AUDITORÍA INFORMÁTICA A LOS PROCESOS Y ORGANIZACIÓN DEL ÁREA DE SISTEMAS EN LA EMPRESA AGROPEZ LTDA DE LA CIUDAD DE IPIALES

FERNANDO JAVIER PEPINOSA ORTEGA
JOSE ANDRES SALAZAR ARAUJO

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

AUDITORÍA INFORMÁTICA A LOS PROCESOS Y ORGANIZACIÓN DEL ÁREA DE SISTEMAS EN LA EMPRESA AGROPEZ LTDA DE LA CIUDAD DE IPIALES

FERNANDO JAVIER PEPINOSA ORTEGA
JOSE ANDRES SALAZAR ARAUJO

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

Asesor:
MANUEL BOLAÑOS GONZÁLEZ
Ingeniero de Sistemas

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

NOTA DE RESPONSABILIDAD

Las ideas y conclusiones aportadas en este Trabajo de Grado son Responsabilidad de los autores.

Artículo 1 del Acuerdo No. 324 de octubre 11 de 1966, emanado por el Honorable Consejo Directivo de la Universidad de Nariño.

“La Universidad de Nariño no se hace responsable de las opiniones o resultados obtenidos en el presente trabajo y para su publicación priman las normas sobre el derecho de autor”.

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

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____
Presidente de tesis

_____
Jurado

_____
Jurado

San Juan de Pasto, Febrero de 2016

AGRADECIMIENTOS

A mis padres y familiares, por su apoyo, comprensión y colaboración incondicional y permanente.

Al Ingeniero Manuel Bolaños, Asesor del proyecto, por su tiempo, paciencia y asistencia continúa durante el desarrollo del proyecto.

A nuestros amigos y compañeros, por ser partícipes en el proceso de esta etapa de nuestra vida.

A nuestros profesores, por compartir con nosotros sus conocimientos y experiencias.

A Yesyca Chávez, por creer en mí y darme esa voz de aliento para culminar mi carrera.

Y a todas aquellas personas que contribuyeron en la realización de este proyecto.

Fernando Javier Pepinosa Ortega

DEDICATORIA

Dedico este trabajo a mis padres, Ángel Felipe Pepinosa Narváez, Clemencia Ortega, a mis hermanos, familiares y a todos los que de una u otra manera contribuyeron a obtener este gran logro en la vida.
A la Universidad de Nariño, a todos los docentes y compañeros que me dieron la oportunidad de alimentar mis conocimientos.

Fernando Javier Pepinosa Ortega

RESUMEN

HOY EN DÍA, LAS EMPRESAS DEBEN ACOGER LAS LEYES PLANTEADAS A LA PARTE INFORMÁTICA Y DE COMUNICACIONES PARA NO TENER PROBLEMAS CON LOS ÓRGANOS DE CONTROL ENCARGADOS COMO LA CONTRALORÍA PARA NO INFRINGIR ALGUNA NORMA, ADEMÁS, ES MUY IMPORTANTE LA EJECUCIÓN DE AUDITORÍAS PARA LA DETERMINACIÓN DE RIESGOS, VULNERABILIDADES Y AMENAZAS QUE LAS EMPRESAS ENFRENTAN EN SUS ACTIVIDADES DIARIAS, LAS BUENAS PRÁCTICAS EN LOS DIFERENTES ÁMBITOS SE DEBEN MANEJAR PARA QUE LAS COSAS FUNCIONEN ADECUADAMENTE Y ASÍ, MEJORAR CONTINUAMENTE SU DESEMPEÑO EMPRESARIAL.

PARA EJECUTAR EL PROCESO DE AUDITORIA SE TOMÓ COMO MARCO DE REFERENCIA EL MODELO “COBIT” (OBJETIVOS DE CONTROL PARA TECNOLOGÍAS DE LA INFORMACIÓN), SELECCIONANDO LOS PROCESOS DE CADA DOMINIO QUE FUERON APLICADOS SEGÚN LOS OBJETIVOS DE ESTE PROYECTO.

LA AUDITORIA INFORMÁTICA SE REALIZÓ A LA EMPRESA AGROPEZ LTDA DEL MUNICIPIO DE IPIALES, CON EL FIN DE DAR RECOMENDACIONES PARA FORTALECER Y MEJORAR LOS PROCESOS Y ORGANIZACIÓN EN EL ÁREA DE SISTEMAS, ANALIZANDO LA INFORMACIÓN SUMINISTRADA POR LA INSTITUCIÓN AUDITADA Y LA RECOLECTADA POR EL EQUIPO AUDITOR.

ABSTRACT

TODAY, COMPANIES MUST ACCEPT THE LAWS POSED TO COMPUTER PART AND COMMUNICATIONS TO AVOID PROBLEMS WITH THE SUPERVISORY BODIES RESPONSIBLE AS THE COMPTROLLER TO AVOID VIOLATING ANY RULE ALSO IS VERY IMPORTANT CONDUCTING AUDITS TO DETERMINE RISKS, VULNERABILITIES AND THREATS THAT COMPANIES FACE IN THEIR DAILY ACTIVITIES, GOOD PRACTICES IN DIFFERENT AREAS SHOULD BE MANAGED TO MAKE THINGS WORK PROPERLY AND THUS CONTINUALLY IMPROVE THEIR BUSINESS PERFORMANCE.

TO RUN THE AUDIT PROCESS WAS TAKEN AS A REFERENCE MODEL "COBIT" (CONTROL OBJECTIVES FOR INFORMATION TECHNOLOGY), SELECTING THE PROCESSES OF EACH DOMAIN WERE APPLIED ACCORDING TO THE OBJECTIVES OF THIS PROJECT.

COMPUTER AUDIT WAS CONDUCTED AT THE COMPANY AGROPEZ LTDA TOWNSHIP IPIALES, IN ORDER TO GIVE RECOMMENDATIONS TO STRENGTHEN AND IMPROVE PROCESSES AND ORGANIZATION IN THE AREA OF SYSTEMS, ANALYZING THE INFORMATION PROVIDED BY THE AUDITED INSTITUTION AND COLLECTED BY THE AUDIT TEAM .

CONTENIDO

Pág.

LISTADO DE FIGURAS

Pág.

LISTADO DE TABLAS

Pág.

LISTADO DE ANEXOS

(Anexos en medio digital)

ANEXO 1. Fuentes de conocimiento.docx
ANEXO 2. Cuestionarios cuantitativos.docx
ANEXO 3. Formatos Entrevista.docx
ANEXO 4. Formato Cuestionarios.docx
ANEXO 5. Hallazgos.docx
ANEXO 6. Evidencias.docx

GLOSARIO

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

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.

Auditoría: proceso planificado y sistematico 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.

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

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.

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.

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.

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.

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.

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

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.

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.

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 costo 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.

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

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.

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

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.

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: (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.

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.

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: 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.

Políticas de seguridad: 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.

Proceso: 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.

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.

Riesgo: según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

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

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.

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'.

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

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.

Vulnerabilidad: según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

INTRODUCCION

En la actualidad es de vital importancia la utilización de herramientas informáticas para realizar las tareas diarias, como también, optimizar procesos, por esta razón el proveer a cualquier empresa de tecnología es hoy en día una necesidad primordial, ya que la sistematización trae como resultado mejorar el cumplimiento de los objetivos empresariales y así tener mejor capacidad de adaptación a los cambios asegurando su existencia en el mercado.

Para estar preparado a los problemas emergentes es necesario identificar las vulnerabilidades, riesgos y amenazas que acechan a las organizaciones, luego debe generar políticas, controles, planes que ayuden a reducir el impacto producido dentro de las actividades diarias de la empresa y así estar disponible y prestar los servicios de manera adecuada aun en situaciones que no sean las más óptimas. La Auditoría consiste en apoyar a los miembros de la empresa en el desempeño de sus actividades por tal motivo se hace necesario definir métodos y controles que ayuden a estimar la magnitud del manejo de cada área o de cada proceso que se lleve dentro de la empresa como tal.

AGROPEZ LTDA, es una empresa dedicada a la comercialización y la importación de productos agrícolas y pesqueros en diferentes departamentos de Colombia, como también otros países, llevando un proceso de crecimiento durante quince años desde su fundación, a pesar de esto, y de enfocarse en la efectividad del negocio, se ha descuidado la eficiencia de la organización. Es por ello que la auditoria daría una visión y evaluación de cómo están desempeñando sus funciones enfocando a los objetivos que tienen plasmados.

La aplicación de la auditoría va orientada a evaluar los procesos y organización del área de sistemas, lo cual permitirá obtener un diagnóstico para así definir planes de mejoramiento para la integración de la tecnología a los procesos de la organización.

El presente documento se organizó de la siguiente forma: en la primera parte se planteó el problema y su sistematización, los objetivos que se alcanzaron, luego se habló de los antecedentes directamente relacionados con el proyecto, de la factibilidad y la metodología a seguir. En la última parte se especificó los recursos que se utilizaron así como la distribución del tiempo de las tareas que se programaron para realizarse.

IDENTIFICACION DEL PROBLEMA

Título del proyecto

"AUDITORÍA INFORMÁTICA A LOS PROCESOS Y ORGANIZACIÓN DEL ÁREA DE SISTEMAS EN LA EMPRESA AGROPEZ LTDA DE LA CIUDAD DE IPIALES".

TEMA

Auditoría informática aplicada a los procesos y organización del área de sistemas de la empresa AGROPEZ LTDA de la ciudad de Ipiales.

MODALIDAD

Este trabajo de grado, corresponde a la modalidad de TRABAJO DE APLICACION, a realizarse en la EMPRESA AGROPEZ LTDA de la ciudad de Ipiales. 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, con Acuerdo 045 de octubre 10 de 2002 dado por el Consejo de Facultad, el trabajo 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 Auditoría de Sistemas.

DESCRIPCIÓN DEL PROBLEMA

Al crear las empresas, por lo general, se define muy bien la forma de trabajo, siguiendo lineamientos de acuerdo con las necesidades del negocio que se ha puesto en marcha, sin embargo, al ir creciendo día a día con la dinámica laboral, la empresa se ve obligada a tomar decisiones que cambian poco a poco su forma de trabajo, la estructura, la organización, los cuales pueden causar, con el paso del tiempo, focos enormes de desorganización, caos, confusión, dando paso a la deficiencia en los recursos de la empresa y en inadecuadas ejecuciones de procesos, creando una atmósfera poco favorable para la competitividad.

Los riesgos que aparecen en las empresas que no se autoevalúan constantemente para su reorganización, para la correcta toma de decisiones, para adaptarse a los objetivos planteados, son muy altos, a tal punto de desaparecer

del mercado laboral.

La Información es un recurso vital para las organizaciones, al ser manejado adecuadamente se pueden tomar las decisiones más acertadas, para ser una empresa competitiva se deben analizar los procesos, identificar riesgos, crear controles y generar políticas que faciliten la correcta disposición del trabajo, para ello se necesita en la empresa etapas fundamentales que son la planificación, recursos humanos y materiales, objetivos concretos a corto, medio y largo plazo, aunque también tecnología y técnicas. La empresa AGROPEZ LTDA, cuenta con más de quince años brindado un servicio de calidad a sus clientes, con un crecimiento moderado que ha servido para mantener el negocio durante tanto tiempo adecuándose a las necesidades diarias, sin embargo, en todo el tiempo de funcionamiento no se ha hecho una auditoria a los diferentes aspectos de la empresa y es por ello que puede estar inmersa en un problema grande que atente con el funcionamiento del negocio, parando todas las actividades sin que la empresa se percate del problema hasta que es demasiado tarde.

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

Con el objetivo de obtener un diagnóstico para definir planes de mejoramiento para la integración de la tecnología a los procesos de la empresa surge la necesidad de desarrollar la auditoría “AUDITORÍA INFORMÁTICA A LOS PROCESOS Y ORGANIZACIÓN DEL ÁREA DE SISTEMAS EN LA EMPRESA AGROPEZ LTDA DE LA CIUDAD DE IPIALES” la cual evaluará su eficiencia y eficacia.

OBJETIVOS

Objetivo general. Desarrollar una auditoría informática a los procesos y organización en la empresa AGROPEZ LTDA de la ciudad de Ipiales teniendo en cuenta el modelo estándar de auditoría y mejores prácticas COBIT como herramienta de apoyo en el proceso evaluación de los riesgos existentes y verificación de cumplimiento de controles.

Objetivos específicos:

- Conocer el área de sistemas de la empresa AGROPEZ LTDA, identificando el manejo de información que ahí se desarrolla, como la utilización de los activos informáticos.
- Planear y diseñar los instrumentos y pruebas para identificar vulnerabilidades, riesgos y amenazas al ejecutar la auditoria en los procesos y organización del área de informática en AGROPEZ LTDA.
- Ejecutar pruebas y aplicar instrumentos adecuados para la identificación de hallazgos dentro de los procesos y organización del área de informática en AGROPEZ LTDA.
- Elaborar del informe final con los resultados obtenidos al ejecutar la auditoría informática a la organización.

JUSTIFICACIÓN

Las empresas deben realizar una continua revisión de los procesos que se llevan a cabo, para determinar su idoneidad en ellos, por esto la auditoría informática aplicada a los diferentes aspectos de la empresa generara los hallazgos necesarios para crear elementos de control ante las vulnerabilidades, riesgos y amenazas con los cuales las políticas dispuestas por la empresa generaran un mejor aprovechamiento en los recursos de la empresa y aseguramiento de los activos informáticos.

La empresa AGROPEZ LTDA, lleva bastante tiempo de funcionamiento, desde su creación no se ha hecho una correcta evaluación a los procesos y organización, por ello, se inició por el área de sistemas para determinar las vulnerabilidades, amenazas y riesgos presentes que no se han detectado y hacer sus correspondientes correcciones para el buen funcionamiento de la empresa y así tener mejorar su funcionamiento.

Es importante resaltar que la mala utilización de recursos genera costos innecesarios que podrían cubrir satisfactoriamente otras áreas, es por tanto, que el desarrollo de esta auditoría abrió las puertas a nueva evaluación para las buenas prácticas en otras dependencias de la empresa y crear una cultura de mejoramiento continuo para resaltar en las necesidades del mercado.

La evaluación de los requerimientos, los recursos y procesos IT (Información y tecnología), son muy importantes para el buen funcionamiento de una empresa y para el aseguramiento de su supervivencia en el mercado. El COBIT es precisamente un modelo para auditar la gestión y control de los sistemas de información y la tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso.

Con lo anterior, se logró que la empresa desarrolle planes de mejoramiento que le permita tomar medidas de seguridad y control para salvaguardar mejor los activos informáticos.

ALCANCE Y DELIMITACIÓN

El alcance del proyecto de auditoría de sistemas implicó la evaluación de los procesos y organización en el área de informática de la empresa AGROPEZ LTDA de la ciudad de Ipiales, determinando las posibles causas a los hallazgos que se presentaron en la ejecución de la auditoria, se verificó el cumplimiento de normas y así, optimizando el uso de los recursos para brindar un buen servicio a los usuarios de la empresa.

Los puntos evaluados son los siguientes:

- ***PROCEDIMIENTO DE LAS ACTIVIDADES DEL PERSONAL:*** conocer los procesos de cada trabajador, los equipos necesarios y/o herramientas que necesitan para realizar su trabajo eficientemente.

- ***VERIFICAR LA EXISTENCIA DE UN MANUAL DE FUNCIONES:*** confirmar que se cumplan las funciones establecidas dentro del manual y que se respeten los cargos jerárquicos dentro del organigrama.

- ***PROCEDIMIENTO PARA LA ADQUISICIÓN DE TECNOLOGÍAS:*** se evaluara si la adquisición de tecnología es adecuada y está plasmada en políticas que van alineada con los objetivos de la empresa.

- ***INVENTARIO DE TECNOLOGÍAS DE INFORMACIÓN:*** revisar políticas y procedimientos referentes a inventario de elementos tecnológicos.

Para el proceso de auditoría se utilizó el estándar COBIT como una metodología de buenas prácticas en el uso de las tecnologías de información, y como el estándar más completo para evaluación de riesgos y cumplimiento de objetivos de control informático a nivel mundial.

1. TITULO

“AUDITORÍA INFORMÁTICA A LOS PROCESOS Y ORGANIZACIÓN DEL ÁREA DE SISTEMAS EN LA EMPRESA AGROPEZ LTDA DE LA CIUDAD DE IPIALES”

2. MARCO TEORICO

2.1 ANTECEDENTES

La información es un conjunto de datos que son supervisados y organizados previamente, crea un registro basado en un acto verídico, la información en las empresas es muy importante puesto que aumenta el conocimiento de los individuos ayudando a tomar decisiones para alcanzar los objetivos de la empresa y así, ser más competentes gracias a la información tomada de diferentes medios de su entorno para comprender que es lo que necesita el cliente para poder brindar un mejor servicio. Para poder adquirir información se recurre a las fuentes externas que pueden ser primarias, secundarias, internas y externas.

Las empresas son más competente cuando aprovechan la información que se encuentra en su entorno. Lo que realmente importa dentro de las organizaciones es que la información genere mayor conocimiento en los miembros de la institución para permitirles tomar decisiones que ayuden a alcanzar los objetivos o metas que se han propuesto en la empresa.

Lo relevante de la información en las organizaciones es que debe aumentar el conocimiento de los individuos reduciendo las inseguridades que se tengan, es decir, tener herramientas para la toma de decisiones que conlleven al logro de objetivos y metas propuestas, generando competitividad, esta no solo depende de la capacidad que tenga la institución para poder ofrecer un producto o servicio con mejor precio que el de sus competidores, debe incluir lo que realmente quiere el consumidor o ver lo que es lo que más valora, como la calidad, el servicio o la atención postventa. Para poder lograrlo, la empresa necesita obtener información que se origina en su entorno.

La información debe integrar las unidades de la organización ya que la información que se obtenga en algunas áreas puede ser de gran utilidad para otras aunque aparentemente no estén relacionadas, a esto se adiciona la mejora de los procesos productivos y administrativos, estos se logran gracias a la información que fluye y aumenta el conocimiento de los recursos humanos.

En los últimos años, la tecnología ha cambiado el mundo laboral, generando mayor competitividad y exigiendo adaptación rápida en el manejo de la tecnología, teniendo como resultado un mayor control a 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, además de estar implementando y utilizando la tecnología adecuadamente para las necesidades previstas, lo anterior combinado con la

necesidad de obtener un plan estratégico y corporativo que le 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.

Es por ello que en la empresa AGROPEZ LTDA vio la necesidad de mejorar los procesos llevados a cabo, para lo cual es importante desarrollar el diagnóstico a todos los procesos de información que se vienen ejecutando en el área de sistemas con la ayuda de la realización de auditoría interna para mejorar la manera como se disponen los recursos, sacando el mejor provecho de ellos.

La auditoría se hizo necesaria para la integración de tecnología a los procesos de manejo de la información, porque hasta el momento no se había realizado ningún tipo de evaluación, en los procesos, como también el uso de los activos informáticos que están actualmente en funcionamiento dentro de la organización.

Existen algunos trabajos de auditorías desarrollados por estudiantes de la Universidad de Nariño, en el programa de Ingeniería de Sistemas, de los cuales se ha tenido en cuenta para este trabajo, los cuales son referenciados a continuación:

Título del trabajo: **"**auditoria de sistemas aplicada a los módulos de facturación, consultas e historia clínica del software info-salud en la IPS indígena Guaitara del municipio de Ipiales" realizado por: Melanny Catherine Oviedo Mesías - Oscar Mauricio aza Arévalo, en 2015

Objetivo general: establecer el grado de confiabilidad e integridad de la información de los módulos de facturación, consultas e historia clínica perteneciente al software de gestión de información info-salud montado en el servidor de la IPS indígena Guaitara, y dar las recomendaciones pertinentes.

El trabajo es tomado como referencia dado que permite conocer aspectos relacionados con la ejecución de la auditoria informática, como también las herramientas para su realización.

"Auditoría informática a nivel de los sistemas e indicadores de funcionamiento del hardware y software en la empresa Dispropan S.A.S del departamento de Nariño y putumayo". realizado por: Jhoana Lorena Hernández Benavides, en 2014

Objetivo general: realizar una auditoría que permita evaluar la eficiencia y eficacia del hardware de equipos de cómputo, equipos móviles, los servidores y el funcionamiento del sistema syscafe para en la empresa Dispropan S.A.S, aplicando los procesos de análisis de riesgos y auditoría teniendo en cuenta el modelo estándar de auditoría y mejores prácticas cobit como herramienta de apoyo en el proceso evaluación de los riesgos existentes y verificación de

cumplimiento de controles, con el propósito de ayudar a definir y establecer un plan de mejoramiento e integración de tecnología.

El proyecto sirvió de base para la realización del actual proyecto porque es muy parecida la temática que se tiene y la aplicación.

“Auditoria de sistemas aplicada al sistema de información de la Ips indígena Guaitara del municipio de Ipiales”, ejecutado por: Julio Cesar Burgos - Nelson Andrés Cortes Bernal, en 2013.

Objetivo general: aplicar técnicas de auditoria al sistema de información de la Ips indígena Guaitarra que contribuyan a evidenciar vulnerabilidades en la seguridad física y lógica a los que se encuentra expuesta.

El trabajo es tomado como referencia dado que permite conocer aspectos relacionados con la empresa, en tanto que evalúa su seguridad física y lógica a nivel general en la organización, permitiendo entender que todo funciona como un sistema y lo que afecte a un componente afectara a la organización.

“Auditoría de sistemas aplicada al sistema integral de información en la secretaría de planeación municipal de la alcaldía de Pasto”, realizado por: Oscar Julián Estrada Obando, En 2009

Objetivo general: “ejecutar auditoria al sistema integral de información a la secretaria de planeación municipal de la alcaldía de pasto que contribuyan a evidenciar vulnerabilidades en la seguridad física y lógica a los que se encuentra expuesta el sistema integral de información”.

El trabajo es tomado como referencia dado que permite conocer aspectos relacionados con la empresa, en tanto que evalúa su seguridad física y lógica a nivel general en la organización, permitiendo entender el funcionamiento integral del sistema y cómo puede afectar cada uno de sus componentes.

Título del trabajo: “auditoria del módulo de historia clínica electrónica del sistema de información en el hospital universitario departamental de Nariño” realizado por: Jenny Nayibi Burgos – María Carolina Domínguez.

Año de publicación: 2009.

Objetivo general: evaluar el proceso y el módulo de historias clínicas electrónicas, que garanticen la confiabilidad, integridad y seguridad permitiendo adelantar actividades de mejoramiento del sistema del hospital universitario departamental de Nariño E.S.E.

El proyecto es tomado como referencia puesto que evalúa el proceso de entrada, salida y procesamiento de datos; estableciendo controles y recomendaciones a esta institución de salud.

2.2 ASPECTOS GENERALES DE LA AUDITORÍA

2.2.1 Definición de auditoria. La auditoría es una serie de métodos de investigación y análisis con el objetivo de producir la revisión y evaluación profunda de la gestión efectuada[1]. Básicamente la auditoria consiste en emitir un concepto profesional sobre si el objeto o situación en estudio de qué forma cumple o no las condiciones que le han sido prescritas.

Con frecuencia la palabra auditoría se ha empleado incorrectamente y se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas; por eso se ha llegado a utilizar la palabra "auditoría" como sinónimo de que desde antes de realizarse, ya se encontraron fallas y por lo tanto se está haciendo la auditoría. El concepto de auditoría es más amplio: no sólo detecta errores, sino que es un examen técnico que se realiza con objeto de evaluar la eficiencia y eficacia de una sección o de un organismo con el fin de realizar las mejores prácticas en los aspectos evaluados.

Existen normas y procedimientos específicos para la realización de auditorías en informática como parte de una profesión, estas pueden estar basadas en las experiencias de otras profesiones pero con algunas características propias y siempre guiándose por el concepto de que la auditoría debe ser más amplia que la simple detección de errores, recordemos que la base fundamental al encontrar hallazgos es determinar la causa de la vulnerabilidad, amenaza o riesgo, como también la auditoría debe evaluar para mejorar lo existente, corregir errores y proponer alternativas de solución.

La auditoría no es una actividad meramente mecánica que implique la aplicación de ciertos procedimientos cuyos resultados, una vez llevados a cabo, son de carácter indudable. La auditoría requiere el ejercicio de un juicio profesional, sólido y maduro, para juzgar los procedimientos que deben de seguirse y estimar los resultados obtenidos.

2.2.2 Auditor. Se refiere a la persona capacitada y experimentada que se designa por una autoridad competente o por una empresa de consultoría, para revisar, examinar y evaluar con coherencia los resultados de la gestión administrativa y

[1] Amado Suárez, Adriana et al. (2008). Auditoría de comunicación, editorial La Crujía, Buenos Aires. ISBN 978-987-601-054-2. (Sans de la Tejada, 1998: 63)

financiera de una dependencia o entidad con el propósito de informar o dictaminar acerca de ellas, realizando las observaciones y recomendaciones pertinentes para mejorar su eficacia y eficiencia en su desempeño[2].

A) Clasificación de auditoria según el lugar de origen

Al hablar del concepto de auditoria, se decía que es un proceso de verificación sistemático y documentado con el ánimo de obtener y evaluar de forma objetiva evidencias que permitan determinar si el objeto de la auditoria se ajusta a unos requisitos especificados dependiendo del criterio y finalidad[3], según esto se puede distinguir lo siguientes tipos de auditoría que se basan según quien audita:

B) Auditoría externa

Es el personal independiente contratado para emitir conceptos profesionales sobre el funcionamiento y eficiencia que tiene una organización en el desarrollo de una determinada gestión, este trabajo lo realizan de en forma lucrativa o no.

La ventaja de realizar la auditoría externa es la de estar desligados de todas las funciones que se realicen dentro de la empresa dando un concepto muy veraz, libre de sesgo, es decir, desde un punto de vista totalmente apartado a la comodidad que se ha venido dando dentro de la organización, sin embargo la complicación que se presenta es que se necesita muchos recursos en conocer cómo funciona la empresa

La auditoría externa para cumplir con su objetivo debe seguir los siguientes procedimientos específicos:

- Identificar riesgos (Negocio, Fraude y Procesos).
- Evaluar su susceptibilidad a distorsiones (errores) en la información.
- Diseñar procedimientos de auditoría que permitan evaluar el diseño, la implementación y efectividad de los controles implementados.
- Diseñar procedimientos de auditoría sustantivos de acuerdo con la evaluación de los riesgos

C) Auditoría interna

La necesidad de la auditoría interna se pone de manifiesto en una empresa a medida que ésta aumenta en volumen, extensión geográfica y complejidad y hace imposible el control directo de las operaciones por parte de la dirección, es decir, adecuar las decisiones que se han dado por el crecimiento empresarial.

[2] Enrique Murillo, La Función del Auditor, AOB News, Consultado el 26 de marzo de 2013.
[3] www.cge.es/portalcge/novedades/2009/prl/...auditoria/capitulo3_1.pdf.

La auditoría interna surge por la necesidad de mantener un control permanente y eficaz dentro de la empresa y de hacer más rápida y eficaz la función del auditor externo. Generalmente, se ocupa fundamentalmente del sistema de control interno, es decir, del conjunto de medidas, políticas y procedimientos establecidos en las empresas para proteger sus activos, minimizar las posibilidades de fraude, incrementar la eficiencia operativa y optimizar la calidad de la información económico-financiera.

El objetivo principal es ayudar a la dirección en el cumplimiento de sus funciones y responsabilidades proporcionándoles objetivos, evaluaciones, recomendaciones y todo tipo de comentarios pertinentes sobre las operaciones examinadas. El Instituto de Auditores Internos de los Estados Unidos define la auditoría interna como "una actividad independiente que tiene lugar dentro de la empresa y que está encaminada a la revisión de operaciones contables y de otra naturaleza, con la finalidad de prestar un servicio a la dirección"[4], por lo tanto, es un control de dirección que tiene por objeto la medida y evaluación de la eficacia de otros controles.

2.2.3 Clasificación de auditoría según el área de aplicación. Entre los principales enfoques de Auditoría, se tiene los siguientes:

- **Auditoría financiera (contable):** es un proceso cuyo resultado final es la emisión de un informe, en el que el auditor da a conocer su opinión sobre la situación financiera de la empresa, este proceso solo es posible llevarlo a cabo a través de un elemento llamado evidencia de auditoría, ya que el auditor hace su trabajo posterior a las operaciones de la empresa[5].

- **Auditoría administrativa:** es la revisión analítica total o parcial de una organización con el propósito de precisar su nivel de desempeño y perfilar oportunidades de mejora para innovar valor y lograr una ventaja competitiva sustentable[6], todo esto con el objetivo de impulsar el crecimiento en las organizaciones.

- **Auditoría operacional:** la auditoría operacional se centra en la eficacia, la eficiencia y la economía de las operaciones, se centra en la medición de la posición financiera, de los resultados de las operaciones y de los flujos de efectivos de una entidad. El auditor operacional evalúa los controles

[4] Suárez Suárez Andrés, La Moderna Auditoría, McGraw Hill, 1991, p22.
[5] Gabriel Sánchez Curiel, Auditoría de estados financieros – Practica moderna e integral, Segunda edición, pág. 35.
[6] Enrique Benjamin Franklin, Auditoria Administrativa: Gestión Estratégica del Cambio, Prentice Hall, Segunda edición, 2007, pág. 11.

operativos de la administración y de los sistemas sobre actividades tan diversas como las compras, procesamiento de datos, recepción, envió, servicios de oficina, publicidad, entre otros.

- **Auditoría gubernamental:** es la revisión y examen que llevan a cabo las entidades fiscalizadoras superiores a las operaciones de diferente naturaleza, que realizan las dependencias y entidades del gobierno central, estatal y municipal en el cumplimiento de sus atribuciones legales.

- **Auditoría integral:** es la revisión exhaustiva, sistemática y global que realiza un equipo multidisciplinario de profesionales a todas las actividades y operaciones de una empresa, en un período determinado, dando evidencia relativa a las siguientes temáticas: la Información financiera, la estructura del control interno, el cumplimiento de las leyes pertinentes y la conducción ordenada en el logro de las metas y objetivos propuestos, con el propósito de informar sobre el grado de correspondencia entre la temática y los criterios o indicadores establecidos para su evaluación de todas las áreas de una misma empresa.

- **Auditoría de sistemas:** 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.

2.2.4 Auditoria informática. Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo[7]. El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa.

La auditoría en informática se desarrolla en función de normas, procedimientos y

[7] Carlos Muñoz Razo, Auditoria en sistemas computacionales, Pearson Educación, México, 2002, pág. 23.

técnicas definidas por institutos establecidos a nivel nacional e internacional; por lo tanto, es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

De este modo, la auditoria informática sustenta y confirma la consecución de los objetivos tradicionales de la auditoría:

- Objetivos de protección de activos e integridad de datos.
- Objetivos de gestión que abarcan, no solamente los de protección de activos sino también los de eficacia y eficiencia.

2.2.5 Auditoria de sistemas como objeto de estudio. Se encarga de llevar a cabo la evaluación de normas, controles, técnicas y procedimientos que se tienen establecidos en una empresa para lograr confiabilidad, oportunidad, seguridad y confidencialidad de la información que se procesa a través de los sistemas de información.

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 lograr la utilización más eficiente y segura 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.
- Abuzo 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.

La información es un factor importante y cada día cobra más valor para una empresa u organización para la continuidad de las operaciones, ya que la imagen de su ambiente depende de la situación actual, su desarrollo y competitividad

dependen del ambiente pasado y futuro, ya que tomar una decisión incorrecta mediante datos erróneos proporcionados por los sistemas trae como consecuencia efectos significativos que afectan directamente a la organización.

2.2.6 Objetivo fundamental de la auditoría informática. Lo fundamental en una empresa es que el negocio marche bien, dando los frutos previstos, por ello, es vital que el funcionamiento de todos los elementos de la organización tengan el mejor desempeño, desde las maquinas pequeñas hasta las más grandes, todas relacionadas para servir a los objetivos corporativos. La auditoría se debe realizar en el momento en que la maquinaria informática está en funcionamiento, con el fin de identificar falencias que obstruyan la operatividad de las mismas, con el objeto de corregir o buscar alternativas de solución a tiempo, sin tener que parar el trabajo.

La operatividad de los Sistemas ha de constituir entonces la principal preocupación del auditor informático. Para que el funcionamiento del negocio marche adecuadamente, debe hacer uso de *controles técnicos generales de operatividad y controles técnicos específicos de operatividad*, previos a cualquier actividad.

Los Controles Técnicos Generales, son importantes en las instalaciones de empresas grandes, ya que se realizan para verificar la compatibilidad de funcionamiento simultáneo del sistema operativo y el software de base con todos los subsistemas existentes, como también la compatibilidad del hardware y del software instalado. En una empresa existen diferentes entornos de trabajo que conlleva a la contratación de productos de software básico, así como software especial para algunos departamentos, con el riesgo de abonar más de una vez el mismo producto o desaprovechar el software instalado, así mismo puede existir software desarrollado por personal de sistemas de la misma empresa que hagan mal uso y que no se aprovechen todos los recursos de este, sobre todo cuando los diversos equipos están ubicados en Centros de Proceso de Datos geográficamente alejados. Lo negativo de esta situación es que puede producir la inoperatividad del conjunto. Cada Centro de Proceso de Datos tal vez sea operativo trabajando independientemente, pero no será posible la interconexión e intercomunicación de todos los Centros de Proceso de Datos si no existen productos comunes y compatibles.

Los Controles Técnicos Específicos, menos evidentes, son también necesarios para lograr la operatividad de los sistemas. Es decir por más pequeña que sea la aplicación que se deba ejecutar, esta debe funcionar al máximo, evitando así la inoperatividad, bien sea en hardware como en software. Una vez conseguida la Operatividad de los Sistemas, el segundo objetivo de la auditoría es la verificación de la observación de las normas teóricamente existentes en el departamento de Informática y su coherencia con las del resto de la empresa. Para ello, habrán de

revisarse sucesivamente y en este orden:

- Las Normas Generales de la Instalación Informática. Se realiza una revisión inicial sencilla, verificando la aplicación de las normas pero también registrando las áreas que no cumplan o que no las apliquen, sin olvidar que esta normativa no está en contradicción con alguna norma no informática de la empresa.

- Los Procedimientos Generales Informáticos. Se verificará su existencia, al menos en los sectores más importantes, por ejemplo, la recepción definitiva de las máquinas debería estar firmada por la persona responsable de este cargo. Tampoco el alta de una nueva Aplicación podría producirse si no existieran los Procedimientos de Backup y Recuperación correspondientes.

- Los Procedimientos Específicos Informáticos. Igualmente, se revisará su existencia en las áreas fundamentales. Así, Explotación no debería explotar una Aplicación sin haber exigido a Desarrollo la pertinente documentación. Del mismo modo, deberá comprobarse que los Procedimientos Específicos no se opongan a los Procedimientos Generales. En todos los casos anteriores, a su vez, deberá verificarse que no existe contradicción alguna con la Normativa y los Procedimientos Generales de la propia empresa, a los que la Informática debe estar sometida.

2.3 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 al tipo de auditoría, los hallazgos encontrados y pruebas que avalen estos resultados son indispensables en la realización de una auditoría. Para llegar al resultado hay que seguir una serie de pasos que permiten tener claridad y orden de la auditoría aplicar.

El método de trabajo del auditor pasa por las siguientes etapas:

- Alcance y objetivos de la auditoría informática.
- Estudio inicial del entorno auditable.
- Determinación de los recursos necesarios para realizar la auditoría.
- Elaboración del plan y programa de Trabajo.
- Actividades propiamente dichas de la auditoría.
- Desarrollo del Informe Final.
- Redacción de la carta de introducción o Carta de presentación del informe

final.

2.3.1 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.

2.3.2 Estudio inicial del entorno auditable. Esta etapa es una de las más importantes en el desarrollo de la auditoría, 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 la organización y el entorno operacional.

A) 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.*** El organigrama expresa la estructura oficial de la organización a auditar. Permite identificar las jerarquías, dependencias y direcciones entre las áreas existentes.

- ***Departamentos.*** Se entiende como departamento a los órganos que siguen inmediatamente a la Dirección. El equipo auditor describirá brevemente las funciones de cada uno de ellos.

- ***Relaciones jerárquicas y funcionales entre órganos de la organización.*** El auditor verificará si se cumplen las relaciones funcionales y Jerárquicas previstas por el organigrama, o por el contrario detectará, por ejemplo, si algún empleado tiene dos jefes. Las de Jerarquía implican la correspondiente subordinación. Las funcionales por el contrario, indican relaciones sin subordinación.

- ***Flujos de información*****.** Además de las corrientes verticales entre departamentos, la estructura organizativa cualquiera que sea, produce corrientes de información horizontales y oblicuas extra-departamentales.

- ***Número de puestos de trabajo*****.** El equipo auditor comprobará que los nombres de los Puestos de Trabajo de la organización corresponden a las funciones reales distintas.

- ***Número de personas por puesto de trabajo*.** Es un parámetro que los auditores informáticos deben tener en cuenta ya que la inadecuación del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.

B) Entorno operacional

El auditor informático debe tener una referencia del entorno en el que va a desenvolverse y se obtiene determinando lo siguiente:

- ***Situación geográfica de los sistemas*:** se determinará la ubicación geográfica de los distintos Centros de Proceso de Datos en la empresa, continuando con la verificación de la existencia de responsables en cada uno de ellos, así como el uso de los mismos estándares de trabajo.

- ***Arquitectura y configuración de hardware y software*:** cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas está muy ligada a las políticas de seguridad lógica de las compañías, para esto es importante que los auditores, en su estudio inicial, deben tener en su poder la distribución e interconexión de los equipos.

- ***Inventario de hardware y software*:** el auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a Hardware figurarán las CPU"S, unidades de control local y remoto, periféricos de todo tipo, etc. El inventario de software debe contener todos los productos lógicos del Sistema, desde el software básico hasta los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables.

- ***Comunicación y redes de comunicación*:** al realizar el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones, igualmente, poseerán información de las Redes Locales de la Empresa y todo lo que tenga que ver con la red de Comunicaciones.

2.3.3 Determinación de los recursos necesarios para realizar la auditoría. Mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoría.

Recursos humanos: la cantidad de recursos depende del volumen auditable. Las características y perfiles del personal seleccionado dependen de la materia auditable. Es igualmente señalarle que la auditoría en general suele ser ejercida por profesionales universitarios y por otras personas de probada experiencia multidisciplinaria.

Recursos materiales: los recursos materiales del auditor son de dos tipos:

- ***Recursos software:*** cantidad y complejidad de Bases de datos y ficheros, que son programas propios de la auditoría, son muy potentes y flexibles.

- ***Recursos materiales hardware:*** los recursos hardware que el auditor necesita son proporcionados por el cliente. Los procesos de control deben efectuarse necesariamente en las Computadoras del auditado. Por lo cual habrá de convenir, tiempo de máquina, espacio de disco, impresoras ocupadas, scanner, etc.

2.3.4 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 a 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.

2.3.5 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 al 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 general inicial.

❖ Cuestionario Checklist.

❖ Estándares.

- ❖ Monitores.
- ❖ Simuladores (Generadores de datos).
- ❖ Paquetes de auditoría (Generadores de Programas).
- ❖ Matrices de riesgo.

2.3.6 Desarrollo 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.

2.3.7 Redacción de la 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.

Así como pueden existir tantas copias del informe Final como solicite el cliente, la auditoría no hará copias de la citada carta de Introducción. La carta de introducción poseerá los siguientes atributos:

- Tendrá como máximo 4 folios.
- Incluirá fecha, naturaleza, objetivos y alcance.
- Cuantificará la importancia de las áreas analizadas.
- Proporcionará una conclusión general, concretando las áreas de gran debilidad.
- Presentará las debilidades en orden de importancia y gravedad.
- En la carta de Introducción no se escribirán nunca recomendaciones.

A) 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.

Para cada tema, se seguirá el siguiente orden a saber:

- Situación actual. Cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expondrá la situación prevista y la situación real.

- Tendencias. Se tratarán de hallar parámetros que permitan establecer tendencias futuras.
- Puntos débiles y amenazas.
- Recomendaciones y planes de acción. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática. e) Redacción posterior de la Carta de Introducción o Presentación.

B) Modelo conceptual de la exposición del informe final:

Los parámetros que se deben seguir para la parte conceptual del informe final son:

- 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.

C) Consolidación de hechos

La consolidación de los hechos debe satisfacer, al menos los siguientes criterios:

- El hecho debe poder ser sometido a cambios.
- Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.
- No deben existir alternativas viables que superen al cambio propuesto.
- La recomendación del auditor sobre el hecho, debe mantener o mejorar las normas y estándares existentes en la instalación.

D) Características de los hechos

La aparición de un hecho en un informe de auditoría implica necesariamente la existencia de una debilidad que ha de ser corregida, hay que determinar el flujo del hecho o debilidad, consecuencia del hecho, repercusión del hecho y conclusión del hecho

- **Flujo del hecho o debilidad**: Los hechos encontrados o hallazgos deben ser:

- ❖ Relevantes para el auditor y para el cliente.
- ❖ Exactos, y además convincente.
- ❖ No 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.

E) Recomendación del auditor informático

Las recomendaciones que realiza el auditor informático en el informe final deberán ser:

- Entenderse fácilmente, por simple lectura.
- Soportadas suficientemente en el propio texto.
- Concreta y exacta en el tiempo, para que pueda ser verificada su implementación.
- Redactar las recomendaciones de forma que vaya dirigida expresamente a la persona o personas que puedan implementarla.

2.4 HERRAMIENTAS Y TÉCNICAS PARA LA AUDITORÍA INFORMÁTICA

Con el fin de obtener información suficientemente eficaz para determinar los riesgos, vulnerabilidades y amenazas, se hace uso de herramientas y técnicas que se describen a continuación[8]:

2.4.1 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.
Para esto, suele ser lo habitual comenzar solicitando la cumplimentación de cuestionarios pre-impresos que se envían a las personas concretas que el auditor

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

cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar. Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma. Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría.

Cabe aclarar, que esta primera fase puede omitirse cuando los auditores hayan adquirido por otro medios la información que aquellos pre-impresos hubieran proporcionado.

2.4.2 Entrevistas. El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:

- Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.

- Mediante "entrevistas" en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.

- Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas.

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste 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 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.

2.4.3 Checklist o listas de chequeo. El auditor profesional y experto es aquél que reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior, lo cual no

quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada. Muy por el contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para la cumplimentación sistemática de sus Cuestionarios, de sus listas de chequeo.

Hay opiniones que descalifican el uso de las listas de chequeo, ya que consideran que leerle una pila de preguntas recitadas de memoria o leídas en voz alta descalifica al auditor informático. Por esto no usan listas de chequeo, es una evidente falta de profesionalismo. El profesionalismo pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente.
El conjunto de estas preguntas recibe el nombre de listas de chequeo. Salvo excepciones, las listas de chequeo 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 le 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 listas de chequeo, 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 las listas de chequeo 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 listas de chequeo 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.

Los cuestionarios o listas de chequeo responden fundamentalmente a dos tipos de "filosofía" de calificación o evaluación:

A) Listas de chequeo de rango

Contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo). Ejemplo: se supone que se está realizando una auditoría sobre la seguridad física de una instalación y, dentro de ella, se analiza el control de los accesos de personas y cosas al Centro de Cálculo. Podrían formularse las preguntas que figuran a continuación, en donde las respuestas tienen los siguientes significados:

- Muy deficiente,
- Deficiente,
- Mejorable,
- Aceptable,
- Correcto.

Se figuran posibles respuestas de los auditados. Las preguntas deben sucederse sin que parezcan encasillado, ni clasificadas previamente. El cumplimiento de la lista de chequeo no debe realizarse en presencia del auditado:

- ¿Existe personal específico de vigilancia externa al edificio?

Rta/ No, solamente un guarda por la noche que atiende además otra instalación adyacente.
<Puntuación: 1>

- Para la vigilancia interna del edificio, ¿Hay al menos un vigilante por turno en los aledaños del Centro de Cálculo?

Rta/ Si, pero sube a las otras 4 plantas cuando se le necesita.
<Puntuación: 2>

- ¿Hay salida de emergencia además de la habilitada para la entrada y salida de máquinas?

Rta/ Si, pero existen cajas apiladas en dicha puerta. Algunas veces las quitan.
<Puntuación: 2>

- El personal de Comunicaciones, ¿Puede entrar directamente en la Sala de Computadoras?

Rta/ No, solo tiene tarjeta el Jefe de Comunicaciones. No se la da a su gente más que por causa muy justificada, y avisando casi siempre al Jefe de Explotación.
<Puntuación: 4>

El resultado sería el promedio de las puntuaciones: (1 + 2 + 2 + 4) /4 = 2,25 Deficiente.

B) Lista de chequeo Binaria

Es la constituida por preguntas con respuesta única y excluyente: Si o No. Aritméticamente, equivalen a 1(uno) o 0(cero), respectivamente. Ejemplo:

Se supone que se está realizando una Revisión de los métodos de pruebas de programas en el ámbito de Desarrollo de Proyectos.

- ¿Existe Normativa de que el usuario final compruebe los resultados finales de los programas?

<Puntuación: 1>

- ¿Conoce el personal de Desarrollo la existencia de la anterior normativa?

<Puntuación: 1>

- ¿Se aplica dicha norma en todos los casos?

<Puntuación: 0>

- ¿Existe una norma por la cual las pruebas han de realizarse con juegos de ensayo o copia de Bases de Datos reales?

<Puntuación: 0>

Obsérvese como en este caso están contestadas las siguientes preguntas:

- ¿Se conoce la norma anterior?

<Puntuación: 0>

- ¿Se aplica en todos los casos?

<Puntuación: 0>

Las listas de chequeo de rango son adecuadas si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones. Permiten una mayor precisión en la evaluación que en la lista de chequeo binaria. Sin embargo, la bondad del método depende excesivamente de la formación y competencia del equipo auditor. Las listas de chequeo Binarias siguen una elaboración inicial mucho más ardua y compleja. Deben ser de gran precisión, como corresponde a la suma precisión de la respuesta. Una vez construidas,

tienen la ventaja de exigir menos uniformidad del equipo auditor y el inconveniente genérico del < Si o No> frente a la mayor riqueza del intervalo. No existe lista de chequeo estándar para todas y cada una de las instalaciones informáticas a auditar. Cada una de ellas posee peculiaridades que hacen necesarios los retoques de adaptación correspondientes en las preguntas a realizar.

2.4.4 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.

2.4.5 Observación. La observación es una de las técnicas más utilizadas en la recolección de información para aplicación de una auditoría, 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,
- Observación Externa,
- Observación histórica, entre las cuales están.

❖ Observación controlada.
❖ Observación natural.

2.4.6 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.

2.4.7 Metodologías de auditoria de sistemas. El auditor en cualquier área deberá seguir una metodología en donde utilice diferentes técnicas y herramientas para poder asegurar una correcta recolección y evaluación de evidencia que le permita establecer si se cumple o no con los objetivos organizacionales.

Las metodologías para la auditoría de sistemas o auditoria a la tecnología de información son muy variadas, encontrándose entre ellas la que propone una revisión de objetivos de control propuesta en el COBIT por la ISACA (Information Systems Audit and Control Association). Con esta metodología se permite la verificación y comprobación del sistema de control en tecnologías de la información. Los controles ahí descritos y la guía de auditoría pueden ser

utilizados por los auditores o por los directores como una forma de verificar el cumplimiento de los objetivos. Sin embargo, una metodología completa debe abarcar más pasos para poder asegurar una evaluación completa que incluya revisión de elementos ligados a los objetivos de control y elementos de presentación de documentos con recomendaciones y hechos importantes dirigidos a los interesados en el negocio.

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

"Esta metodología presenta un enfoque amplio y logra un plan de trabajo flexible y reactivo. Sin embargo, tiene la desventaja de depender mucho de la experiencia, habilidad y calidad del profesional involucrado. Dicha anomalía nace de la dificultad que tiene un profesional sin experiencia que asume la función auditora y busca una fórmula fácil que le permita empezar su trabajo rápidamente. Por lo tanto es necesario que el auditor tenga una gran experiencia y una gran formación tanto auditora como informática. Esta formación debe ser adquirida mediante el estudio y la práctica"[9].

"En la auditoría de sistemas existen varias metodologías como: COBIT (ISACA), COSO, SAC, AICPA (SAS), IFAC (NIA), MARGERIT y EDP."[10] . Sin embargo, las metodologías más utilizadas son: COBIT, MARGERIT y COSO.

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

A) COBIT (control objectives for information and related technology)

Las siglas COBIT significan Objetivos de Control para Tecnología de Información y Tecnologías relacionadas (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), se formó como una fundación de educación para llevar a cabo los esfuerzos de investigación a gran escala para expandir el conocimiento y el valor de la gobernanza de las Tecnologías de Información (TI)[11].

La adecuada implementación de un modelo COBIT en una organización, provee

[9] PIATTINI, Mario y Emilio del Peso, Auditoría Informática: Un enfoque práctico, Editorial RA-MA.
[10] Jenny Burgos y Carolina Domínguez, Tesis, Auditoria al módulo de historia clínica, Año 2007, Pág. 59-60 y 87-94.
[11] www.megapuntes.com.ar/auditoria/ALUMNOS2008/ISACA.doc

una herramienta automatizada, para evaluar de manera ágil y consistente el cumplimiento de los objetivos de control y controles detallados, 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.

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.

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:

- Planificación y organización.
- Adquisición e implantación.
- Soporte y servicios.
- Monitoreo.

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

"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"[12].

Dominio: planificación y organización (PO)

Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos de negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas. Los procesos de este dominio son:

- PO1 Definir un Plan Estratégico de TI
- PO2 Definición de la arquitectura de información

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

- PO3 Determinación de la dirección tecnológica
- PO4 Definición de la organización y de las relaciones de TI
- PO5 Manejo de la inversión
- PO6 Comunicación de la dirección y aspiraciones de la gerencia
- PO7 Administración de recursos humanos
- PO8 Asegurar el cumplimiento con los requerimientos externos
- PO9 Evaluación de riesgos
- PO10 Administración de proyectos
- PO11 Administración de calidad

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, sus procesos son:

- AI1 Identificación de soluciones automatizadas
- AI2 Adquisición y mantenimiento del software aplicativo
- AI3 Adquisición y mantenimiento de la infraestructura tecnológica
- AI4 Desarrollo y mantenimiento de procedimientos
- AI5 Instalación y aceptación de los sistemas
- AI6 Administración de los cambios

Dominio: entrega 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. Los principales procesos, son:

- DS1 Definición de niveles de servicio
- DS2 Administración de servicios prestados por terceros
- DS3 Administración de desempeño y capacidad
- DS4 Asegurar el servicio continúo
- DS5 Garantizar la seguridad de sistemas
- DS6 Educación y entrenamiento de usuarios
- DS7 Identificación y asignación de costos
- DS8 Apoyo y asistencia a los clientes de TI
- DS9 Administración de la configuración
- DS10 Administración de problemas

- DS11 Administración de datos
- DS12 Administración de las instalaciones
- DS13 Administración de la operación

Dominio: monitoreo 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. Los procesos de este dominio son:

- M1 Monitoreo del proceso
- M2 Evaluar lo adecuado del control interno
- M3 Obtención de aseguramiento independiente
- M4 Proveer auditoría independiente

Los 34 procesos propuestos se concretan en 32 objetivos de control detallados anteriormente.

Un Control se define como "las normas, estándares, procedimientos, usos y costumbres y las estructuras organizativas, diseñadas para proporcionar garantía razonable de que los objetivos empresariales se alcanzaran y que los eventos no deseados se preverán o se detectaran, y corregirán".

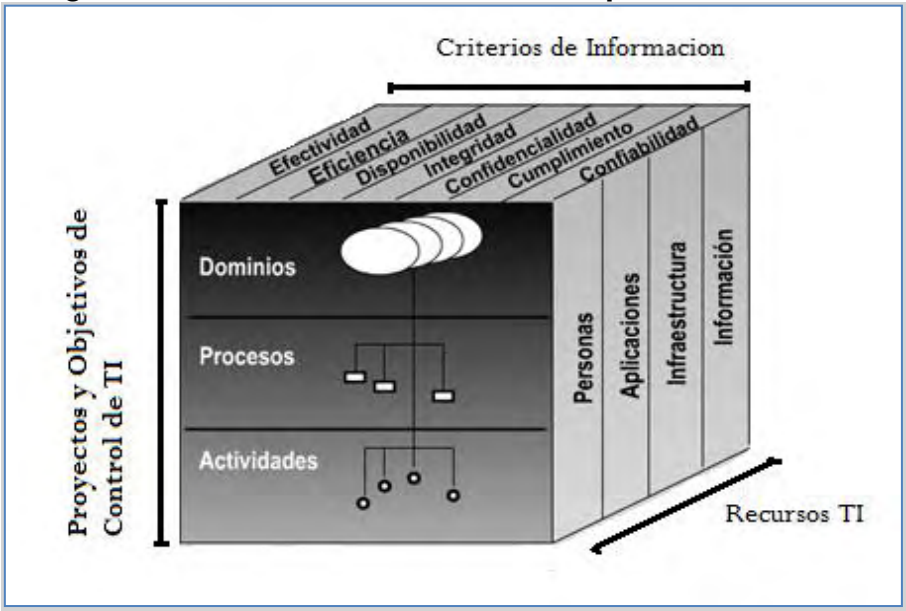
Un Objetivo de Control, se define como "la declaración del resultado deseado o propuesto que se ha de alcanzar mediante la aplicación de procedimientos de control en cualquier actividad de TI".

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

- Los recursos de las TI.
- Los criterios empresariales que deben satisfacer la información.
- Los procesos de TI.

Estos dominios facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. Como se muestra en la siguiente figura. (Ver figura 1)

Figura 1. Las tres dimensiones conceptuales de COBIT



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

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

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

Ventajas que ofrece COBIT

COBIT es un marco de referencia aceptado mundialmente de gobierno IT basado en estándares y mejores prácticas de la industria. Una vez implementado, es posible asegurarse de que IT se encuentra efectivamente alineado con las metas del negocio, y orientar su uso para obtener ventajas competitivas.

Suministra un lenguaje común que les permite a los ejecutivos de negocios comunicar sus metas, objetivos y resultados con Auditores, IT y otros profesionales.

Proporciona las mejores prácticas y herramientas para monitorear y gestionar las actividades de IT. El uso de sistemas usualmente requiere de una inversión que

necesita ser adecuadamente gestionada.

Ayuda a los ejecutivos a entender y gestionar las inversiones en IT a través de sus ciclo de vida, así como también proporcionándoles métodos para asegurarse que IT entregara los beneficios esperados.

“Al ser COBIT reconocida y aceptada internacionalmente como una herramienta de gestión, su implementación es un indicativo de la seriedad de una organización. Ayuda a Empresas y profesionales de IT a demostrar su competitividad ante las demás compañías. Así como existen procesos genéricos de muchos tipos de negocios, existen estándares y buenas prácticas específicos para IT que deben seguirse por las compañías cuando se soportan en IT, en donde COBIT agrupa tales estándares y entrega un marco de referencia para su implementación y gestión”[13]

[13] Marco de referencia COBIT versión 4.1

3. DESARROLLO DE LA AUDITORÍA

3.1 METODOLOGÍA

La metodología que se utilizó para la realización de la auditoria informática a los procesos y organización de la empresa nariñense AGROPEZ LTDA fue de tipo cuantitativo subjetivo, basado en un modelo matemático numérico, dando como resultado un listado de hallazgos, obtenidos de la aplicación de cada proceso auditado, resaltando el impacto e importancia dentro del área de sistemas, desde ese punto se dará la calificación y recomendaciones correspondientes.

La responsabilidad de la información suministrada por la empresa AGROPEZ LTDA, está a cargo del grupo de auditores conformado por FERNANDO JAVIER PEPINOSA ORTEGA Y JOSE ANDRES SALAZAR ARAUJO, estudiantes de la Universidad de Nariño, con la cual, se hizo los diferentes análisis para desarrollar la presente auditoria.

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

3.2 ETAPAS DE LA METODOLOGÍA UTILIZADA

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

3.2.1 Etapa 1: familiarización con el entorno. Este primer paso se realizó con el fin de familiarizarse con la infraestructura tecnológica de la empresa AGROPEZ LTDA, se hace un estudio previo de la empresa como su plataforma estratégica, sus fines y diferentes aspectos que sirvieron para la auditoria en especial la parte de los procesos a auditar obteniendo así las herramientas necesarias para una adecuada planeación de la auditoría, también se definieron en esta etapa, los elementos utilizados para elaborar la auditoría.

Se realizaron visitas a las instalaciones de AGROPEZ LTDA, con el fin de conocer y observar los diferentes procesos, identificando y familiarizando con ellos, se dio

inicio a la recolección de información, ayudando a la creación de cuestionarios cuantificables que luego se realizó a los diferentes funcionarios de los departamentos implicados con el área de sistemas.

Al final de la etapa de reconocimiento, se generó un archivo permanente el cual contiene información constante o variable en el tiempo de la empresa y sirvió para dar una visión real hacia donde se debe encaminar la auditoria, para pasar a la siguiente etapa.

3.2.2 Etapa 2: planeación de las actividades de auditoría. Aquí se realizó la planificación de todo el proceso de la auditoría, con las siguientes actividades:

- Realizar estudio previo a la infraestructura tecnológica de AGROPEZ LTDA, obteniendo información necesaria respecto al tema.

- Establecer objetivos y alcances de la auditoría.

- Elaborar planes, programas y presupuestos para realizar la auditoría.

- Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría.

3.2.3 Etapa 3: ejecución de la auditoría. En esta etapa se procedió a ejecutar los planteamientos realizados en la etapa anterior, con la aplicación de las metodologías y técnicas seleccionadas que garantizan el cumplimiento de los objetivos planeados. Las actividades realizadas dentro de esta etapa, fueron:

- Ejecución de la auditoría informática con las herramientas y metodología escogida y preparada en la fase anterior.

- Asignación de la probabilidad de ocurrencia e impacto para los riesgos detectados mediante la aplicación de formatos de hallazgos.

3.2.4 Etapa 4: presentación del informe final. En esta etapa se realizó el informe ejecutivo y el informe general de auditoria, después de analizar y encontrar los riesgos, vulnerabilidades y amenazas de todos los procesos evaluados con la descripción del comportamiento que estos tienen dentro de la empresa o los hallazgos encontrados con sus respectivas recomendaciones que permitan mitigarlos al máximo.

El informe ejecutivo y el informe general de auditoria se presentaron y entregaron al gerente de la empresa AGROPEZ LTDA, para que tomen las decisiones para implementar un plan de mejoramiento y así mejorar la funcionalidad de la entidad.

4. DESARROLLO DEL TRABAJO

4.1 ARCHIVO PERMANENTE

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

4.1.1 Plataforma estratégica AGROPEZ LTDA

A) Misión

AGROPEZ LTDA es una empresa de importaciones, exportaciones y distribuidora de fruta, marisco y pescado a toda la población de la región del suroccidente de Colombia y norte del ecuador enfocado en ofrecer una excelente y homogénea calidad de los productos que comercializa, generando condiciones que resalten la comercialización de productos de mar, a través de procesos transparentes, eficientes y oportunos, protegiendo y garantizando de manera efectiva la mercancía

B) Visión

En el 2017 AGROPEZ LTDA será una empresa altamente competitiva, responsable y reconocida como líder en la importación y exportación de productos del mar logrando generar condiciones que protejan la mercancía de nuestros clientes, basados en la cultura del mejoramiento permanente de nuestros procesos y en el desarrollo eficiente del talento humano y tecnológico

C) Objeto social

La sociedad tendrá como objeto principal[14]:

- Comercialización y la importación de productos agrícolas y pesqueros
- El comercio en general al por Mayor y Detal.
- Compra y venta de mercancías sean nacionales o extranjeras, importación y exportación de materias primas y equipo.

[14] Certificación de la Cámara de Comercio CCP-0313451

Todas las actividades mercantiles, civiles, financieras y accesorias o complementarias que se relacionen directamente con el objeto social, así mismo. Podrá realizar cualquier otra actividad económica lícita tanto en Colombia como en el extranjero. La sociedad podrá llevar a cabo, en general todas las operaciones de cualquier naturaleza que ellas fueren relacionadas con el objeto mencionado, así como cualquier actividad similar, conexa o complementaria o que permitan facilitar o desarrollar el comercio o la industria de la sociedad.

D) Política de calidad

Garantizar la prestación de los servicios de importaciones y exportaciones de productos del mar, brindando a sus clientes:

- Facilidad de acceso a los servicios.
- Red idónea y suficiente que permita la prestación oportuna y segura de los servicios de importaciones y exportaciones de productos del mar.
- Permanente desarrollo del talento humano.
- Manejo adecuado de los recursos.

Están convencidos que el mejoramiento continuo de los procesos permitirá lograr la satisfacción de nuestros clientes.

e) Valores institucionales

- Competitividad: en el aseguramiento de las diferentes mercancías que comercializamos
- Compromiso y sentido de pertenencia con la empresa para el cumplimiento de la misión y el alcance de la visión
- Calidad Humana en el desarrollo de las actividades institucionales e individuales.
- Idoneidad para el desarrollo de las actividades, funciones, y procesos referentes a comercio exterior.
- Vocación de servicio: Aptitud de servir con amabilidad, sencillez, humildad y confianza.

F) Metas empresariales

- Ofrecer una excelente y homogénea calidad de productos que comercializa además encargarse de los planes y logística de sus mercancía,

- Consolidarse en el mercado nacional como un referente importador de la región.

- Dar al cliente la mejor atención e información con respecto a la mercancía.

4.2 ARCHIVO CORRIENTE

Para llevar a cabo el proceso de auditoría se hizo la recopilación de documentos que tendrán que ver directamente con este desarrollo.

4.2.1 Memorando de planeación de auditoria

A) Antecedentes de auditorías dentro de AGROPEZ LTDA

Después de 15 años en el mercado, AGROPEZ LTDA no ha realizado ningún trabajo de auditoría, por lo que es importante resaltar que la auditoria es una herramienta para controlar el alineamiento de la organización con la estrategia propuesta por la administración y asegurar un adecuado funcionamiento de las diferentes áreas del negocio.

La mayoría de empresas pequeñas no tienen la obligación de hacer auditorías, es por ello, que las empresas no tienen una cultura para prevenir, evaluar y controlar riesgos, sin embargo, hay que recordad que la auditoría ayudar a la organización a optimizar los recursos utilizados, mejorando sus operaciones.

B) Objetivos

Objetivo general. Evaluar la estructura organizacional del área de informática de la empresa AGROPEZ LTDA de la ciudad de Ipiales, los procesos informáticos y manejo de la información.

Objetivos específicos:

- Conocer el área de informática y los procesos internos de la empresa AGROPEZ LTDA de la ciudad de Ipiales.
- Realizar un análisis de riesgos para identificar y conocer la causa de los mismos para proponer alternativas de solución.
- Aplicar el proceso de auditoría a los riesgos más relevantes que afecten el funcionamiento del sistema, utilizando las técnicas apropiadas para realizar las pruebas que permitan evidenciar.
- Aplicar los instrumentos diseñados, realizar pruebas y ejecutar el proceso de análisis y evaluación de riesgos para su valoración.
- Elaborar y entregar el informe final que contenga los riesgos confirmados y controles propuestos.

4.2.2 Alcance y delimitación. De la estructura organizacional de AGROPEZ LTDA de la ciudad de Ipiales se evaluó lo siguiente:

- **De los procesos del área de informática se evaluara y revisara:**

❖ Existencia de procesos documentados.

❖ Cumplimiento de los procesos documentados.

❖ Definición de personal y responsabilidades a cargo.

- **De los procesos informáticos y de información:**

❖ Existencia de sistemas de control.

❖ Existencia de políticas organizacionales relacionadas con el manejo de información.

4.2.3 Metodología. Para realizar la auditoría informática de la empresa AGROPEZ LTDA de la ciudad de Ipiales, se realizaron as siguientes etapas, así:

A) Etapa 1: familiarización con el entorno

En esta fase se realizó la recolección, clasificación y análisis de información sobre técnicas de auditoría de sistemas.

Se realizó una visita el día 13 de enero de 2016, con el objetivo de recolectar información de la empresa en los siguientes puntos:

- Plataforma estratégica,
- Dependencias o forma de organización de trabajo,
- Número de empleados y funciones a realizar,
- Hardware y software que utilizan,
- Seguridad física,
- Funcionamiento del negocio,
- Contratos con otras empresas,
- Técnicas de respaldo de información que utilizan.
- Políticas de adquisición tecnológica.

Esta visita ayudo a recolectar la información y a familiarizarse con el entorno, se solicitó documentos escritos y el grupo de auditores hizo la observación directa del manejo de la empresa.

B) Etapa 2: planeación de las actividades de auditoría

En la fase de planeación se realizaron las siguientes actividades:

- Realizar el estudio inicial de la empresa como caso de estudio,
- Crear el plan de auditoria con la información recolectada,
- Determinar recursos disponibles para el desarrollar de la auditoria,
- Crear el programa de auditoria, identificando estándar, seleccionando los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría.

C) Etapa 3: ejecución de la auditoría

En esta etapa se ejecutó la auditoria, se realizaron las siguientes actividades:

- Aplicar instrumentos y pruebas.
- Análisis y evaluación de riesgo.

D) Etapa 4: presentación del informe final

En esta etapa, con la información obtenida se procedió a:

- Analizar hallazgos obtenidos, determinando causas de ellos y proporcionando planes para mitigarlos.
- Elaboración de informe con los Hallazgos encontrados, detectando las causas y su efecto.
- Creación de informe ejecutivo.
- Creación de informe general de auditoria.

4.2.4 Recursos:

A) Recursos humanos

Para el desarrollo de este trabajo se contó con los estudiantes egresados de ingeniería de sistemas: FERNANDO JAVIER PEPINOSA ORTEGA, JOSE ANDRES SALAZAR ARAUJO con la asesoría del Ingeniero MANUEL BOLAÑOS GONZALEZ y colaboración del ingeniero LUIS SALAZAR, Ingeniero del área de sistemas de la empresa AGROPEZ LTDA.

A) Recursos tecnológicos

Computador portátil para la realización de informes con las siguientes características:

Procesador Intel Core i5
Memoria RAM de 4 Gb
Disco duro de 500 Gb
Un quemador de DVD de 16X
Sistema Operativo Windows Seven, Office 2013

Cámara digital utilizada para la captura de entrevistas y material fotográfico

B) Recursos materiales

El trabajo se llevó a cabo utilizando los recursos disponibles en la entidad. (Ver tabla 1)

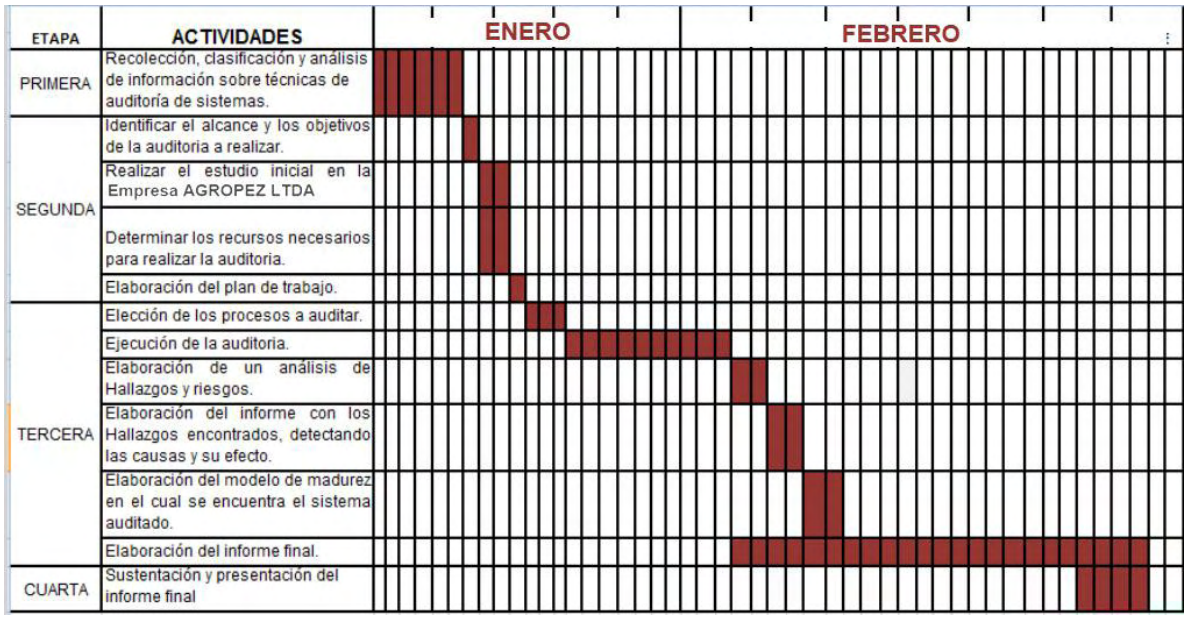
C) Recursos financieros

Tabla 1. Recursos financieros de la investigación

CANTIDAD	DETALLE	VALOR UNITARIO	VALOR TOTAL
3	Resma de papel tamaño carta	10.000	30.000
70	Horas de internet	1.000	70.000
320	Fotocopias de material de consulta	50	16.000
	Otros gastos	100.000	100.000
		Total	216.000

Nota: Estos gastos están a cargo de los estudiantes quienes realizarán el proyecto

D) Cronograma



4.3 PROGRAMA DE AUDITORÍA

4.3.1 Determinar estándar aplicable de la auditoria. Esta auditoría se ejecutó mediante la aplicación de la metodología COBIT 4.1 (objetivos de control para la información y tecnologías afines), donde se evaluaron algunos objetivos de control que se encuentran dentro de los cuatro dominios para evidenciar los riesgos, amenazas y vulnerabilidades en los procesos y organización del área de sistemas de la empresa AGROPEZ LTDA de la ciudad de Ipiales.

4.3.2 Seleccionar dominios, procesos y objetivos de control. Es importante acoplar la definición de un estándar con la situación de estudio, aquí se empezó a determinar del estándar COBIT 4.1, los dominios, procesos y objetivos de control que estuvieron directamente relacionados con el objetivo general y alcances de la auditoria, es bueno aclarar que los procesos escogidos estaban directamente ligados con las metas de tecnología de información del negocio a auditar.

A) Dominio 1: planeación y organización (PO)

Este dominio cubre la contribución de la tecnología de información a los objetivos del negocio en cuanto a las estrategias y tácticas utilizadas, Además, evaluar la visión estratégica de la empresa en los aspectos de planeación, comunicación y administración. Finalmente, se verificó si la infraestructura tecnológica es la

apropiada, procesos:

PO3 Determinación de dirección tecnológica

Aprovechar al máximo la tecnología disponible y las emergentes, satisfaciendo los requerimientos de negocio, a través de la creación y mantenimiento de un plan de infraestructura tecnológica. Toma en consideración:

PO3.1 Planeación de la dirección tecnológica

Comprobar la existencia y dirección de la tecnología es la adecuada para el negocio.

PO3.2 Plan de infraestructura tecnológica

Verificar que haya un plan de infraestructura tecnológica, evaluar planes de contingencia, evaluar procesos para la adquisición y la evolución de recursos tecnológicos.

PO3.3 Monitoreo de tendencias y regulaciones futuras

Evaluar la presencia de procesos para monitorear las directrices del funcionamiento de la infraestructura tecnológica.

PO3.4 Estándares tecnológicos

Verificar el desarrollo de prácticas de asesoría sobre el funcionamiento o selección de la infraestructura, verificar si existen guías para la selección de la tecnología, medir el cumplimiento de estándares y directrices.

PO9 Evaluar y Administrar los riesgos de TI

Responder a las amenazas hacia la provisión de servicios de TI y asegurar el logro de los objetivos de TI. Se requiere la identificación de riesgos de TI y análisis de impacto, considerando las medidas de seguridad requeridas para mitigar los riesgos. Toma en consideración:

PO9.3 Identificación de eventos

Identificación de los riesgos asociados a TI con la finalidad de que los mismos puedan ser administrados, registrar eventos de riesgo (una amenaza importante y realista que explota una vulnerabilidad aplicable y significativa) con un impacto potencial negativo sobre las metas o las operaciones de la empresa, se evaluara la existencia de una bitácora de errores en donde se registra los riesgos relevantes y su incidencia.

PO9.4 Evaluación de riesgos de TI

Definición de alcances, límites de los riesgos y la metodología para las evaluaciones de los riesgos usando métodos cualitativos y cuantitativos.

PO9.5 Respuesta a los riesgos

Verificar la existencia de un proceso de respuesta a riesgos diseñado para asegurar que controles efectivos en costo mitigan la exposición en forma continua. El proceso de respuesta a riesgos debe identificar estrategias tales como evitar, reducir o aceptar riesgos, determinar responsabilidades y considerar los niveles de tolerancia a riesgos.

B) Dominio 2: adquisición e implementación (AI)

Este dominio está diseñado para llevar a cabo la estrategia TI, identificando, desarrollando o adquiriendo solucione tecnológicas, así como implementar e integrar con los procesos empresariales, esto para garantizar que las soluciones satisfaga los objetivos del negocio. De este dominio se aplicaran las siguientes actividades:

AI3 Adquisición y mantenimiento de la infraestructura tecnológica

Proporcionar las plataformas apropiadas para soportar aplicaciones de negocios mediante la realización de una evaluación de desempeño de hardware y software, como también, el respectivo mantenimiento.

.

AI3.1 Plan de adquisición de infraestructura tecnológica

Evaluación de tecnología disponible para identificar el impacto de nuevo hardware o software sobre el rendimiento del sistema general.

AI3.3 Mantenimiento de la infraestructura:

Mantenimiento preventivo del hardware con el objeto de reducir la frecuencia y el impacto de fallas de rendimiento.

AI3.4 Ambiente de prueba de factibilidad

Evaluar la efectividad y eficacia de la infraestructura, sobre todo en los procesos de adquisición, funcionalidad, configuración de hardware, pruebas de desempeño, estructura de Red.

AI4 Facilitar la operación y el uso

Asegurar el uso apropiado de las aplicaciones tecnológicas de la entidad, lográndolo con la realización de documentación como manuales de procedimientos y manuales de funciones para usuarios enfocados a proporcionar un correcto entrenamiento y uso eficiente de las aplicaciones.

AI4.3 Transferencia de conocimiento a usuarios finales

Verificar la existencia de un plan de entrenamiento que aborden capacitación inicial y continua, así como el desarrollo de habilidades, materiales de entrenamiento, manual de usuario, manual de procedimientos, asistencia a usuarios y evaluación permitiendo que los usuarios finales utilicen con efectividad y eficiencia la aplicación.

AI4.4 Transferencia de conocimiento al personal de operaciones y soporte

Evaluar la existencia de transferencia de conocimiento que permite que el personal de operaciones y soporte entreguen, apoyen y mantengan la aplicación y la infraestructura funcionando de manera efectiva y eficiente. La transferencia de conocimiento incluye el desarrollo de planes de entrenamiento que aborden capacitación inicial y continua, así como el desarrollo de habilidades, materiales de entrenamiento, manual de usuario, manual de procedimientos, material de uso del sistema en la práctica diaria.

C) Dominio 3: Entrega y soporte (DS)

En este dominio se hace referencia a la entrega de los servicios TI requeridos. Abarca desde las operaciones de procesamiento de datos tradicionales hasta el entrenamiento de usuarios; incluye también la seguridad informática y el aseguramiento de continuidad del servicio. Este dominio incluye el procesamiento de transacciones atendido por los sistemas de aplicación, los procesos a evaluar en este dominio son:

DS2 Administrar los servicios de terceros

El objetivo es asegurar que las tareas y responsabilidades de los proveedores de servicios informáticos estén claramente definidas y que cumplan 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 cumplimiento de las políticas de la organización. Toma en consideración:

DS2.1 Identificación de todas las relaciones con proveedores

Acuerdos de servicios con terceras partes a través de contratos entre la organización y el proveedor evaluando niveles de procesamiento requeridos, seguridad, monitoreo y requerimientos de contingencia, así como en otras estipulaciones según sea apropiado.

DS2.2 Gestión de relaciones con proveedores

Acuerdos de confidencialidad.

DS2.3 Administración de riesgos del proveedor

Requerimientos legales regulatorios de manera de asegurar que estos concuerde con los acuerdos de seguridad establecidos.

DS2.4 Monitoreo del desempeño del proveedor

Monitoreo de la entrega de servicio con el fin de asegurar el cumplimiento del contrato.

DS4 Garantizar la continuidad del servicio

El objetivo es garantizar la continuidad de los servicios, para esto se hace necesario desarrollar, mantener y aprobar planes de continuidad de TI. Almacenando respaldos para minimizar la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio.

DS4.2 Planes de continuidad de TI

Revisar la existencia de planes de continuidad, diseñados para reducir el impacto de una interrupción mayor de las funciones y los procesos clave de la entidad. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de los servicios TI.

DS4.6 Entrenamiento del plan de continuidad de TI

Verificar si todas las partes involucradas reciben sesiones de entrenamiento de forma regular respecto a los procesos, sus roles y responsabilidades en caso de incidente o desastre. Evaluar si se hacen pruebas de contingencia y de acuerdo a los resultados si se verifica o incrementa el entrenamiento.

DS4.8 Recuperación y reanudación de los servicios

En el momento en que los servicios TI se estén recuperando y reanudando sus servicios se deben activar los sitios de respaldo, el inicio del procedimiento alternativo, realizar procedimientos de reanudación entre otras actividades.

DS4.9 Almacenamiento de respaldos fuera de las instalaciones

Verificar si se almacena fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad de la dependencia. El contenido de los respaldos a almacenar debe determinarse en conjunto entre los responsables de los procesos de la dependencia y el personal de TI. La administración del sitio de almacenamiento externo a las instalaciones, debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de la entidad prestadora servicios de salud. Las directivas de TI debe asegurar que los acuerdos con sitios externos sean evaluados periódicamente, al menos una vez por año, respecto al contenido, a la protección ambiental y a la seguridad.

DS4.10 Revisión post reanudación

Una vez lograda una exitosa reanudación de las funciones de TI después de una suspensión en sus servicios, determinar si las directivas de TI han establecido procedimientos para valorar lo adecuado del plan y actualizar el plan en consecuencia.

DS9 Administrar la configuración

Disponer de un inventario de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el manejo de cambios, monitorear 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.

DS9.1 Repositorio y línea base de configuración

Poseer Inventario de activos TI, establecer procedimientos para asegurar que éstos sean registrados al momento de adquisición e instalación.

DS9.2 Identificación y mantenimiento de elementos de configuración

Administración de cambios en la configuración asegurando que los registros de configuración reflejen la situación real de todos los elementos de la configuración, integrar esto con la gestión de cambios, gestión de incidentes y procedimientos de gestión de problemas.

DS9.3 Revisión de Integridad de la configuración

Utilizar procedimientos de chequeo de software instalado, detectando productos no autorizados.

4.3.3 Diseño de instrumentos para realizar la auditoria. Para el desarrollo de la auditoría informática en la empresa AGROPEZ LTDA de la ciudad de Ipiales se diseñaron los siguientes formatos de recolección de información para utilizarlos en la etapa de ejecución:

A) Cuadro de definición de fuentes de conocimiento

Pruebas de análisis, y pruebas de auditoría: este cuadro es un instrumento que sirvió 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 formatos de cuadros de definición de fuentes de conocimiento contienen lo siguiente:

- ***REF:*** Identificación del cuadro de definición de fuentes de conocimiento.
- ***ENTIDAD AUDITADA:*** nombre de la entidad a la cual se le está realizando el proceso de auditoría.
- ***ÁREA AUDITADA:*** nombre del área a la cual se aplicara la auditoria.
- ***OBJETO DE ESTUDIO:*** nombre del objeto de estudio de la auditoria.
- ***DESCRIPCIÓN DE ACTIVIDAD/PRUEBA*****:** breve referencia al objetivo del proceso seleccionado dentro de los dominios del COBIT que se está revisando.
- ***MATERIAL DE SOPORTE:*** nombre del material que soporta el proceso de la auditoria, para el este proyecto, siempre será COBIT.
- ***DOMINIO:*** nombre del dominio de COBIT que se está evaluando.
- ***PROCESO:*** nombre del proceso específico que se está auditando dentro de los dominios del COBIT.
- ***FUENTES DE CONOCIMIENTO:*** listado de herramientas necesarias para obtener la información, puede ser a través de entrevistas, manuales, política,

archivos físicos o magnéticos, reportes, contratos, etc.

- ***REPOSITORIO DE PRUEBAS APLICABLES:*** se divide en dos tipos de pruebas:

❖ ***DE ANÁLISIS*****:** describir pruebas de análisis que se realizan para evaluar el proceso específico que se encuentre en estudio.

❖ ***DE EJECUCIÓN*****:** describir pruebas de ejecución que se realizan para evaluar el proceso específico que se encuentre en estudio, son las acciones a realizar para la ejecución de la auditoria, como revisión, verificación, pruebas, obtención de inconsistencia, etc.

- ***AUDITORES RESPONSABLES:*** nombre del auditor o auditores.

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 de esta investigación, entregados en medio digital (Ver anexo No. 1). (Ver figura 2)

Figura 2. Cuadro de definición de fuentes de conocimiento

	CUADRO DE DEFINICION DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANALISIS Y PRUEBAS DE AUDITORIA	REF	PLAN PO3		
		Pág.	1	de	1

ENTIDAD AUDITADA	AGROPEZ LTDA		
AREA AUDITADA	AREA DE SISTEMAS	OBJETO ESTUDIO	PROCESOS Y ORGANIZACION TI
DESCRIPCIÓN DE ACTIVIDAD/PRUEBA	Aprovechar al máximo la tecnología disponible y las emergentes, satisfaciendo los requerimientos de negocio, a través de la creación y mantenimiento de un plan de infraestructura tecnológica		

MATERIAL DE SOPORTE	COBIT		
DOMINIO	Planeación y organización	PROCESO	PO3 Determinación de dirección tecnológica

FUENTE DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANALISIS	DE EJECUCION
• Entrevista al jefe de área de informática. • Entrevista a gerente. • Política de adquisición de IT. • Facturas de compra. • Inventario de IT. • Cuestionario a funcionario responsable de adquisición.	Analizar políticas y procedimientos de infraestructura con respecto a los requerimientos del negocio, monitoreo de desarrollo tecnológico emergente, planes de adquisición.	Revisión de las políticas de adquisición de IT, procesos de monitoreo de desarrollo tecnológico, revisión de planes de adquisición de IT.

AUDITORES RESPONSABLES	ANDRES SALAZAR – FERNANDO PEPINOSA

B) Cuestionario cuantitativo

El cuestionario cuantitativo permite dar una calificación numérica a un requerimiento dentro de los procesos que se estén auditando para determinar su vulnerabilidad.

Este cuestionario cuantitativo está conformado por los siguientes puntos:

- ***REF:*** Identificación del cuadro de definición.

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

- ***ÁREA AUDITADA:*** nombre del área a la cual se aplicara la auditoría.

- ***OBJETO DE ESTUDIO:*** nombre del objeto de estudio de la auditoria.

- ***MATERIAL DE SOPORTE:*** nombre del material que soporta el proceso, para el caso será COBIT.

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

- ***PROCESO:*** nombre del proceso que se está auditando dentro de los dominios del COBIT.

- ***PREGUNTA:*** planteamiento de la descripción de la información requerida a evaluar.

- ***SI-NO-N/A:*** 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.

- ***FUENTE:*** fuente de donde se obtiene la información requerida

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

- ***TOTAL CUESTIONARIO:*** sumatoria de los SI + NO + NA.

- ***PORCENTAJE DE RIESGO:*** probabilidad de que el proceso se vea afectado por las acciones de las cuales se está indagando, entre mas alto el porcentaje mayor probabilidad de riesgo tiene el proceso de salir perjudicado.

A continuación se muestra el cuestionario cuantitativo, en este caso es para el proceso PO3. Evaluar lo adecuado del control interno, que se ubica dentro del dominio de Monitoreo de COBIT. Ver figura 3.

Figura 3. Cuestionario cuantitativo

	CUESTIONARIO CUANTITATIVO	REF	PLAN PO3		
		Pág.	1	de	1

ENTIDAD AUDITADA	AGROPEZ LTDA		
AREA AUDITADA	ÁREA DE SISTEMAS	OBJETO ESTUDIO	PROCESOS Y ORGANIZACIÓN TI

MATERIAL DE SOPORTE	COBIT		
DOMINIO	Planeación y organización	PROCESO	PO3 Determinación de dirección tecnológica

PREGUNTA	SI	NO	N/A	FUENTE
1. ¿Existen políticas y procedimientos referentes a la adquisición de infraestructura tecnológica?		5		
2. Estas políticas contemplan: a. Descripción detallada de los procedimientos de adquisición de infraestructura tecnológica.		5		
b. Se realiza monitoreo de nuevas tecnologías para implementarlas en la empresa.		3		
c. ¿Quién debe ejecutar el monitoreo?		4		
3. ¿Estas políticas y procedimientos están documentados?		5		
4. ¿El plan de adquisición de infraestructura tecnológica es adecuado con los objetivos de la empresa		5		
5. Se verifican o monitorean los desarrollos tecnológicos actuales mirando que tan óptimos son para el negocio.		5		
TOTALES	0	32	0	
TOTAL CUESTIONARIO		32		

PORCENTAJE DE RIESGO: $\frac{0*100}{32-0}$ = 100- 0 = 100%

AUDITORES RESPONSABLES	ANDRES SALAZAR – FERNANDO PEPINOSA

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, se aplicó la siguiente fórmula matemática

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

$$Porcentaje\ de\ Riesgo 1 = \frac{\text{Total de SI} * 100}{\text{Total de Cuestionario} - (\text{N/A})}$$

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

$$Porcentaje\ de\ Riesgo\ Total = 100 - \text{Porcentaje de Riesgo1}$$

  Después de haber calculado este porcentaje, se procedió 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 para los objetivos de la institución, 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.

- ***AUDITORES RESPONSABLES:*** nombre del auditor o auditores.

Todos los cuestionarios cuantitativos utilizados en el proceso de auditoría se encuentran en los anexos entregados en medio digital (Ver anexo No. 2).

Entrevistas preguntas abiertas y preguntas cerradas

Las entrevistas que se hicieron a la empresa AGROPEZ LTDA fueron realizadas por el equipo auditor, la visita se hizo sin previo aviso, por lo tanto, los entrevistados no tuvieron tiempo previo para preparar las respuestas, contestándolas de inmediato.

Se realizó dos tipos de entrevistas:

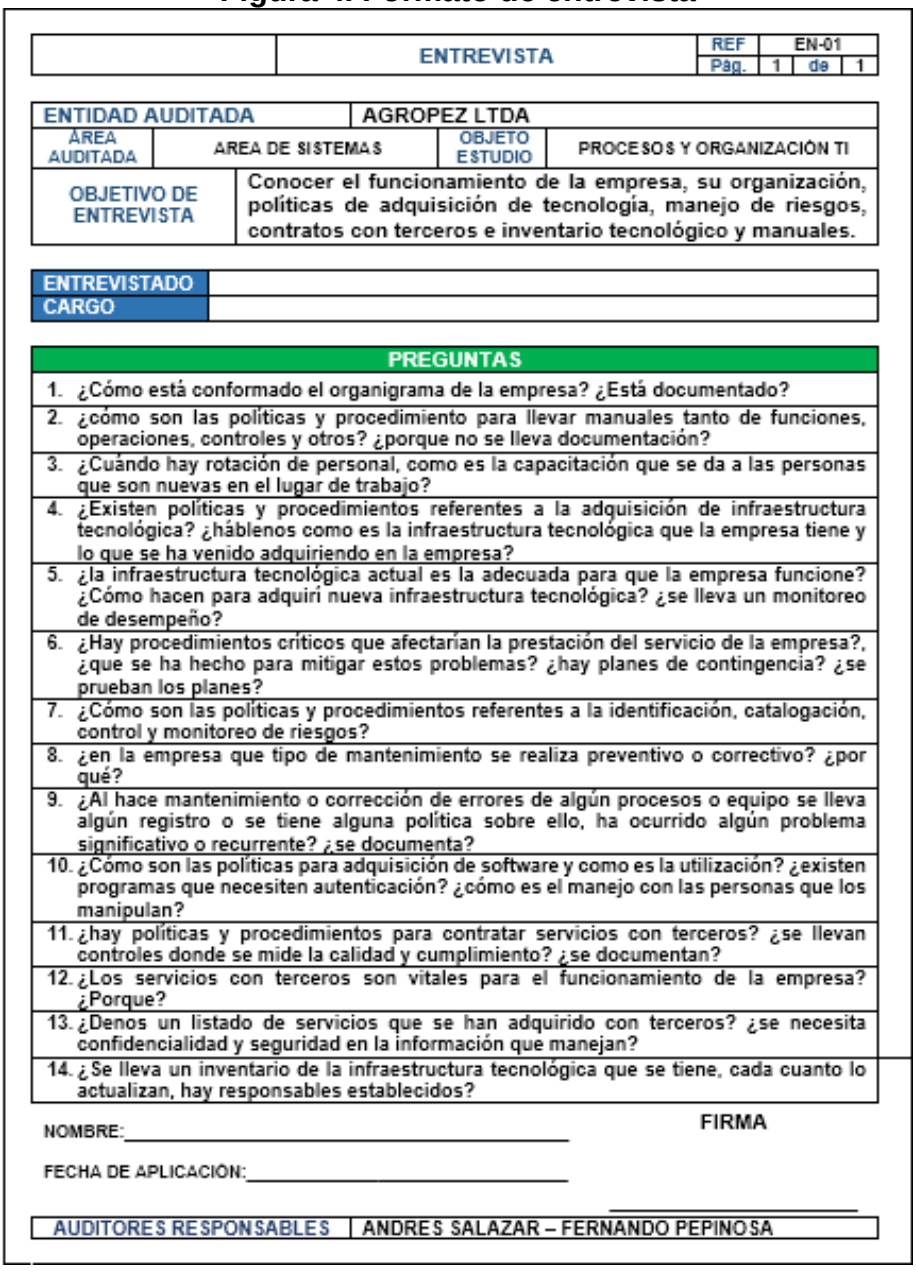
Entrevistas con preguntas abiertas: donde la persona entrevistada pueda expresar libremente su respuesta, generando respuesta con detalles, permitiendo hacer más preguntas según vaya respondiendo cada una.

Entrevistas 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.

Todas las entrevistas aplicadas y los formatos utilizados en el proceso de auditoría se encuentran en los Anexos entregados en medio digital (Ver anexo No. 3).

A continuación, se muestra el ejemplo de un formato de entrevista que se utilizó para realizar el proceso de Auditoría. (Ver figura 4)

Figura 4. Formato de entrevista



	ENTREVISTA	REF	EN-01
		Pág.	1 de 1

ENTIDAD AUDITADA	AGROPEZ LTDA		
ÁREA AUDITADA	AREA DE SISTEMAS	OBJETO ESTUDIO	PROCESOS Y ORGANIZACIÓN TI
OBJETIVO DE ENTREVISTA	Conocer el funcionamiento de la empresa, su organización, políticas de adquisición de tecnología, manejo de riesgos, contratos con terceros e inventario tecnológico y manuales.		

ENTREVISTADO	
CARGO	

PREGUNTAS
1. ¿Cómo está conformado el organigrama de la empresa? ¿Está documentado?
2. ¿cómo son las políticas y procedimiento para llevar manuales tanto de funciones, operaciones, controles y otros? ¿porque no se lleva documentación?
3. ¿Cuándo hay rotación de personal, como es la capacitación que se da a las personas que son nuevas en el lugar de trabajo?
4. ¿Existen políticas y procedimientos referentes a la adquisición de infraestructura tecnológica? ¿háblenos como es la infraestructura tecnológica que la empresa tiene y lo que se ha venido adquiriendo en la empresa?
5. ¿la infraestructura tecnológica actual es la adecuada para que la empresa funcione? ¿Cómo hacen para adquirí nueva infraestructura tecnológica? ¿se lleva un monitoreo de desempeño?
6. ¿Hay procedimientos críticos que afectarían la prestación del servicio de la empresa?, ¿que se ha hecho para mitigar estos problemas? ¿hay planes de contingencia? ¿se prueban los planes?
7. ¿Cómo son las políticas y procedimientos referentes a la identificación, catalogación, control y monitoreo de riesgos?
8. ¿en la empresa que tipo de mantenimiento se realiza preventivo o correctivo? ¿por qué?
9. ¿Al hace mantenimiento o corrección de errores de algún procesos o equipo se lleva algún registro o se tiene alguna política sobre ello, ha ocurrido algún problema significativo o recurrente? ¿se documenta?
10. ¿Cómo son las políticas para adquisición de software y como es la utilización? ¿existen programas que necesiten autenticación? ¿cómo es el manejo con las personas que los manipulan?
11. ¿hay políticas y procedimientos para contratar servicios con terceros? ¿se llevan controles donde se mide la calidad y cumplimiento? ¿se documentan?
12. ¿Los servicios con terceros son vitales para el funcionamiento de la empresa? ¿Porque?
13. ¿Denos un listado de servicios que se han adquirido con terceros? ¿se necesita confidencialidad y seguridad en la información que manejan?
14. ¿Se lleva un inventario de la infraestructura tecnológica que se tiene, cada cuanto lo actualizan, hay responsables establecidos?

NOMBRE:_____ FIRMA

FECHA DE APLICACIÓN:_____

AUDITORES RESPONSABLES	ANDRES SALAZAR – FERNANDO PEPINOSA

B) Matriz de probabilidad de ocurrencia e impacto según relevancia del proceso

La matriz sirve para catalogar un riesgo, saber qué clase de daño puede causar un mal procedimiento en el proceso auditado.

En la matriz existe la columna de probabilidad de ocurrencia donde se pondrá el valor del porcentaje de riesgo según su resultado.

Luego se deberá clasificar el impacto según la relevancia del proceso, esta clasificación será hecha por el equipo auditor basándose en el conocimiento de la entidad y del proceso auditado.

Una vez hecho estos procedimientos se podrá clasificar el riesgo para su posterior entendimiento. (Ver tabla 2)

Tabla 2. Matriz de probabilidad de ocurrencia e impacto según relevancia del proceso

PROBABILIDAD				
	ALTO 71-100%	**ZONA DE RIESGO MODERADO**	**ZONA DE RIESGO IMPORTANTE**	**ZONA DE RIESGO INACEPTABLE**
	MEDIO 31-70%	**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**
		BAJO (LEVE)	**MEDIO (MODERADO)**	**ALTO (CATASTROFICO)**
	IMPACTO			

C) Manual de navegación de hallazgos

En este manual se describe las inconsistencias encontradas.

Esta información fue desglosado de la siguiente manera:

- ***REF:*** Identificación del hallazgo.

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

- ***ÁREA AUDITADA:*** nombre del área a la cual se aplicara la auditoría.

- ***OBJETO DE ESTUDIO:*** nombre del objeto de estudio de la auditoria.

- ***MATERIAL DE SOPORTE:*** nombre del material que soporta el proceso, para el caso será COBIT.

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

- ***PROCESO:*** nombre del proceso que se está auditando dentro de los dominios del COBIT.

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

- ***CONSECUENCIAS Y RIESGOS:*** descripción de las consecuencias del hallazgo así como la cuantificación del riesgo encontrado.

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

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

- **NIVEL DE RIESGO:** se identifica el nivel el hallazgo según:

❖ ***PROBABILIDAD:***

❖ ***IMPACTO:***

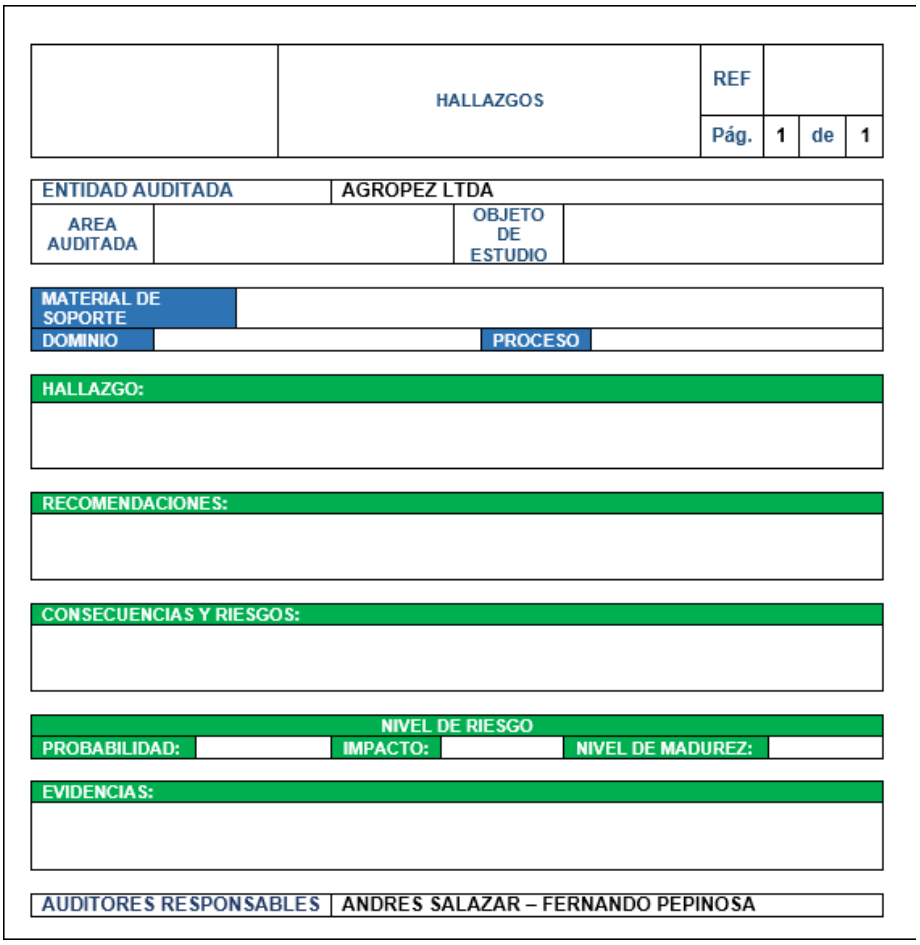
❖ ***NIVEL DE MADUREZ:***

- ***AUDITORES RESPONSABLES:*** nombre del auditor o auditores.

El formato en blanco utilizado en esta investigación es el de la Figura 5.

Todos los formatos de hallazgos utilizados en el proceso de auditoría se encuentran en los Anexos entregados en medio digital (Ver anexo No. 5).

Figura 5. Formato de hallazgos



	HALLAZGOS	REF			
		Pág.	1	de	1

ENTIDAD AUDITADA	AGROPEZ LTDA		
AREA AUDITADA		OBJETO DE ESTUDIO	

MATERIAL DE SOPORTE			
DOMINIO		PROCESO	

HALLAZGO:

RECOMENDACIONES:

CONSECUENCIAS Y RIESGOS:

NIVEL DE RIESGO					
PROBABILIDAD:		IMPACTO:		NIVEL DE MADUREZ:	

EVIDENCIAS:

AUDITORES RESPONSABLES	ANDRES SALAZAR – FERNANDO PEPINOSA

4.3.4 Análisis y evaluación riesgos preliminares. Después de haber realizado el análisis de riesgos se procede a identificar las vulnerabilidades de cada proceso evaluado.

A) Hallazgos dominio 1: planeación y organización (PO)

Los hallazgos encontrados en este dominio fueron los siguientes:

B) Hallazgos PO3 Determinación de dirección tecnológica

Los hallazgos encontrados en este proceso son:

- ***H-PO3:*** No existen políticas y procedimientos referentes a la adquisición de infraestructura tecnológica.

Hallazgos PO9 evaluar y administrar los riesgos de TI

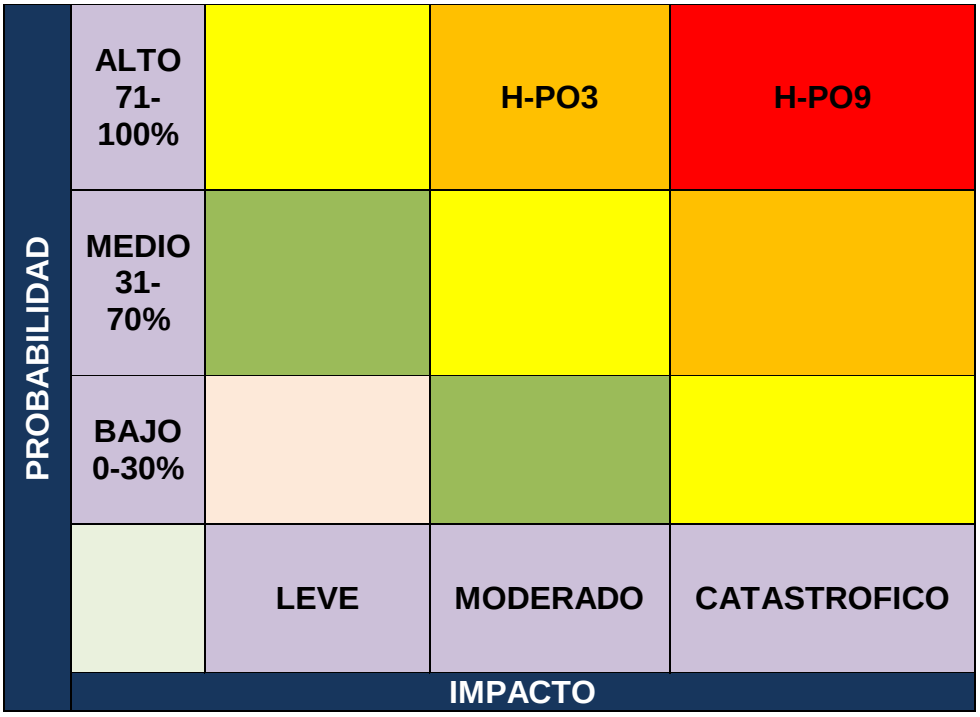
Los hallazgos encontrados en este proceso son:

- ***H-PO9:*** No existen políticas y procedimientos referentes a la identificación de riesgos asociados a TI debidamente documentados, estableciendo alcances, límites y métodos para evaluar, haciendo un posterior monitorio y ejecución de planes de contingencia. (Ver tabla 3)

Matriz de impacto dominio PO

La matriz de impacto del dominio de Planeación y organización es la siguiente:

Tabla 3. Matriz de impacto dominio PO



- ***H-PO3:*** La falta de un rumbo en la tecnología desaprovecha nuevos mercados y mecanismos para abordar el negocio.

- ***H-PO9:*** La inexistencia de políticas y controles para la identificación, evaluación, control de riesgos puede causar la parada de procesos, dejando de brindar el servicio la empresa.

C) Hallazgos dominio 2: adquisición e implementación (AI)

Los hallazgos encontrados en este dominio fueron los siguientes:

Hallazgos AI3 adquisición y mantenimiento de la infraestructura tecnológica

Los hallazgos encontrados en este proceso son:

- ***H-AI3-1-2:*** no existen políticas y procedimientos referentes a evaluación de tecnologías disponibles tanto de software como de hardware e infraestructura.

- ***H-AI3-2-2:*** no Existe políticas y procedimientos para solicitar y llevar a cabo mantenimiento preventivo en los recursos tecnológicos.

AI4 Facilitar la operación y el uso

Los hallazgos encontrados en este proceso son:

- ***H-AI4-1-2:*** no existen políticas y procedimientos referentes a creación y manejo de manuales para las funciones, procedimientos, control o entrenamiento de las tareas diarias.

- ***H-AI4-2-2:*** la Empresa no cuenta con un organigrama escrito. (Ver tabla 4)

Matriz de impacto dominio AI

Tabla 4. Matriz de impacto dominio AI

PROBABILIDAD				
	ALTO 71-100%		H-AI3-1-2 H-AI4-2-2	H-AI3-2-2 H-AI4-1-2
	MEDIO 31-70%			
	BAJO 0-30%			
		LEVE	MODERADO	CATASTROFICO
		IMPACTO		

- ***H-AI3-1-2:*** la inexistencia de políticas y procedimientos referentes a evaluación de tecnologías disponibles tanto de software como de hardware e infraestructura debilita el cumplimiento de los objetivos de la empresa.

- ***H-AI3-2-2:*** al hacer uso únicamente de mantenimiento correctivo se pierde la posibilidad de minimizar el impacto de los problemas, el mantenimiento preventivo ayuda a que los recursos tengan menos probabilidad de que funcionen inadecuadamente, mejorando la prestación del servicio.

- ***H-AI4-1-2:*** la de manuales, información documentada de las funciones, procedimientos, controles y material de entrenamiento dificulta la rotación de personal, creando dependencia directa con las personas que trabajan.

- ***H-AI4-2-2:*** sin un organigrama claro y conocido los empleados genera desorganización y dificulta el trabajo en equipo, como también una correcta comunicación.

D) Hallazgos dominio 3: entrega y soporte (DS)

Los hallazgos encontrados en este dominio son:

DS2 Administrar los servicios de terceros

Los hallazgos encontrados en este proceso son:

- ***H-DS2:*** no existe políticas documentadas y procedimientos para llevar un adecuada contratación de tercero, ni monitoreo y calidad en los servicios.

DS4 Garantizar la continuidad del servicio

Los hallazgos encontrados en este proceso son:

- ***H-DS4:*** no existen políticas y procedimientos para disponer de servicios, planes de contingencia.

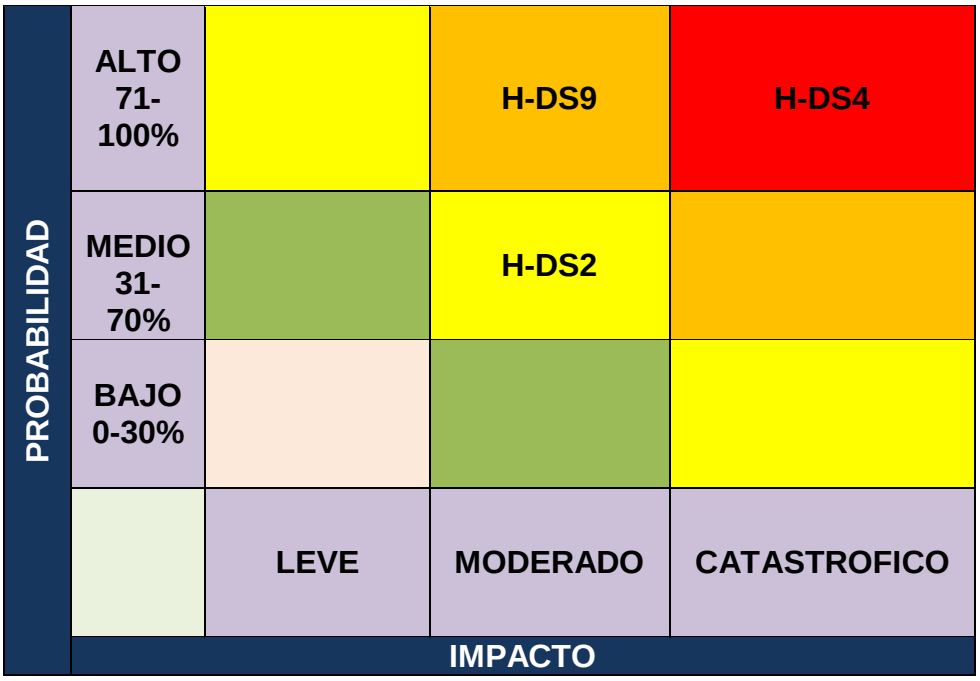
DS9 Administrar la configuración

Los hallazgos encontrados en este proceso son:

- ***H-DS9:*** no existen políticas y procedimientos referentes al manejo de inventario de componentes de TI

Matriz de impacto dominio DS

Tabla 5. Matriz de impacto dominio DS



H-DS2: la contratación de servicios se estipula en los contratos algunas necesidades, se necesita aclarar los puntos importantes de la empresa que se basan en que el servicio esté disponible como por ejemplo internet, además de hacer cotizaciones, monitoreo, evaluación de calidad de los proveedores y planes de contingencia para no depender de un solo proveedor.

H-DS4: sin documentación la dependencia del personal actual es grande, además de no tener posibilidad de crear alternativas en especial de los procesos críticos, causarían traumas en la prestación del servicio o podrían parar las actividades diarias, hay que aprovechar la experiencia del personal y crear controles a los procesos críticos.

H-DS9: sin un inventario, el desconocimiento de lo que se tiene no permite aprovechar los recursos, tampoco se pueden asumir responsabilidades, ni intentos porque estos recursos puedan perdurar, hay que recordar que esos recursos son los que permiten ayudar a los funcionarios para que tomen las mejores decisiones en sus labores.

4.3.5 Informe de Auditoría:

A) Objetivos

Objetivo general

Evaluar la estructura organizacional del área de informática de la empresa AGROPEZ LTDA de la ciudad de Ipiales, los procesos informáticos y manejo de la información.

Objetivos específicos

- Conocer el área de informática y los procesos internos de la empresa AGROPEZ LTDA de la ciudad de Ipiales.

- Realizar un análisis de riesgos para identificar y conocer la causa de los mismos para proponer alternativas de solución.

- Aplicar el proceso de auditoría a los riesgos más relevantes que afecten el funcionamiento del sistema, utilizando las técnicas apropiadas para realizar las pruebas que permitan evidenciar.

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

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

Limitaciones

La auditoría se realizó con completa normalidad, cabe resaltar la colaboración de todo el personal de la empresa AGROPEZ LTDA para hacer posible la toma de datos y la realización de todos los procesos aplicados en el COBIT.

Resultados de la auditoría

A continuación, se presentan los resultados de la auditoría aplicada a la empresa AGROPEZ LTDA, también se presentan las recomendaciones de mejoramiento para cada uno de los procesos COBIT auditados.

B) DOMINIO - PLANIFICACION Y ORGANIZACIÓN (PO)

Proceso COBIT PO3: Determinación de dirección tecnológica:

Hallazgo

No existen políticas y procedimientos referentes a la adquisición de infraestructura tecnológica.

Recomendaciones

- Crear una política y procedimientos para la adquisición de infraestructura tecnológica con base en los objetivos del negocio
- Establecer el plan de la infraestructura tecnológica equilibrado costos contra los riesgos y requerimientos del negocio.
- Establecer un foro para orientar la arquitectura y verifique el cumplimiento.

REF: H-PO3

Proceso COBIT PO9: evaluar y administrar los riesgos de TI

Hallazgo

No existen políticas y procedimientos referentes a la identificación de riesgos asociados a TI debidamente documentados, estableciendo alcances, límites y métodos para evaluar, haciendo un posterior monitorio y ejecución de planes de contingencia.

Recomendaciones

Crear políticas y procedimientos definidos para que administren los riesgos.

Realizar evaluaciones de riesgos periódicas con los gerentes y con el personal clave

Categorizar los riesgos evaluando su impacto, llevando un monitoreo.

Aumentar la probabilidad de la ocurrencia de que se presenten problemas.

La gestión de riesgo permite anticiparse al futuro y prevenir a la empresa de diferentes problemas en este caso riesgos que pongan en peligro el buen funcionamiento de AGROPEZ LTDA, al no tener definido políticas de gestión de riesgos implica la toma de decisiones inmediata frente a un problema emergente sin tener previo análisis del riesgo, ni tener la certeza de poder mitigar ese riesgo.

REF: HD_02

DOMINIO: ADQUISICION E IMPLEMENTACION (AI)

Proceso COBIT AI3: adquisición Y mantenimiento de la infraestructura Tecnológica

Hallazgo

No existen políticas y procedimientos referentes a evaluación de tecnologías disponibles tanto de software como de hardware e infraestructura.

No Existe políticas y procedimientos para solicitar y llevar a cabo mantenimiento preventivo en los recursos tecnológicos.

Recomendaciones

- Crear un plan de adquisición de tecnología que esté de acuerdo con el plan de infraestructura de tecnología.
- Planear el mantenimiento de la infraestructura.
- Proporcionar infraestructura y ambientes de desarrollo de prueba.
- Categorizar los riesgos evaluando su impacto, llevando un monitoreo.
- Implementar medidas de control interno, seguridad y auditoria.
- Crear un proceso de generación de solicitud de nueva tecnología que tenga los siguientes pasos:

❖ Realización de una solicitud formal que describa las características o requerimientos que debe cumplir el software o el hardware que se va a adquirir.

❖ Se deben solicitar por lo menos tres cotizaciones diferentes de los productos a adquirir.

❖ Análisis (mediante cuadros comparativos) de las cotizaciones y elección de la propuesta (costo/beneficio) para la entidad.

- Estas políticas deben ser de conocimiento general, para garantizar la transparencia en estos procesos.

- Crear políticas para llevar a cabo mantenimiento correctivo para los diferentes equipos tecnológicos.
- Generar un cronograma de mantenimiento preventivo.

- Documentar para cada equipo tecnológico hoja de vida de los diferentes mantenimientos.

- Monitorear comportamiento de los recursos tecnológicos frente a los diferentes mantenimientos que se realizan.

REF: H-AI3-1-2, H-AI3-2-2

Proceso COBIT AI4: Facilitar la operación y el uso

Hallazgos

No existen políticas y procedimientos referentes a creación y manejo de manuales para las funciones, procedimientos, control o entrenamiento de las tareas diarias.

La Empresa no cuenta con un organigrama escrito.

Recomendaciones:

- Generar una política para la implementación de manuales de funciones, procedimientos, control y material de entrenamiento de cada funcionario.

- Identificar responsables.

- Crear políticas de participación para actualización de los manuales y transferencia de conocimiento.

- Crear el organigrama de la empresa donde se muestre la estructura organizacional

- Darlo a conocer

REF: H-AI4-1-2, H-AI4-2-2

Dominio: entrega de servicio y soporte

Proceso COBIT DS2: Administrar los servicios de Terceros

Hallazgos

No existe políticas documentadas y procedimientos para llevar un adecuada contratación de tercero, ni monitoreo y calidad en los servicios.

Recomendaciones:

- Crear políticas bien definidas y documentadas para:
- Solicitar servicios con terceros
- Cotizar servicios
- Monitorear llevando registros documentados para evaluar servicios.
- Determinar calidad de servicios.
- Crear planes de contingencia para mitigar riesgos en los servicios del proveedor

REF: H-DS2

Proceso COBIT DS4: Garantizar la continuidad del servicio

Hallazgos

No existen políticas y procedimientos para disponer de servicios, planes de contingencia.

Recomendaciones:

- Crear políticas bien definidas y documentadas para generar controles los cuales permita realizar las tareas de formas alternativas para minimizar el riesgo de depender de elementos externos o minimizar el impacto en especial de procesos críticos de la empresa.
- Documentar procesemos, desarrollar manual de procedimientos.
- Crear un plan de contingencia documentado.
- Hacer pruebas y entrenamiento sobre los planes de contingencia que se implementen.
- Es importante la participación del personal que labora a diario porque

conocen de procesos críticos, como también, posibles soluciones para que mejore el servicio.

- Crear procesos de respaldo de información y equipamiento de back-up.

REF: H-DS4

Proceso COBIT DS9: Administrar la configuración

Hallazgos

No existen políticas y procedimientos referentes al manejo de inventario de componentes de TI.

Recomendaciones

- Crear políticas bien definidas y documentadas para crear un inventario tecnológico disponible.

- Crea mecanismos para actualizar el inventario para que corresponda con la realidad.

- Disponer de hojas de vida de los equipos tecnológicos para llevar un monitoreo adecuado.

- Crear conciencia de la utilización adecuada de los recursos tecnológicos dispuestos.

- Crear mecanismos para solicitud de instalación de software y responsabilidad del uso.

REF: H-DS9

4.3.6 Informe ejecutivo de auditoría

Ipiales

Señor:
JUAN BENAVIDES
Gerente AGROPEZ LTDA
Ciudad

REF: AUDITORÍA INFORMÁTICA A LOS PROCESOS Y ORGANIZACIÓN DEL

ÁREA DE SISTEMAS EN LA EMPRESA AGROPEZ LTDA DE LA CIUDAD DE IPIALES.

Cordial Saludo,

El presente es el informe de la auditoría a la que fue sometida la empresa AGROPEZ LTDA, con el objetivo de evaluar los procesos y organización del área de sistemas.

Los resultados obtenidos son producto de la aplicación de técnicas y herramientas de auditoría, teniendo como base la información y documentación que fue suministrada por el personal laboral de la empresa.

Los resultados obtenidos se sustentan como hallazgos con sus respectivas recomendaciones y en algunos casos fortalezas encontradas. Estas son:

Política de creación y manejo de manuales: falta de manuales de funciones, procedimiento, controles y material de entrenamiento, la falta de este material, hace que la empresa dependa del personal actual, la rotación de personal es complicada, porque se necesita que la personas anterior al cargo capacite a la nueva y si ocurren nuevas necesidades o procesos que no se explicaron en la capacitación, podrían haber riesgos de actuar de forma inadecuada y perder la experiencia de cómo solucionar esas situaciones. Los manuales también permiten apoyar al personal para identificar claramente sus responsabilidades y sus obligaciones, también da un referente de cómo afrontar ciertos casos, los cuales, por falta de experiencia no podrían dar una respuesta rápida, con los manuales se da un modelo de cómo hacer su trabajo, según como la empresa lo necesite y pueda encaminar el trabajo hacia los objetivos planteados.

Hay que recordar que luego de crear los manuales, hay que implementar políticas para actualizarlos y que el personal lo estudie y disponga de ellos para prever problemas y cuando los necesite.

Este punto es el más necesario para empezar a crear documentación empresarial importante para que fortalezca las actividades diarias.

Políticas de manejo de riesgos: crear políticas referentes a identificación de riesgos, los empleados conocen puntos críticos en sus actividades diario, es importante aprovechar este conocimiento para llevar documentado estos procesos y generar actividades alternativas para mitigar riesgos y así, generar un ambiente ante los clientes de disponibilidad de servicio.

El monitoreo de riesgos es importante realizarlo para prevenir sucesos fortuitos que dañen la imagen y reputación de la empresa.

Política, procedimientos y cronograma de Mantenimiento preventivo: es evidente que vivimos en una cultura de reacción, de corregir lo que se daña, sin embargo, una de las principales ayudas que la empresa puede tener para minimizar riesgos operacionales es crear una mentalidad de prevenir antes que curar, el mantenimiento lo que hace es bajar la cantidad de mantenimientos correctivos, esto significa bajar el índice de planes de contingencia o imprevistos en las actividades diarias.

El personal de auditores recalca que este es el punto primordial para que la empresa de un salto gigante a la planeación de actividades, mejorando la organización y prevención de riesgos.

Política de inventario tecnológico: otro de los puntos que se debe tener en cuenta es la inexistencia de inventario tecnológico, la empresa ha hecho un esfuerzo grande por tener equipos que sirvan a los procesos diarios, para brindar un buen servicio, sin embargo no se tiene políticas de llevar conocimiento de los recursos que se tienen y como están estos recursos, al no tener un inventario se pierde la noción de lo que se tiene y las responsabilidades solo recaerían en la buena fe de las personas. Hay recordar que con implementar un inventario tecnológico no es suficiente, sino tener una política empresarial sobre ello, junto a un monitoreo de estos equipos y disponer de actualizaciones del inventario, como también, de sus responsabilidades.

Política de adquisición de tecnología: al hablar de tecnología debemos saber que esta cambia constantemente, mostrando nuevas herramientas, que pueden ayudar a las metas tanto de brindar mejores formas de trabajo, como de también ampliar los límites del mercado, es por ello que colocar políticas de adquisición de equipos hardware, como de recursos software e infraestructura tecnológica, hace que la empresa crezca, mejorando la idea de adquirir cuando se tenga, sino evidenciando en un plan de adquisición la importancia de encaminar estos recursos con los objetivos del negocio.

Política y monitoreo de contratación de terceros: es importante que la empresa cuente con una política bien definida de la contratación con terceros colocando puntos clave como para que se necesita, como se necesita, cuales son las especificaciones técnicas mínimas, especificaciones técnicas adecuadas, disposición, responsabilidades, contraindicaciones, monitoreo de servicio, procedimiento de peticiones, como también cláusulas de no prestación adecuada del servicio, esto es importante para no tener inconvenientes al contratar servicios, además el monitoreo es muy importante, como también la calificación de calidad del servicio, por último la estandarización en la empresa de contratación permite evitar inconvenientes legales. Al contar con servicios con terceros críticos es importante tener planes de contingencia conocidos por los usuarios de la empresa, que en sus actividades diarias, utilizan dichos servicios.

Planes de contingencia: en caso de que el hardware no funcione no existe un plan de contingencia documentado. El no contar con un plan de contingencia dificulta la recuperación de seguir trabajando en un plazo mínimo después de que se haya presentado un problema o desastre inesperado, en caso de presentarse un fallo del hardware la solución de un proceso practico a seguir sería aplicable para un problema técnico y pequeño pero no para un desastre o catástrofe, la interrupción de los servicios de computación y comunicación seria prolongada llevando a las empresas pérdidas financieras significativas. En la empresa debe existir un plan de contingencia documentado que permita dar solución inmediata, este debe contener objetivos de cómo restaurar los servicios de forma rápida, eficiente y con el menor tiempo, costos y pérdidas posibles. La empresa actualmente cuenta con personal capaz de solucionar cualquier problema que se presente aun cuando el plan de contingencia no esté documentado aunque cuando esta presentes terceros estos problemas toman su tiempo haciendo que se vean reflejados los resultados en pérdidas.

Creación de organigrama: otros puntos que la empresa no debe descuidar es la creación de un organigrama, donde se visualice la estructura de la institución para que se pueda organizar el trabajo, junto a sus responsabilidades, además de ayudar al trabajo colectivo.

Plan de mejoramiento: con la realización de la auditoría se espera que esta genere un plan estratégico que asegure el manejo y control de la información concerniente a los PROCESOS Y ORGANIZACIÓN DEL ÁREA DE SISTEMAS, a fin de asegurar la calidad en la infraestructura tecnológica de la empresa AGROPEZ LTDA y que mediante las vulnerabilidades encontradas se diseñe un plan de mejoramiento que permita mitigar los riesgos.

Puntos Positivos: en AGROPEZ LTDA se resalta que los computadores que tiene la organización, son muy buenos, resaltando la disponibilidad por parte de las directivas para invertir en recursos que mejoren la competitividad de la empresa en el mercado, se ha hecho avances en la seguridad física, al utilizar cámaras de vigilancia y elementos de seguridad física que ayuda a salvaguardar los activos tecnológicos, la calidad humana de sus trabajadores es muy buena, junto con su sentido de pertenecía con la empresa, demostrando gran interés por mejorar los procesos que realizan a diario, por todo ello, la empresa teniendo en cuenta con los resultados de la auditoria podrá empezar un cambio, que en el futuro será significativo en los procesos y organización de la tecnología permitiéndole avanzar en el mejoramiento de su organización y así, alcanzar los objetivos planteados.

Atentamente,

JOSE ANDRES SALAZAR
Auditor

FERNANDO JAVIER PEPINOSA ORTEGA
Auditor

5. CONCLUSIONES

La Auditoría de Sistemas de Información, hoy en día es de vital importancia para las empresas modernas con visión de futuro, sobre todo inmersas en el mundo globalizado, porque si no se prevé los mecanismos de control, seguridad y respaldo de la información ésta se verá sumida a riesgos lógicos, físicos y humanos, que conlleven a fraudes no solamente económicos sino de información, es decir, pérdidas para la empresa, para ello toda empresa pública o privada deben de someterse a un control estricto de evaluación de eficiencia y eficacia con el objetivo de que los diferentes procesos funcionen correctamente.

Por medio de COBIT, el auditor logra entender la importancia de la seguridad de la información y de cómo se debe estar pendiente de esta seguridad, de que los sistemas y procesos funcionen correctamente para que cumplan con el objetivo por el cual fueron implementados.

Mediante el proceso de auditoría realizado en AGROPEZ LTDA se logró determinar situaciones de debilidad en cuanto a la adquisición de infraestructura, manejo de riesgos, inventario tecnológico, manuales de funciones, procedimiento y entrenamiento, como también la contratación y monitoreo de servicios con terceros.

A pesar de que existen falencias en el manejo de la infraestructura tecnológica el personal encargado de cada una de las áreas de la empresa han demostrado un total sentido de pertenencia y están comprometidos con los procesos de mejoras, dependiendo también del apoyo que pueda brindar la alta gerencia.

Durante el desarrollo de la auditora es importante mencionar que dentro del análisis y observación se reparó que en AGROPEZ LTDA no existen políticas para el análisis y la gestión de riesgos que permitan la identificación y clasificación de estos, También, hace falta realizar una revisión detallada de la red eléctrica, pues en las agencias se manifestó que hay inseguridad en la red eléctrica y se verifico mediante revisión visual, esta situación está afectando la seguridad de las personas y de los equipos pues se pueden provocar graves accidentes como incendios causados por sobrecarga eléctrica o descuido de cables sueltos o tendidos por el piso.

La realización de la auditoría aporta considerables beneficios a la empresa ya que mejora la eficiencia en los procesos pertenecientes al área de sistemas, desarrollar un plan de mejoramiento que permita garantizar la seguridad, confiabilidad y disponibilidad de los recursos tecnológicos, mediante los resultados obtenidos de la auditoría, entre otros.

Finalmente, con la realización de la Auditoría se ha logrado que se hayan aplicado conocimientos y que como estudiantes hayamos ampliado el aprendizaje de las aulas de clases. Es importante la formación que se obtiene en la Universidad ya que uno se alimenta con el conocimiento y puede así alcanzar capacidades para analizar situaciones a los que se expone la información, identificando debilidades y fortalezas de los procesos que existen en una empresa, consiguiendo así mejorar la calidad de la información.

6. RECOMENDACIONES

Realizar planes de contingencia que permitan garantizar la continuidad de los servicio, ya que son claves para el correcto funcionamiento de los procesos que realizan en la empresa.

Crear un inventario tecnológico de los equipos de cómputo, servidores, entre otros con el fin de llevar un control y un registro adecuado de los activos de la empresa.

Capacitar al personal administrativo de la empresa en cuanto al manejo básico de un computador y de los programas ofimáticos.

Documentar un manual de funciones, uno de procedimiento, uno de controles y de entrenamiento del personal que labora en la empresa.

Evaluar y estudiar el desempeño de la red de datos en su aspecto físico, teniendo en cuenta que hace falta una documentación adecuada de la red de datos.

Crear políticas y procedimientos relacionados con el estudio o análisis de nuevas tecnologías.

Documentar el organigrama de la empresa y hacerlo disponible para el conocimiento de los diferentes participantes de la actividades del negocio.

Crear una cultura de mantenimiento preventivo, junto a controles para llevar el monitoreo de desempeño de los diferentes recursos tecnológicos

REFERENCIAS BIBLIOGRAFICAS

ARENS, Alvin A. Auditoría un Enfoque Integral. 6 Edición. México: Prentice Hall, 1996.

CASTELLANOS, Ricardo J., Auditoria en entornos informáticos, 2ª Ed., Argentina, 2006.

ECHENIQUE GARCIA, José Antonio, Auditoria en informática, 2ª Ed., McGraw-Hill, 2009.

MUÑOZ RAZO, Carlos, Auditoria en sistemas computacionales, 1ª Ed., México: Pearson Educación, 2002.

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

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

ANEXOS