad de TI.
PO4.7 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento.
PO4.8 Propiedad de datos y de sistemas.
PO4.9 Supervisión.
PO4.10 Segregación de funciones.
PO4.11 Personal de TI.
PO4.12 Personal clave de TI.
PO4.13 Políticas y procedimientos para personal contratado.
PO4.14 Relaciones.

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. 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.
PO9.2 Establecimiento del contexto del riesgo.
PO9.3 Identificación de eventos.
PO9.4 IT Evaluación de riesgos.
PO9.5 Respuesta a los riesgos.

PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos.

DOMINIO DE ADQUISICION E IMPLEMENTACION (AI).

En este dominio las soluciones tienen que ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Igualmente, tiene en cuenta los cambios y mantenimiento que deben tener los sistemas que existan dentro de la empresa. Los procesos utilizados en este dominio son:

AI3 Adquirir y mantener infraestructura tecnológica.

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 de software del sistema y toma en consideración los siguientes objetivos de control:

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.

DOMINIO DE ENTREGAR Y DAR SOPORTE (DS).

El soporte en una empresa es uno de los factores más importantes ya que a través de este se pueden realizar capacitaciones a los usuarios que utilizan los sistemas de información, además que las empresas contratistas están obligadas a hacer este tipo de soportes para la empresa.

DS4 Garantizar la continuidad del servicio.

Mantener el servicio disponible de acuerdo con los requerimientos y continuar con la provisión en caso de interrupciones. Para ello se tiene un plan de continuidad aprobado y funcional, que este alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio y toma en consideración los siguientes objetivos de control:

DS4.1 IT Marco de trabajo de continuidad.
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.

DS5 Garantizar la seguridad de los sistemas.

Salvaguardar la información contra el uso no autorizados, divulgación, modificación, diseño o pérdida. Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración los siguientes objetivos de control:

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 de 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.

DS7 Educar y entrenar a los usuarios.

Para una educación efectiva de todos los usuarios de sistemas de TI incluyendo aquellos dentro de TI, se requiere identificar las necesidades de entrenamiento de cada grupo de usuarios. Además de identificar las necesidades, este proceso incluye la definición y ejecución de una estrategia para llevar a cabo un entrenamiento efectivo y para medir los resultados. Un programa efectivo de entrenamiento mejora el uso efectivo de la tecnología al disminuir errores, incrementando la productividad y el cumplimiento de los controles claves tales como las medidas de seguridad de los usuarios.

DS7.1 Identificación de necesidades de entrenamiento y educación.
DS7.2 Impartición de entrenamiento y educación.
DS7.3 Evaluación del entrenamiento recibido.

DS12 Administrar el ambiente físico.

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 brinden control de acceso del personal a las instalaciones y contemplen su seguridad física.

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.

Diseño de elementos de la auditoria.

Para la realización del proceso de auditoría a la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales - Nariño, se utilizaron diferentes instrumentos de recolección de información, a continuación se describe cada uno de ellos:

Observación directa.

Se utiliza esta técnica como un elemento de auditoría muy importante que permite observar, tomar información y registrarla. En las visitas a las instituciones también se evidencia información mediante fotografías y videos, sirviendo de apoyo en el análisis que finalmente se hizo.

Cuadro de definición de fuentes de conocimiento, pruebas de análisis, y pruebas de auditoría.

Este cuadro es un instrumento que sirve para identificar, cuál es la información que se necesita para evaluar un determinado proceso dentro de los dominios del COBIT, también se especifica en el cuales son las pruebas de análisis y de ejecución que se deben realizar. Los ítems relacionados a continuación son los que describirán el elemento de auditoría:

- **REF:** se refiere al ID del elemento.

- **ENTIDAD AUDITADA:** en este espacio se indicara el nombre de la entidad a la cual se le está realizando el proceso de auditoría.

- **AREA AUDITADA:** nombre del área a la cual se aplicara la auditoria (p.ej. red de datos, seguridad física y lógica).

- **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA:** en este espacio se hace una breve referencia al objetivo del proceso seleccionado dentro de los dominios del COBIT que se está revisando.

- **MATERIAL DE SOPORTE:** en este espacio se indicara el nombre del material que soporta el proceso, para el caso será COBIT.

- **DOMINIO:** espacio reservado para colocar el nombre del dominio de COBIT que se está evaluando.
- **PROCESO:** espacio reservado para el nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.

- **FUENTES DE CONOCIMENTO:** en este espacio se deberá consignar todas las fuentes de donde se extrajo la información para el proceso de auditoria lo que servirá como respaldo del proceso.

- **REPOSITORIO DE PRUEBAS:** se divide en dos tipos de pruebas:
  - DE ANÁLISIS: este espacio está destinado para describir las pruebas de análisis que se van a realizar para evaluar el proceso especifico que se encuentre en estudio.
  - DE EJECUCIÓN: este espacio está destinado para describir las pruebas de ejecución que se van a realizar para evaluar el proceso especifico que se encuentre en estudio.

- **RESPONSABLES:** en este espacio se indicaran los nombres del equipo auditor que está llevando a cabo el proceso de auditoría.

El modelo de la tabla de definición de fuentes de conocimiento, pruebas de análisis de auditoría, se encuentra detallado con un ejemplo. Ver Tabla 2.

Todos los cuadros de definición de fuentes del conocimiento, pruebas de análisis y pruebas de auditoría utilizados en el proceso de auditoría se encuentran en los anexos entregados en medio digital. (Ver anexo 2): en la carpeta anexos TransAndes SAS/Anexo 2 CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO TRANSANDES SAS.docx

Tabla 2. Definición de fuentes de conocimiento, pruebas de análisis de auditoria

	CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS DE AUDITORÍA	**REF** ( )
ENTIDAD AUDITADA		Página
Empresa de transporte TransAndes S.A.S. de Ipiales – Nariño.		
AREA AUDITADA		
DESCRIPCIÓN DE LA ACTIVIDAD / PRUEBA:		
MATERIAL DE SOPORTE: COBIT		
DOMINIO	**PROCESO**	
FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
AUDITORES RESPONSABLES		
EDWARD CAMILO MUÑOZ ORDOÑEZ EDWIN ROBERT VELASCO MEJIA		

Cuestionario cuantitativo.

El cuestionario es una técnica utilizada para recopilar datos, permite llegar a un mayor número de participantes y facilita el análisis, consiste en una serie de preguntas, escritas, que debe responder el entrevistado. Además permite dar un puntaje que permite analizar los riesgos de cada proceso.

Los campos que utiliza este formato se describen a continuación:

- **REF:** espacio reservado para la identificación del cuestionario.
- **INSTITUCIÓN AUDITADA:** nombre de la institución a la cual se aplica el proceso de auditoría.
- **ÁREA AUDITADA:** nombre del área a la cual se aplicara la auditoria (p.ej. red de datos, seguridad física y lógica)

- **DESCRIPCIÓN DE ACTIVIDAD/PRUEBA:** en este espacio se describe el objetivo del proceso establecido dentro de los dominios del COBIT.

- **MATERIAL DE SOPORTE:** nombre del material que da soporte al proceso establecido.

- **DOMINIO:** nombre del dominio del COBIT que se va a evaluar.

- **PROCESO:** nombre del proceso que se va a auditar dentro de los dominios del COBIT.

- **PREGUNTA:** descripción de la información requerida la cual se quiere investigar.

- **SI - NO - NA:** aquí se establece un valor de 1 a 5 de acuerdo a si cumple o no con la información requerida. Teniendo en cuenta que:
  1: es el mínimo puntaje que se le puede asignar y es irrelevante.
  5: es el máximo puntaje que se le puede asignar y es de gran importancia.

- **RPT:** fuente de donde se obtuvo la información requerida.

Las equivalencias que se utilizan para asignares valores a los requerimientos, va entre 1 y 5, siendo 1 un valor insignificante, esto quiere decir que no es importante, pero el valor 5 un valor crítico, cuando aparece el 5 en el lado de los NO, esto automáticamente se convierte en un hallazgo.

- **TOTALES:** espacio para asignar el valor de:
  - Sumatoria de los valores de la columna SI.
  - Sumatoria de los valores de la columna NO.
  - Sumatoria de los valores de la columna NA.

- **TOTAL CUESTIONARIO:** en este espacio se asigna la suma de los totales (SI, NO y NA).

Para calcular el porcentaje de riesgo, aplicamos la siguiente fórmula matemática

- **PORCENTAJE DE RIESGO:** para calcular el porcentaje de riesgo se aplica la siguiente fórmula matemática:

$$\text{Porcentaje de riesgo (parcial)} = \frac{\text{Totales SI} * 100}{\text{Total cuestionario - Totales NA}}.$$

Luego de obtener el anterior porcentaje se calcula el porcentaje de riesgo total así:

Porcentaje de riesgo (total) = 100 - Porcentaje de riesgo (parcial)

Después de haber calculado este porcentaje, se procede a determinar el nivel de riesgo en el que se encuentra, para esto se tiene en cuenta la siguiente escala:

1%	-	30%	=	Riesgo bajo
31%	-	70%	=	Riesgo medio
71%	-	100%	=	Riesgo alto

Riesgo bajo: las deficiencias que se presentan en este nivel no son de gran importancia, sin embargo se deben considerar soluciones preventivas a largo plazo.

Riesgo medio: las medidas para reducir el riesgo deben implantarse en un periodo determinado puesto que el daño causado puede ser controlado.

Riesgo alto: en este nivel se deben establecer estrategias radicales e inmediatas para reducir el riesgo, porque de lo contrario afectaría el logro de los objetivos de la institución.

- **RESPONSABLES:** nombres del equipo auditor.

El modelo de la tabla de cuestionario cuantitativo se encuentra detallado con un ejemplo. Ver tabla 3.

Todos los cuestionarios cuantitativos utilizados en el proceso de auditoría se encuentran en los anexos entregados en medio digital: (Ver anexo 3): en la carpeta ANEXOS TRANSANDES SAS/Anexo 3 CUESTIONARIO CUANTITATIVO TRANSANDES SAS.docx

Tabla 3. Formato cuestionario cuantitativo.

	CUESTIONARIO CUANTITATIVO	REF (_)
ENTIDAD AUDITADA		Página
Empresa de transporte TransAndes S.A.S. de Ipiales – Nariño.		
AREA AUDITADA		
MATERIAL DE SOPORTE: COBIT		
DOMINIO	PROCESO	

PREGUNTA	SI	NO	NA	RPT
TOTALES				
TOTAL CUESTIONARIO				
PORCENTAJE DE RIESGO:	= = %			=

AUDITORES RESPONSABLES
EDWARD CAMILO MUÑOZ ORDOÑEZ EDWIN ROBERT VELASCO MEJIA

Encuesta y entrevista.

Las encuestas y entrevistas que se hicieron a la empresa fueron realizadas por el equipo auditor. Cabe resaltar que la empresa auditada tenía conocimiento de estas visitas, por lo tanto los entrevistados tuvieron previa preparación.

Encuestas con preguntas cerradas: el entrevistado se limita a contestar Si o No, se recoge información útil para nuestra investigación, permitiendo en este formato adicionar la cantidad de algunos elementos y algunas observaciones.

Entrevistas con preguntas abiertas: donde la persona entrevistada pueda expresar libremente su respuesta, generando respuesta con detalles, permitiendo hacer más preguntas según vaya respondiendo cada una.

Todas las encuestas y entrevistas aplicadas y los formatos utilizados en el proceso de auditoría se encuentran en los anexos entregados en medio digital. (Ver anexo 4): En la carpeta ANEXOS TRANSANDES SAS/Anexo 4 ENCUESTAS

TRANSANDES SAS.docx y (Ver anexo 5): en la misma carpeta ANEXOS TRANSANDES SAS/Anexo 5 ENTREVISTAS TRANSANDES SAS.docx

A continuación, se presentan ejemplos de los cuestionarios de encuestas y entrevistas que se utilizaron para realizar este proceso de Auditoría. Ver tablas 4 y 5.

Tabla 4. Formato de encuesta.

	ENCUESTA	**REF**
		(_)
ENTIDAD AUDITADA		Página
Empresa de transporte TransAndes S.A.S. de Ipiales – Nariño.		
AREA AUDITADA		
MATERIAL DE SOPORTE: COBIT		
NOMBRE DEL ENCUESTADO	**CARGO**	
PREGUNTA	**SI**	**NO**
AUDITORES RESPONSABLES		
EDWARD CAMILO MUÑOZ ORDOÑEZ EDWIN ROBERT VELASCO MEJIA		

Tabla 5. Formato de entrevista.

	ENTREVISTA	REF (_)
ENTIDAD AUDITADA		Página
Empresa de transporte TransAndes S.A.S. de Ipiales – Nariño.		
AREA AUDITADA		
MATERIAL DE SOPORTE: COBIT		
NOMBRE DEL ENTREVISTADO	**CARGO**	
PREGUNTA		
ENTREVISTADO		
NOMBRE: _____ FIRMA: _____		
AUDITORES RESPONSABLES		
EDWARD CAMILO MUÑOZ ORDOÑEZ EDWIN ROBERT VELASCO MEJIA		

Matriz de probabilidad e impacto.

La matriz de probabilidad e impacto es un elemento fundamental para determinar el nivel de riesgo de cada proceso auditado y a su vez identificar los riesgos más críticos. El porcentaje de riesgo obtenido se ubica en la respectiva casilla de acuerdo a la clasificación del riesgo.

En la tabla 6, se muestra el diseño de la matriz de probabilidad e impacto:
Las matrices de probabilidad e impacto se encuentran dentro de (Ver anexo 6): la carpeta ANEXOS TRANSANDES SAS/Anexo 6 HALLAZGOS TRANSANDES SAS.docx y se muestra una matriz por cada dominio o grupo de procesos.

Tabla 6. Formato matriz de probabilidad e impacto.

PROBABILIDAD DE OCURRENCIA				
	ALTO 61-100%	ZONA DE RIESGO MODERADO	ZONA DE RIESGO IMPORTANTE	ZONA DE RIESGO INACEPTABLE
	MEDIO 31-60%	ZONA DE RIESGO TOLERABLE	ZONA DE RIESGO MODERADO	ZONA DE RIESGO IMPORTANTE
	BAJO 0-30%	ZONA DE RIESGO ACEPTABLE	ZONA DE RIESGO TOLERABLE	ZONA DE RIESGO MODERADO
		LEVE	**MODERADO**	**CATASTRÓFICO**
		I M P A C T O		

Clasificación del riesgo:

Riesgo bajo

Riesgo moderado

Riesgo intolerable

Hallazgos aplicados en la auditoria a la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales – Nariño.

Manual de navegación de hallazgos.
En este manual se describe las inconsistencias encontradas.

Esta información será desglosada de la siguiente manera:

- **REF:** se refiere al ID del elemento.
- **ENTIDAD AUDITADA:** en este espacio se indicara el nombre de la entidad a la cual se le está realizando el proceso de auditoría.
- **MATERIAL DE SOPORTE:** en este espacio se indicara el nombre del material que soporta el proceso, para el caso será COBIT.
- **DOMINIO (E):** espacio reservado para colocar el nombre del dominio de COBIT que se está evaluando.

- **PROCESO (F):** espacio reservado para el nombre del proceso en específico que se está auditando dentro de los dominios del COBIT.

- **HALLAZGO:** aquí se encontrara la descripción de cada hallazgo, así como la referencia al cuestionario cuantitativo que lo soporta.

- **CONSECUENCIAS Y RIESGOS:** en este apartado se encuentra la descripción de las consecuencias del hallazgo así como la cuantificación del riesgo encontrado.

- **RECOMENDACIONES:** en este último apartado se hace una descripción de las recomendaciones que el equipo auditor ha presentado a las entidades auditadas.

- **EVIDENCIAS:** aquí se encuentra en nombre de la evidencia y el número del anexo donde ésta se encuentra.

- **RESPONSABLES:** an este espacio se indicaran los nombres del equipo auditor que está llevando a cabo el proceso de auditoría.

La tabla que a continuación se muestra es un modelo para la definición de los hallazgos. Ver tabla 7.

Todos los hallazgos encontrados en la auditoria del sistema de información y los formatos utilizados en el proceso se encuentran en los anexos entregados en medio digital. (Ver anexo 6): En la carpeta ANEXOS TRANSANDES SAS/Anexo 6 HALLAZGOS TRANSANDES SAS.docx

Tabla 7. Hallazgos.

	HALLAZGOS	REF (_)
ENTIDAD AUDITADA		Página
Empresa de transporte TransAndes S.A.S. de Ipiales – Nariño.		
AREA AUDITADA		
MATERIAL DE SOPORTE: COBIT		
DOMINIO	PROCESO	
HALLAZGO		
CONSECUENCIAS		
RIESGO		
RECOMENDACIONES		
EVIDENCIAS		
AUDITORES RESPONSABLES		
EDWARD CAMILO MUÑOZ ORDOÑEZ EDWIN ROBERT VELASCO MEJIA		

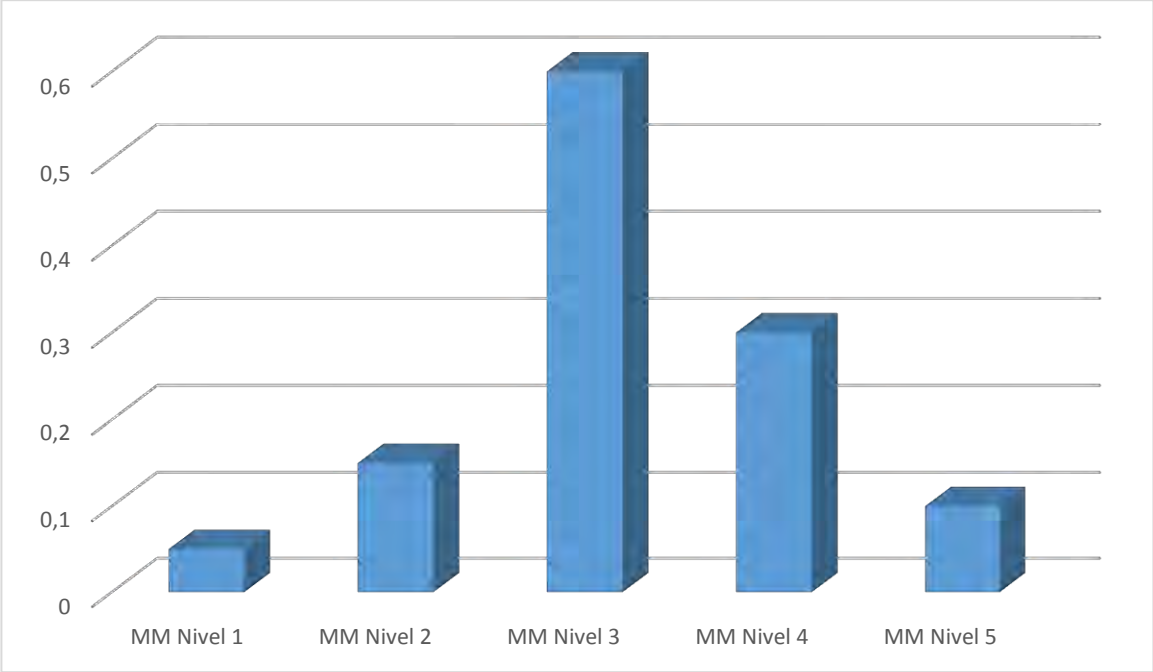
Modelo de madurez.

Se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí misma desde un nivel de no-existente (0) hasta un nivel de optimizado (5. El propósito no es evaluar el nivel de adherencia a los objetivos de control.

Los niveles de madurez están diseñados como perfiles de procesos de TI que una organización reconocería como descripciones de estados posibles actuales y futuros. No están diseñados para ser usados como un modelo limitante, donde no

se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior. Una evaluación de la madurez de COBIT resultará en un perfil donde las condiciones relevantes a diferentes niveles de madurez se han conseguido, como se muestra en el ejemplo gráfico de la figura siguiente. Ver figura 7.

Figura 7. Modelo de Madurez.



Posible nivel de madurez de un proceso de TI: el ejemplo ilustra el proceso que está ampliamente en el nivel 3, pero cumple algunas acciones con menor nivel de requerimiento mientras sigue investigando en la medición del desarrollo.

Esto se debe a que cuando se emplea la evaluación de la madurez con los modelos de COBIT, a menudo algunas implementaciones estarán en diferentes niveles aunque no esté completa o suficiente:

- El desempeño real de la empresa - dónde se encuentra la empresa hoy.
- El objetivo de mejora de la empresa - dónde desea estar la empresa.
- El crecimiento requerido entre "como es" y "como será".

Gráficamente el modelo de madurez se describe a continuación. Ver figura 8.

Figura 8. Grafica modelo de madurez.

Estas escalas deben ser prácticas en su aplicación y razonablemente fáciles de entender.

La ventaja de un modelo de madurez es que es relativamente fácil para la dirección ubicarse a sí misma en la escala y evaluar qué se debe hacer si se requiere desarrollar una mejora. La escala incluye al 0 ya que es muy posible que no existan procesos en lo absoluto.

La escala del 0-5 se basa en una escala de madurez simple que muestra como un proceso evoluciona desde una capacidad no existente hasta una capacidad optimizada.

Los hallazgos encontrados en la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales- Nariño fueron:

DOMINIO - PLANIFICACION Y ORGANIZACIÓN (PO).
PO4. Definir los procesos, organización y relaciones de TI.
PO9. Evaluar y administrar los riesgos de TI.

DOMINIO - ADQUIRIR E IMPLEMENTAR (AI).
AI3 Adquirir y mantener infraestructura tecnológica.

DOMINIO - ENTREGA DE SERVICIOS Y SOPORTE (DS).
DS4 Garantizar la continuidad del servicio.
DS5 Garantizar la seguridad de los sistemas.
DS7 Educación y entrenamiento de usuarios.
DS12 Administrar el ambiente físico.

Informe ejecutivo de auditoría.

Ipiales, febrero de 2016.

Doctora:
MARTHA L. SANCHEZ
Gerente General empresa de transporte TransAndes S.A.S.
Ciudad

REF: AUDITORIA A LOS PROCESOS DEL SISTEMA INFORMÁTICO Y DE INFORMACIÓN DE LA EMPRESA DE TRANSPORTE TRANSANDES S.A.S DE LA CIUDAD DE IPIALES – NARIÑO.

Cordial Saludo.

Como es de su conocimiento la empresa de transporte TransAndes S.A.S. del municipio de Ipiales, fue sometida a una auditoría de sistemas, para detectar y evaluar vulnerabilidades, amenazas y riesgos en los procesos que afectan la seguridad informática y de la información.

El presente informe contiene información y documentación que fue suministrada por la entidad auditada, así como también la recolección de datos y hallazgos detectados por el equipo auditor. La evaluación se realizó en el periodo comprendido entre septiembre de 2015 y enero de 2016. Los resultados que se obtuvieron fueron los siguientes.

Hallazgos.

No existe un manual de funciones actualizado, el personal clave e Indispensable para el funcionamiento del sistema de información y del área de sistemas no está disponible de forma permanente por lo cual los planes de contingencia para el reemplazo del personal clave en esta área no están definidos. No existen planes, programas o un cronograma para capacitación continua dentro de la empresa.

Las políticas y procedimientos para el análisis y gestión del riesgo para las TI, carecen de elementos fundamentales para garantizar la minimización del riesgo, no se evidencia la existencia de un documento en donde se muestre el proceso para la adquisición de equipos de cómputo y en general de hardware y software.

El mantenimiento preventivo y correctivo no se realiza con la evidencia requerida para este proceso, en caso de presentarse daños, no se cuenta con los procesos adecuados para solventar este percance, los procedimientos o planes de contingencia para asegurar la información no se encuentran definidos. Para

acceder e interactuar con el sistema de Información, no existen políticas para la creación y administración de las contraseñas que diariamente emplean los usuarios. Por otra parte el sistema de información carece de un software licenciado y especializado para la detección y eliminación de virus, troyanos, gusanos, etc. Las copias de seguridad del sistema de Información no se encuentran bien protegidas por lo cual la integridad de la información es vulnerable.

No existe un procedimiento de seguridad que actualmente se lleva a cabo para controlar el acceso y la salida de las instalaciones de la empresa, la señalización en caso de presentarse un evento natural no está definidas.

Aspectos positivos.

Los funcionarios tienen conocimiento del organigrama de la empresa lo cual facilita la ubicación de sus área de trabajo, en caso de presentarse un impase en los equipos de TI logran identificar el personal clave del área de sistemas.

Todos los operarios del sistema de información manejan el mismo correo electrónico asociado a la empresa, sus conocimientos en el sistema de información tienen fundamentos sólidos, ya que se les brindo capacitación inicial sobre las funcione a desempeñar.

Se tiene distribución adecuada en cuanto a iluminación, espacio de trabajo, papelería, utensilios de oficina, Las instalaciones se limpian con la frecuencia, en caso de presentarse una falla eléctrica Se cuenta con planta eléctrica para evitar el cese de actividades.
Los funcionarios consideran que se debe brindar capacitaciones para un mejor desarrollo de las funciones y lograr con esto mayor eficiencia y eficacia en cada área de trabajo.

Recomendaciones:

- Identificación clara de los diferentes roles o cargos que los funcionarios pueden desempeñar.
- Definición de las funciones que los usuarios deben desempeñar de acuerdo con el rol que tengan.
- Definición de responsabilidades de cada uno de los usuarios.
- Debe existir dentro del personal de la empresa, por lo menos un funcionario que tengan los conocimientos necesarios para proveer soporte al Sistema de Información.
- La persona encargada de esta área debe tener conocimientos necesarios para dicho fin, preferiblemente un profesional en ingeniería de sistemas, o en su defecto tecnólogo en sistemas o técnico en sistemas.
- Se debe tener en cuenta las políticas y procedimientos para el análisis y gestión del riesgo para las TI en la empresa.

- Se debe crear un documento en donde se describa el proceso de adquisición o compra de software y hardware en la empresa.
- El proceso de mantenimiento preventivo y correctivo a los equipos de cómputo de la empresa y en general al hardware debe estar documentado.
- El proceso que deben seguir cuando se presente un daño en los equipos de cómputo o hardware, debe estar documentado.
- Implementar unas políticas de seguridad para salvaguardar las diferentes copias de seguridad existentes en la empresa para que estas puedan ser utilizadas en una catástrofe que pueda ocurrir.
- Capacitar a los usuarios para que tengan conocimiento de los riesgos o situaciones que puedan interrumpir los procesos.
- Debe existir un plan de seguridad documentado para garantizar la continuidad de los servicios de TI para el sistema de información.
- Deben existir políticas que reglamenten la creación y administración de contraseñas para acceder al sistema de información.
- Para garantizar la seguridad lógica de la información almacenada en los equipos de la empresa, se debe contar con un software especializado en la detección y eliminación de software dañino (virus, troyanos, gusanos, etc.) además debe contar con un dispositivo tipo hardware que funcione como firewall.
- Realizar un plan o cronograma para capacitación continua de los usuarios del sistema de información.
- Deben existir procedimientos de seguridad para controlar el acceso y la salida de las instalaciones de la empresa.
- Los equipos de cómputo (servidores, patchpanel, routers, switchs, etc.) que soportan y garantizan el correcto funcionamiento del sistema de Información deben permanecer en un lugar adecuado (centro de cómputo).
- Se debe crear un plan de evacuación en caso de presentarse un evento catastrófico dentro de la empresa.
- Deben existir e implementarse medidas de seguridad en la empresa, que garanticen la integridad física de las copias de seguridad del Sistema de Información.

Atentamente,

EDWARD CAMILO MUÑOZ
Auditor

EDWIN ROBERT VELASCO
Auditor

Informe general de auditoría.

Objetivo general.
Identificar las vulnerabilidades, amenazas y riesgos en los procesos que afectan la seguridad informática y de la información, empleando la planificación de una auditoria, de acuerdo al estándar COBIT en la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales, Nariño.

Objetivos específicos:
- Conocer el área de informática y los procesos internos de la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales – Nariño.
- Identificar y analizar las diferentes vulnerabilidades, amenazas y riesgos que afectan la seguridad informática y de la información.
- Diseñar los instrumentos para la recolección de la información como pruebas o evidencias de los hallazgos encontrados.
- Aplicar los instrumentos diseñados, realizar las pruebas, ejecutar el proceso de análisis y evaluación de riesgos para su valoración.
- Elaborar y entregar el informe final con los riesgos confirmados y controles propuestos.

Limitaciones.

La auditoría se realizó de forma normal y adecuada, llevando a cabo cuestionarios cuantitativos, encuestas y entrevistas a los funcionarios de la empresa objeto de estudio.

Resultados obtenidos de la auditoria.

A continuación se detallan hallazgos y recomendaciones para cada uno de los procesos evaluados en la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales – Nariño.

DOMINIO DE PLANEACION Y ORGANIZACIÓN (PO).
P04 Definir los procesos, la organización y las relaciones de TI.
HALLAZGOS:
- No existe un manual de funciones actualizado o acorde a las funciones que realiza cada funcionario o usuario del sistema de información de la empresa de transporte TransAndes S.A.S.
- No existe personal clave e Indispensable para el funcionamiento del sistema de Información y del área de sistemas de la empresa de transporte TransAndes S.A.S.
- No se tiene planes de contingencia para el reemplazo en caso de ausencia del personal clave en el área de sistemas de la empresa de transporte TransAndes S.A.S.

RECOMENDACIONES:

- Identificación clara de los diferentes roles o cargos que los funcionarios pueden desempeñar.
- Definición de las funciones que los usuarios deben desempeñar de acuerdo con el rol que tengan.
- Definición de responsabilidades de cada uno de los usuarios.
- Se debe dar a conocer a los usuarios el manual de funciones el cual también debe contener recomendaciones de procesos a seguir por parte de los usuarios para garantizar la seguridad de la información.
- Estar en continua actualización de las funciones desempeñadas por los usuarios.
- Debe existir dentro del personal de la empresa, por lo menos un funcionario que tengan los conocimientos necesarios para proveer soporte al sistema de Información de la empresa de transporte TransAndes S.A.S., y en general brindar soporte técnico a como jefe del área de sistemas.
- La persona encargada de esta área debe tener conocimientos necesarios para dicho fin, preferiblemente un profesional en ingeniería de sistemas, o en su defecto tecnólogo en sistemas o técnico en sistemas.
- En caso de ausencia del personal clave en el área de sistemas, se debe determinar un personal de reemplazo para tal fin.
- El personal de reemplazo debe tener conocimientos básicos del sistema de información.
- Capacitar a los usuarios del sistema para que puedan solucionar problemas comunes o de baja relevancia.
- Realizar simulacros en donde se manifieste la ausencia del personal clave en sistemas.
- Implementar un manual de usuario del sistema de información que sirva de guía para la solución de errores.
- Documentar los errores presentados en el sistema de información y sus posibles soluciones como bitácora de consulta.

P09 Evaluar y administrar los riesgos de TI.

HALLAZGOS:

- Las políticas y procedimientos para el análisis y gestión del riesgo para las TI, dentro de la empresa de transporte TransAndes S.A.S. y específicamente para el sistema de Información, carecen de elementos fundamentales para garantizar la minimización del riesgo.

RECOMENDACIONES:

Se debe tener en cuenta las políticas y procedimientos para el análisis y gestión del riesgo para las TI en la empresa de transporte TransAndes S.A.S., las cuales deben abarcar los siguientes temas:

- La definición del contexto de la entidad.
- El establecimiento de los objetivos que se pretende alcanzar con la aplicación de la gestión del riesgo.
- La identificación de los activos del sistema de Información.
- La identificación y clasificación de los riesgos a los que se encuentran expuestos los activos de los sistemas de Información.
- La determinación de la probabilidad de ocurrencia de los riesgos que amenazan los activos de los Sistemas de Información.
- La determinación del impacto que causaría la ocurrencia de los riesgos.
- La identificación de controles que mitiguen los riesgos.
- La toma de decisiones frente a los riesgos
- La elaboración del plan de seguridad informática.

DOMINIO DE ADQUISICION E IMPLEMENTACION (AI).

AI3 Adquirir y mantener infraestructura tecnológica.
HALLAZGOS:

- En la empresa de transporte TransAndes S.A.S., no se evidencia la existencia de un documento en donde se muestre el proceso para la adquisición de equipos de cómputo y en general de hardware, así como la adquisición o compra de software para el mejoramiento de los procesos en el sistema de información.
- No se encuentra evidencia de la existencia de procesos sobre el mantenimiento preventivo de los equipos de cómputo en la empresa de transporte TransAndes S.A.S.
- No se encuentra evidencia de la existencia de procesos sobre el mantenimiento correctivo de los equipos de cómputo en la empresa de transporte TransAndes S.A.S.
- No se evidencia la existencia de un documento en donde se explique el proceso que se debe seguir cuando se presenta un daño en un equipo de cómputo perteneciente al sistema de información de la empresa de transporte TransAndes S.A.S.

RECOMENDACIONES:

Se debe crear un documento en donde se describa el proceso de adquisición o compra de software y hardware en la empresa de transporte TransAndes S.A.S., este proceso debe contener lo siguiente:
Con respecto al hardware:

- Solicitud por escrito del hardware solicitado, en donde se describan las características principales, la función para la cual se la va a utilizar.
- Solicitar al menos tres (3) cotizaciones del hardware a adquirir, preferiblemente dos (2) cotizaciones locales y una (1) de otra ciudad, en donde especifique los costos, características y soporte técnico y garantía.
- Análisis de las cotizaciones de acuerdo a comparaciones o cuadros comparativos y elección de la mejor propuesta de acuerdo a costo beneficio.
- Asignación a través de acta del hardware adquirido a la persona que lo va a utilizar, agregándolo en el inventario personal y de la empresa.
- Creación de la hoja de vida del hardware adquirido.
- Este proceso debe estar plasmado dentro de las políticas de la empresa para poder garantizar transparencia en el proceso.

Con respecto al software:

- Solicitud por escrito del software solicitado, en donde se describan las características principales, los requerimientos de hardware y los procesos o funciones que se van a ejecutar con él.
- Solicitar al menos tres (3) cotizaciones del software a adquirir especificando costos de licencia en caso de ser software pagado, versión, características y soporte técnico.
- Análisis de las cotizaciones de acuerdo a comparaciones o cuadros comparativos y elección de la mejor propuesta de acuerdo a costo beneficio.
- Instalación del software en los equipos o equipo al cual fue adquirido el software, es decir teniendo en cuenta si la licencia es para uno o varios equipos. Este proceso será llevado a cabo por el personal de sistemas de la empresa en caso de ser software libre o pagado, y en caso de ser software a la medida debe ser instalado por el desarrollador.
- En caso de ser software desarrollado se debe exigir el manual de usuario del software para tener control del mismo en los procesos.
- Realizar el proceso de capacitación al personal que va a estar en contacto con el software.
- Este proceso debe estar plasmado dentro de las políticas de la empresa para poder garantizar transparencia en el proceso.

El proceso de mantenimiento preventivo a los equipos de cómputo de la empresa de transporte TransAndes S.A.S. y en general al hardware debe estar documento y asignado dentro del manual de funciones al encargado del área de sistemas de la empresa para su conocimiento y ejecución. Este proceso debe estar programado dos (2) o cuatro (4) veces al año, para que de esta forma no se cruce con las actividades propias de los usuarios en los equipos. El proceso debe tener:

- Instalación, configuración y actualización de los programas antivirus.
- Escaneo periódico de los equipos de cómputo, utilizando los programas antivirus.
- Desfragmentación periódica de los discos duros.
- Eliminación de archivos temporales y de software malicioso o no permitido.

- Limpieza física de los equipos de cómputo utilizando sopladora, cremas y productos de limpieza.

El proceso que se debe seguir para la realización de un mantenimiento correctivo en los equipos de cómputo que se encuentran en el sistema de información de la empresa de transporte TransAndes S.A.S., debe estar documentado y plenamente conocido por el personal de sistemas. Y debe continuar con lo siguiente:

- Pruebas de funcionamiento de cada uno de los dispositivos (CPU, RAM, board, tarjeta de red, tarjeta de video, mouse, teclado, monitor, cables de poder, etc.) que conforman el equipo de cómputo o hardware.
- Reparación o adquisición del dispositivo defectuoso.
- Reemplazo del dispositivo defectuoso.
- Pruebas de funcionamiento después de haber realizado el mantenimiento.
- Diligenciamiento de un acta en donde especifique el cambio de dispositivo defectuoso, área a quien pertenece el equipo de cómputo, fecha, observaciones. Esta acta debe ser agregada a la hoja de vida del computador o terminal.

El proceso que deben seguir los clientes de los terminales del sistema de información de la empresa de transporte TransAndes S.A.S. cuando se presente un daño en los equipos de cómputo o hardware, debe estar documentado, de cumplimiento obligatorio y se debe seguir así:

- Se debe realizar una solicitud por parte del cliente asignado a la terminal con el daño en el hardware o software. Esta solicitud debe ser realizado de acuerdo a un formato que se debe crear para este fin y dirigido al jefe de área de sistemas de la empresa.
- Entrega y recepción del funcionario que solicita el servicio de mantenimiento correctivo y del personal que va a realizar el mantenimiento.
- Revisión y arreglo de acuerdo a las políticas y procedimientos estipulados para estos fines.
- Firma a satisfacción del funcionario que solicita el servicio.
- El acta de entrega, recepción y firma a satisfacción debe llevar copia para poder ser adjuntada a la hoja de vida del equipo o del hardware.

DOMINIO DE ENTREGAR Y DAR SOPORTE (DS).
DS4 Garantizar la continuidad del servicio.
HALLAZGOS:

- No existen procedimientos o planes de contingencia para asegurar la información, en caso de ataques físicos o lógicos a los equipos y al sistema de información de la empresa que permita la continuidad del desarrollo de los procesos normales, luego de una falla total en el sistema principal.

RECOMENDACIONES:

- Implementar unas políticas de seguridad para salvaguardar las diferentes copias de seguridad existentes en la empresa para que estas puedan ser utilizadas en una catástrofe que pueda ocurrir.
- Elaborar una bitácora o repositorio documentado de desastres ocurridos en la empresa donde se registren los problemas más comunes, ya que este será una guía para problemas que se pueden repetir en un futuro.
- Capacitar a los usuarios para que tengan conocimiento de los riesgos o situaciones que puedan interrumpir los procesos.

DS5 Garantizar la seguridad de los sistemas.

HALLAZGOS:

- No existen planes de seguridad documentados en la empresa de transporte TransAndes S.A.S., para garantizar la seguridad lógica de los sistemas de información que se manejan.
- No existen políticas dentro de la empresa de transporte TransAndes S.A.S, para la creación y administración de las contraseñas que diariamente emplean los usuarios para acceder e interactuar con el sistema de Información.
- El sistema de información carece de un software licenciado y especializado para la detección y eliminación de software dañino (virus, troyanos, gusanos, etc.)

RECOMENDACIONES:

Deben existir en la empresa de transporte TransAndes S.A.S, un plan de seguridad documentado para garantizar la continuidad de los servicios de TI para el sistema de información. Estas políticas deben:

- Autenticación y acceso.
- Administración de perfiles de usuario y clasificación de la seguridad de datos.
- Reportes y revisión de las violaciones e incidentes de seguridad.
- Aplicación de estándares de administración de llaves criptográficas.
- Detección, resolución y comunicación sobre los virus.
- Clasificación y propiedad de los datos.
- Estas políticas deben estar documentadas y ser de obligatoria cumplimiento.

Deben existir políticas dentro de la empresa de transporte TransAndes S.A.S., que reglamenten la creación y administración de contraseñas para acceder al sistema de información. Estas políticas deben contemplar:

- Cambio inicial de las contraseñas la primera vez de uso.
- Establecer una longitud adecuada mínima de las contraseñas.
- Combinaciones de alfanuméricas obligatorias en las contraseñas.
- Verificación de la contraseña en la lista de valores no permitidos.

- Cambio periódico de las contraseñas.
- Protección adecuada de las contraseñas.
- Estas políticas deben estar documentadas, deben ser de conocimiento de los usuarios que interactúan con el Sistema de Información y deben ser de obligatorio cumplimiento.
- Para garantizar la seguridad lógica de la información almacenada en los equipos de la empresa, se debe contar con un software especializado en la detección y eliminación de software dañino (virus, troyanos, gusanos, etc.) además debe contar con un dispositivo tipo hardware que funcione como firewall.
- Realizar de manera periódica una búsqueda de (virus, troyanos, gusanos, etc.) para poder controlarlos y eliminarlos de manera que no se generen problemas futuros en los equipos y por ende pérdida de información o falla total del equipo.
- Realizar de manera periódica una limpieza de software que no contribuye a las funciones propias de la empresa.

DS7 Educación y entrenamiento de usuarios.

HALLAZGOS:

- No existen planes, programas o un cronograma para capacitación continua dentro de la empresa, además no se ha brindado capacitaciones sobre las buenas prácticas en seguridad informática a los usuarios del sistema de información de la empresa de transporte TransAndes S.A.S.

RECOMENDACIONES:

- Realizar un plan o cronograma para capacitación continua de los usuarios del sistema de información de la empresa de transporte TransAndes S.A.S.
- Programar como mínimo dos capacitaciones al año sobre las buenas prácticas en seguridad informática.

DS12 Administrar el ambiente físico.

HALLAZGOS:

- No existe un procedimiento de seguridad que actualmente se lleva a cabo para controlar el acceso y la salida de las instalaciones de la empresa, para de esta manera brindar un buen nivel de tipo de seguridad para los activos de TI del sistema de información.
- No existe en las instalaciones de la empresa de transporte TransAndes S.A.S., ni fuera de ellas, un lugar reservado y con las características ambientales y de seguridad para albergar los equipos que soportan el funcionamiento del sistema de información. No existe el centro de cómputo.

- No existe señalización en caso de presentarse un evento catastrófico, mas no se cuenta con un plan de evacuación como tal dentro de las instalaciones de la empresa de transporte TransAndes S.A.S.
- No existen en la empresa de transporte TransAndes S.A.S, medidas de seguridad que garanticen la integridad física de las copias de seguridad del sistema de información.
- No existen en las instalaciones de la empresa de transporte TransAndes S.A.S., medidas de seguridad o aislamientos que aseguren la integridad física del cableado (UTP, eléctrico, etc.) que no se encuentra integrado a la estructura del edificio.

RECOMENDACIONES:

Deben existir procedimientos de seguridad para controlar el acceso y la salida de las instalaciones de la empresa de transporte TransAndes S.A.S., Estos procedimientos deberán asegurar que:

- Todas las personas que entran a las instalaciones de la empresa, se identifique, sean autenticados y autorizados para entrar.
- La realización de requisas a las personas que ingresan y que salen de las instalaciones.
- EI registro de los equipos de cómputo (portátiles, PC, etc.) que ingresan a las instalaciones.

Los equipos de cómputo (servidores, patchpanel, routers, switchs, etc.) que soportan y garantizan el correcto funcionamiento del sistema de Información deben permanecer en un lugar adecuado (centro de cómputo) y que satisfaga los requerimientos de:

- Espacio y movilidad: características de las salas, altura, anchura, posición de las columnas, posibilidades de movilidad de los equipos, suelo móvil o falso suelo, etc.
- Iluminación: el sistema de iluminación debe ser apropiado para evitar reflejos en las pantallas, falta de luz en determinados puntos, y se evitará la incidencia directa del sol sobre los equipos.
- Tratamiento acústico: los equipos ruidosos como las impresoras con impacto, equipos de aire acondicionado o equipos sujetos a una gran vibración, deben estar en zonas donde tanto el ruido como la vibración se encuentren amortiguados.
- Sistemas de ventilación: las instalaciones del centro de cómputo deben contar con adecuados sistemas de ventilación y disipadores de calor, para evitar daños en los equipos por recalentamiento.
- Seguridad física: las instalaciones del centro de cómputo cuentan con sistema contra incendios; los materiales del centro de cómputo son incombustibles (pintura de las paredes, suelo, techos, mesas, estanterías, etc.). Existen protecciones contra inundaciones y otros peligros físicos que puedan afectar a las instalaciones.

- Suministro eléctrico: el suministro eléctrico a un centro de cómputo, y en particular la alimentación de los equipos, debe hacerse con unas condiciones especiales, como la utilización de una línea independiente del resto de la instalación para evitar interferencias, con elementos de protección y seguridad específicos y en muchos casos con sistemas de alimentación ininterrumpida (equipos electrógenos, instalación de baterías, etc.).

Se debe crear un plan de evacuación en caso de presentarse un evento catastrófico dentro de la empresa que considere ítems tales como:

- Instalar una señal de alarma (timbre, campana, silbato) que será muy relevante y de fácil reconocimiento por todos los actores institucionales, los cuales ante esta situación se encaminarán hacia la puerta de salida.
- Señalización de las paredes con una flecha roja direccional acompañada de la palabra SALIDA a una altura de 2 m, en corredores, escaleras, rampas, etc.

También se deberá:

- Garantizar una salida rápida y segura hacia el exterior.
- Dar a cargo la toma de decisión de evacuación y orden a una persona responsable.
- El trayecto de escape deberá estar libre de obstrucciones o entorpecimiento de circulación.
- Se establecerán roles y responsabilidades para el personal de la empresa.
- Se deben realizar simulacros de evacuación.
- Los extintores y otros elementos de protección se controlarán periódicamente, y se capacitará al personal acerca de su uso.
- El plan de evacuación debe estar documentado y debe ser de conocimiento de todos los funcionarios de la empresa.

Deben existir e implementarse medidas de seguridad en la empresa, que garanticen la integridad física de las copias de seguridad del sistema de información. Algunas de estas medidas son:

- Los medios de almacenamiento físico (CD, DVD, cintas magnéticas, etc.) en donde se encuentran las copias de seguridad del Sistema de Información, deben guardarse bajo llave.
- Solo las personas autorizadas pueden tener acceso a las copias de seguridad.
- Debe existir un sitio fuera de las instalaciones de la empresa, en donde se almacenen las copias de seguridad.
- Los sitios dentro y fuera de las instalaciones de empresa, que sirvan para almacenar las copias de seguridad, deben contar con factores ambientales (humedad, iluminación, ventilación, etc.) óptimos, que garanticen la integridad de los medios de almacenamiento.
- El cableado (UTP, eléctrico, etc.) que no se encuentre incorporado a la estructura del edificio de la empresa, bebe contar con medidas de aislamiento que garanticen su seguridad y su integridad.
    - Se recomienda el uso de canaletas para proteger estos activos de TI.

4. CONCLUSIONES

En esta auditoría desarrollada en la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales, se desarrollaron procesos de evaluación al sistema informático y de información de la empresa, con el fin de identificar vulnerabilidades, amenazas y riesgos que se puedan presentar, tanto en la infraestructura, en el hardware, en el software, en el talento humano.

Todo este desarrollo de la auditoría se debió en primer lugar al conocimiento integral de los procesos que afectan la seguridad informática y de la información con vulnerabilidades, amenazas y riesgos en la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales, Nariño.

Se planificó de acuerdo al estándar de auditoria COBIT 4.0. Identificando los procesos asociados a cada dominio del estándar y que pudieran tener algún riesgo al interior de la empresa. Para esto se hizo necesario la construcción de cuadros de fuentes de conocimiento, cuestionarios cuantitativos para tener una primera impresión de cómo se encuentra la seguridad informática y de la información.

Para continuar con el proceso de hizo necesario la implementación de encuestas y entrevistas a los usuarios del sistema de información de la empresa, en donde se pudo confirmar los hallazgos encontrados concernientes a la seguridad informática y de información.

Se propusieron recomendaciones a los hallazgos encontrados en cada uno de los procesos evaluados, con el fin de que la administración de la empresa pueda tomar decisiones en la generación de controles que minimicen el riesgo.

Por último, se presenta un informe final de resultados, en donde se presentan los hallazgos y recomendaciones en el informe ejecutivo y un informe general de auditoria más específico para la toma de decisiones por el personal clave del área de sistemas de la empresa.

5. RECOMENDACIONES

Implementar un manual de usuario para las personas que manipulan los diferentes programas de la empresa de transporte TransAndes S.A.S. de la ciudad de Ipiales, Nariño.

Adoptar políticas de seguridad para la implementación de procesos de seguridad que beneficien a la empresa y que siempre se encuentren disponibles.

Implementar simulacros donde puedan verificar el estado la reacción de cada persona para afrontar posible amenazas como la entrada de personas que tengan intenciones de causarles daño físico o psicológico, para que así el personal este más atento y maneje un proceso que se ira creando según la necesidad de la empresa

Implementar un cronograma de capacitaciones y actividades ya sean semanales o mensuales para fomentar en los usuarios las buenas prácticas sobre seguridad informática y garantizar un mejor desempeño de cada uno de ellos.

BIBLIOGRAFIA

ARENS, ALVIN A. Auditoria un Enfoque Integral. 6 Edición. México: Prentice Hall, 1996.

CAICEDO, Liliana. ORDONEZ, Claudia. Técnicas de Auditoria de Sistemas Aplicadas al Proceso de Contratación y Páginas Web en Entidades Oficiales del Departamento de Nariño. Universidad de Nariño. 2010.

ECHENIQUE GARCIA, José A., Auditoría en informática, 2da Ed., Me GRAW-HILL,
México D.F., 2005.

SOLARTE, Francisco Nicolás, GUSTÍN Enith, HERNANDEZ Ricardo. Manual De Procedimientos para Llevar a la Práctica La Auditoría Informática y de Sistemas, lUCESMAG, Pasto, 2013.

BIBLIOWEB

http://es.wikipedia.org/wiki/COBIT

http://www.gerencie.com/auditoria-de-sistemas-de-informacion.html

http://www.isacabogota.net/metodologias/cobit.aspx

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

ANEXOS

- **Anexo 1: Manual de funciones TransAndes S.A.S.:**

Se encuentran en la carpeta ANEXOS TRANSANDES SAS consta del archivo llamado: Anexo 1 NATURALEZA JURIDICA TRANSANDES SAS MANUAL DE FUNCIONES.docx

- **Anexo 2: Cuadros de definición de fuentes de conocimiento:**

Se encuentran en la carpeta ANEXOS TRANSANDES SAS consta del archivo llamado: Anexo 2 CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO TRANSANDES SAS.docx

- **Anexo 3: Cuestionarios:**

Se encuentran en la carpeta ANEXOS TRANSANDES SAS consta del archivo llamado: Anexo 3 CUESTIONARIO CUANTITATIVO TRANSANDES SAS.docx

- **Anexo 4: Encuestas:**

Se encuentran en la carpeta ANEXOS TRANSANDES SAS consta del archivo llamado: Anexo 4 ENCUESTAS TRANSANDES SAS.docx

- **Anexo 5: Entrevistas:**

Se encuentran en la carpeta ANEXOS TRANSANDES SAS consta del archivo llamado: Anexo 5 ENTREVISTAS TRANSANDES SAS.docx

- **Anexo 6: Hallazgos:**

Se encuentran en la carpeta ANEXOS TRANSANDES SAS consta del archivo llamado: Anexo 6 HALLAZGOS TRANSANDES SAS.docx

- **Evidencias Fotográficas:**

Se encuentra una carpeta llamada ANEXOS TRANSANDES SAS y se encuentran insertadas en el desarrollo de los hallazgos en el archivo: Anexo 6 HALLAZGOS TRANSANDES SAS.docx

- **Anexo 7: Evidencias de audio:**

Se encuentra una carpeta llamada ANEXOS TRANSANDES SAS y consta de archivo llamado: Anexo 7 ENTREVISTA TRANSANDES SAS.mp3.