UNIVERSIDAD CENTROAMERICANA
Facultad de Ciencia Tecnología y Ambiente
Departamento de Desarrollo Tecnológico

Auditoría Informática Física y Lógica a la Empresa Almacenes Americanos S.A.

Monografía para Obtener el Título de Ingeniero(s) en Sistemas y Tecnologías de la Información.

Autores:

Br. Cristhian Alberto Narváez Morazán (2007000073).
Bra. Hazell Giovannia Sevilla Mercado (2008930050).

Tutor:

Lic. José Torres Gómez

Managua, Nicaragua
Diciembre, 2012

DEDICATORIA

A Dios por brindarnos la oportunidad y la dicha de la vida, al darnos los medios necesarios para continuar nuestra formación como profesionales, y siendo un apoyo incondicional para lograrlo ya que sin él no hubiera sido posible terminar este trabajo de culminación de estudios.

A nuestros padres: Martha del Socorro Mercado Granados, Sandra del Socorro Morazán García y José Alberto Narváez Martínez, que han sido los motores que impulsan a que nuestros sueños sean una realidad, que nos han apoyado tanto durante nuestra vida y que siempre están cuando más los necesitamos, las personas que realmente creyeron en nosotros, infinitas gracias por haber sido y seguir siendo como son, sin ustedes y sin Dios nada de esto hubiera podido ser posible.

Por último como mención especial se la dedicamos a tres personas que significan mucho en nuestras vidas, la primera persona es Dora Marlene García, ella ha sido un gran soporte y ha ayudado mucho moralmente para que este trabajo fuera además de terminado, realizado con éxito, muchas gracias por compartir su sabiduría, sus consejos y su amor, la segunda persona es Norma Guillermina Martínez Gonzales, su carácter fue ejemplo para superar las dificultades que se presentaron y así poder proseguir con la finalización exitosa de este trabajo y a la niña Jimena Alessandra Sevilla, que su nacimiento fue una luz en nuestras vidas y nos regaló ánimo y alegría, esperamos que su vida sea un éxito.

AGRADECIMIENTO

A Dios que todo lo permite, dándonos fortaleza y perseverancia para culminar con este sueño anhelado.

A nuestros padres por habernos apoyado en todo momento, por sus consejos, sus valores, por la motivación constante, que nos ha permitido ser personas de bien, pero más que nada, por su amor.

Al Licenciado y tutor José Torres Gómez quien aporto su dirección y conocimiento para cumplir con esta meta.

A la Empresa "Almacenes Americanos S.A", que nos permitió efectuar este trabajo en sus instalaciones.

Al Lic. Víctor Hernández Méndez, que nos permitió realizar este trabajo en las instalaciones de la empresa y brindarnos todo el apoyo e información requerida.

A todos quienes de una u otra forma apoyaron desinteresadamente al desarrollo de esta monografía.

A todos ellos, muchas gracias.

Resumen Ejecutivo

El presente trabajo, Auditoría Informática Física y Lógica a la Empresa Almacenes Americanos S.A., representa la forma de culminación de estudios de la carrera de Ingeniería en Sistemas y Tecnologías de la Información de la Universidad Centroamericana de Managua, Nicaragua, en la modalidad de Monografía. Esta auditoría se desarrollo en la empresa privada Almacenes Americanos S.A.

La auditoría se desarrolló con el propósito de evaluar los procesos del área de agencia aduanera de la empresa; los procesos que se llevan a cabo en esta área son los procesos informáticos más relevantes de la empresa. El objetivo principal del trabajo fue ejecutar un plan de auditoría informática para de esta manera obtener resultados claros de la situación de la empresa con respecto a activos de información y procesos informáticos, su gestión y procesamiento.

La metodología utilizada para la realización de esta auditoría fue Metodología para auditorías informáticas (MAI). Tomando como apoyo el estándar COBIT 4.1 se procedió a determinar el ámbito inicial del proyecto, fue necesario plantear los controles a evaluar y determinar el alcance de la auditoría en conjunto con la gerencia general, esto fue posible mediante entrevistas y cuestionarios realizados a los involucrados y observando cómo estos ejecutaban cada proceso.

Una vez obtenida la información, se procedió a realizar el informe final de la auditoría, definiendo la estructura del mismo, tomando en consideración todos los Controles y procedimiento trazados en el plan de auditoría. Una vez concluido el informe final se dió paso a la redacción de recomendaciones y conclusiones.

Al concluir este trabajo monográfico, obtuvimos como resultado un informe final que muestra los resultados obtenidos mediante la ejecución del plan de auditoría, en el que se muestran hallazgos y recomendaciones que servirán a la empresa para evaluar la eficiencia de dicha área, para beneficiar tanto a la empresa, a sus departamentos y a los usuarios que de una u otra forma requieren el servicio de la entidad.

Contenido

Glosario

ACTIVOS: Conjunto de todos los bienes y derechos con valor monetario que son propiedad de una empresa, institución o individuo, y que se reflejan en su contabilidad.

ADUANA: Oficina pública, establecida generalmente en las costas y fronteras, para registrar, en el tráfico internacional, los géneros y mercaderías que se importan o exportan, y cobrar los derechos que adeudan.

AFORO: Determinación de la cantidad y valor de los géneros o mercancías que haya en algún lugar, generalmente a fin de establecer el pago de derechos.

ANTENA: Dispositivo de los aparatos emisores o receptores que, con formas muy diversas, sirve para emitir o recibir ondas electromagnéticas.

ANTIVIRUS: Dicho de un programa: que detecta la presencia de virus y puede neutralizar sus efectos.

APLICACIONES: Programa preparado para una utilización específica, como el pago de nóminas, formación de un banco de términos léxicos, etc.

AUTOMATIZAR: Aplicar la automática a un proceso, a un dispositivo.

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

AUDITORÍA: Es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas. Conjunto de métodos y técnicas con los que se procura identificar y evaluar algo.

AUDITORÍA INFORMÁTICA: 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.

AUDITOR INFORMÁTICO: Evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informáticos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoría, incluyendo el uso del software

BD (Base de Datos): Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

CABLE: Cordón formado con varios conductores aislados unos de otros y protegido generalmente por una envoltura que reúna la flexibilidad y resistencia necesarias al uso a que el cable se destine.

CABLE UTP CATEGORÍA 5E: Es un cable de 8 hilos formado por 4 pares que se usa conjuntamente con conectores rj45 en conexiones de red. Cada par viene enroscado y diferenciado por colores. Los 4 pares a su vez vienen enroscados entre sí, para minimizar los efectos negativos entre ellos y el medio ambiente.

CABLEADO: Conjunto de los cables de una instalación.

CANALETAS: Una canaleta es un ducto adherido a la pared o piso por medio del cual pasara el cable (del tipo que sea).

CÓMPUTO: Cálculo u operación matemática. La noción de cómputo también se utiliza en el marco de la teoría de la computación, la rama de la matemática que se especializa en las capacidades fundamentales de las computadoras. Estas máquinas se encargan de utilizar modelos matemáticos para hacer cómputos.

COMTECH: Empresa proveedora de equipos de cómputo, telecomunicaciones, accesorios, repuestos y suministros de equipos tecnológicos.

COBIT: Marco de referencia de buenas prácticas para el control de ti. Acrónimo en inglés de objetivos de control para la información y la tecnología relacionada, emitido por el IT gobernante instituto.

CONTROL: Las políticas, procedimientos, prácticas y estructura organizacional, diseñadas para proveer una razonable seguridad de que los objetivos del negocio serán alcanzados y los eventos indeseados serán prevenidos o detectados y corregidos."

CONTROL INTERNO: Cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos.

DATATEX: Empresa especialista en tecnología emergente, concentrada en el campo de la computación, internet, cableado estructurado y enlaces inalámbricos.

DATO: información dispuesta de manera adecuada para su tratamiento por un ordenador.

DOMINIO: agrupación de objetivos de control en etapas lógicas en el ciclo de vida de inversión en ti.

ENTIDAD: colectividad considerada como unidad. Especialmente, cualquier corporación, compañía, institución, etc., tomada como persona jurídica.

EQUIPO: Un equipo es un grupo de personas que se unen en función de la consecución de un objetivo en común. Dispositivos y accesorios que forman parte de una computadora o que trabajan con ella.

ESTÁNDAR: Modelo que se sigue para realizar un proceso. Producto de software o hardware que cumple determinadas reglas fijadas por acuerdo internacional, nacional o industrial.

FIREWALL: Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

GESTIÓN: Diligencias conducentes al logro de un negocio o de un deseo cualquiera.

GESTIÓN ADUANERA: Conjunto de funciones indicadas para la gestión tributaria pero con la especialidad de los tributos que son objeto de gestión los derechos de aduanas y aquellos tributos que se devengan en el procedimiento aduanero: el IVA (impuesto de valor agregado) importación.

HARDWARE: Conjunto de los componentes que integran la parte material de una computadora.

HERRAMIENTAS OFIMÁTICAS: Aplicaciones o programas que suelen ser utilizados en tareas relacionadas a las oficinas, trabajos escolares y similares.

HALLAZGO: Debilidades, deficiencias o brechas apreciables respecto a un criterio o estándar previamente definido.

IMPRESORAS: Máquina que conectada a un ordenador electrónico, imprime los resultados de las operaciones.

INFORMÁTICOS: Perteneciente o relativo a la informática.

INTERNET: Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.

ISP: Es una compañía que ofrece acceso a internet, normalmente por una cuota. Normalmente, la conexión con el ISP tiene lugar a través de una conexión de acceso telefónico (línea telefónica) o una conexión de banda ancha (cable o ADSL).

INFORMACIÓN: Conjunto organizado de datos procesados, que constituyen un mensaje sobre un determinado ente o fenómeno.

LÓGICA: La que opera utilizando un lenguaje simbólico artificial y haciendo abstracción de los contenidos.

MARCO DE TRABAJO: Un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia para enfrentar y resolver nuevos problemas de índole similar.

MAI: Metodología para la realización de auditorías informáticas.

MANTENIMIENTO CORRECTIVO: Es aquel mantenimiento que se realiza con el fin de corregir o reparar un fallo en el equipo o instalación.

MANTENIMIENTO PREVENTIVO: Consiste en llevar a cabo un seguimiento del funcionamiento a nivel hardware y software de un sistema. Se vigila constantemente el estado de este y se llevan a cabo medidas preventivas para evitar fallos.

METODOLOGÍA: Conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal.

MDF: Instalación principal de distribución principal. Recinto de comunicación primaria de un edificio. El punto central de una topología de networking en estrella donde están ubicados los paneles de conexión, el hub y el router.

MULTIMEDIALES: Que utiliza conjunta y simultáneamente diversos medios, como imágenes, sonidos y texto, en la transmisión de una información.

OBJETIVO DE CONTROL: Una declaración del resultado o propósito que se desea alcanzar al implementar. Procedimientos de control en un proceso en particular.

PAQUETES: Conjunto de servicios que se ofrecen o de requisitos que se exigen.

PC: Computadora personal. Es una microcomputadora diseñada en principio para ser usada por una sola persona a la vez.

PROCESOS INFORMÁTICOS: Un proceso es un programa en ejecución. Formalmente un proceso es "una unidad de actividad que se caracteriza por la ejecución de una secuencia de instrucciones, un estado actual, y un conjunto de recursos del sistema asociados".

POLÍTICAS: Por lo general, un documento que ofrece un principio de alto nivel o una estrategia a seguir. El propósito de una política es influenciar y guiar la toma de decisiones presente y futura, haciendo que estén de acuerdo a la filosofía, objetivos y planes estratégicos establecidos por los equipos gerenciales de la empresa. Además del contenido de la política, esta debe describir las consecuencias de la falta de cumplimiento de la misma, el mecanismo para manejo de excepciones y la manera en que se verificará y medirá el cumplimiento de la política.

PROCESO: Por lo general, un conjunto de procedimientos influenciados por las políticas y estándares de la organización, que toma 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, dueños responsables, roles claro y responsabilidades alrededor de la ejecución del proceso, así como los medios para medir el desempeño.

PROCEDIMIENTO: Es un método de ejecutar una serie común de pasos definidos que permite realizar un trabajo en forma correcta.

ROUTER: Un router es un dispositivo de interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

RED: Sistema de comunicación entre computadoras que permite la transmisión de datos de una máquina a otra.

RIESGO: Es la vulnerabilidad de los bienes de una institución ante un posible o potencial perjuicio o daño.

SEGURIDAD FÍSICA: Aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.

SEGURIDAD LÓGICA: Aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

SERVICIOS: Función o prestación desempeñadas por organizaciones y su personal.

SERVIDOR: En informática, un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos.

SISTEMA: Programa de ordenador o computadora que tiene capacidad para dar respuestas semejantes a las que daría un experto en la materia.

SISTEMAS OPERATIVOS: Es el software encargado de ejercer el control y coordinar el uso del hardware entre diferentes programas de aplicación y los diferentes usuarios. Es un administrador de los recursos de hardware del sistema.

SISTEMATIZAR: Organizar según un sistema.

SOFTWARE: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

SUBREDES: Son un método para maximizar el espacio de direcciones ipv4 de 32 bits y reducir el tamaño de las tablas de enrutamiento en una intrared mayor. En cualquier clase de dirección, las subredes proporcionan un medio de asignar parte del espacio de la dirección host a las direcciones de red, lo cual permite tener más redes. La parte del espacio de dirección de host asignada a las nuevas direcciones de red se conoce como número de subred.

SISTEMA DE INFORMACIÓN: Un sistema de información es un conjunto de partes que funcionan relacionándose entre sí con un objetivo preciso.

TI: Tecnología de información, conjunto de técnicas que permiten la captura, almacenamiento, transformación, transmisión y presentación de la información generada o recibida a partir de procesos, de manera que pueda ser organizada y utilizada en forma consistente y comprensible por los usuarios que estén relacionados con ella. Incluye elementos de hardware, software, telecomunicaciones y conectividad.

TCO: Empresa dedicada a la creación de soluciones integrales para distintas áreas, una de ellas las agencias aduaneras, este sistema cuenta con el nombre TCO que siginfica **Tecnología, Consultoría, Outsorcing**, este automatiza el ciclo

de operaciones de la agencia de aduana, desde el ingreso de la factura del cliente hasta la elaboración de la póliza y su envío a la aduana central mediante la interface del Sidunea World.

TECNOLOGÍA: Conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico.

TERCEROS: Persona que no es ninguna de dos o más de quienes se trata o que intervienen en un negocio de cualquier género.

TIC: Son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Abarcan un abanico de soluciones muy amplio. Incluyen las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesar información para poder calcular resultados y elaborar informes.

USB: Toma de conexión universal de uso frecuente en las computadoras. Puerto USB.

WINDOWS XP: Es una versión de Microsoft Windows, línea de sistemas operativos desarrollado por Microsoft. Lanzado al mercado el 25 de octubre de 2001, a fecha de agosto de 2012, tenía una cuota de mercado del 46,33%, y fue superado por Windows 7 que ya tenía un 46,60% de cuota de mercado. Las letras "XP" provienen de la palabra eXPeriencia (eXPerience en inglés).

WINDOWS 7: Es una versión de Microsoft Windows, línea de sistemas operativos producida por Microsoft Corporation. Esta versión está diseñada para uso en PC, incluyendo equipos de escritorio en hogares y oficinas, equipos portátiles, Tablet, PC, Netbooks y equipos media center.

1. Introducción

El presente documento plantea la ejecución de una auditoría física y lógica a la empresa Almacenes Americanos S.A, empresa que se dedica a la gestión aduanera, las actividades que se realizan en esta empresa son de diversos tipos tales como: gestión aduanera de importaciones y exportaciones, gestión de exoneraciones, asesoría técnica aduanera, entre otros. Esta empresa como parte de su crecimiento hace uso de las Tic's para sistematizar las áreas del negocio y así ofrecer servicio de calidad a sus clientes.

Es por ello que se pretende, usando como base la auditoría, evaluar de forma particular cada proceso del negocio y así identificar fortalezas y debilidades en la gestión de procesos informáticos de dicha empresa.

Durante el desarrollo de la misma se realizará valoración, verificaciones para determinar el nivel de seguridad, planificación, eficacia y eficiencia con que se están dirigiendo los procesos existentes en la empresa.

Con los resultados obtenidos en la auditoría se podrá fortalecer aquellos procesos que presenten debilidades en la revisión y evaluación de controles, sistemas, comunicaciones y procedimientos informáticos de la empresa.

Al llevar a la práctica las recomendaciones obtenidas en la auditoría informática se espera aumentar la eficiencia y seguridad de la información y así mismo el proceso de toma de decisiones.

2. Objetivos

2.1 OBJETIVO GENERAL

- Ejecutar un plan de auditoría informática lógica y física de los sistemas de información y tecnologías de comunicación de la empresa Almacenes Americanos S.A

2.2 OBJETIVOS ESPECÍFICOS

- Evaluar los términos de referencia de la empresa Almacenes Americanos S.A. para determinar los puntos a valorar en la auditoría.

- Comprobar la existencia de controles internos en la empresa Almacenes Americanos S.A.

- Aplicar técnicas de auditoría informática para la evaluación de controles enfocados en los riesgos de procesos informáticos.

- Comprobar la seguridad en los recursos (tecnología, instalaciones. personal, comunicaciones y aplicaciones) para conocer si cumplen con los objetivos del negocio.

- Presentar informe de hallazgos y recomendaciones obtenidos de la ejecución del plan de auditoría.

3. Justificación

Con la ejecución de la auditoría a la empresa **ALMACENES AMERICANOS S.A** se evaluará la eficiencia del manejo de la información y los procesos de la empresa, lo cual requiere vigilar los procesos de recopilación, procesamiento y almacenamiento de la información dentro de la empresa, todo esto mediante el uso de la tecnología informática; en toda entidad este proceso es vital para el buen funcionamiento de la misma.

Después de realizar el análisis del informe de la auditoría, la empresa podrá hacer mejoras en su red y en el uso de los sistemas de información, lo cual conllevará a mejorar el procesamiento de la información, permitiendo optimizar el tiempo de respuesta hacia el cliente.

Cabe destacar que con la ejecución de la auditoría, la empresa podrá tener identificado los riesgos en los procesos informáticos, también le permitirá comprobar su calidad y capacidad en cuanto a los requerimientos de hardware y software que utiliza.

4. Marco Teórico

En esta primera parte se hará un análisis teórico sobre auditoría, su definición, sus objetivos, tipos, importancia, análisis de riesgos, controles internos, metodología, sus funciones, sus tipos y herramientas, la planeación de la auditoría, finalizando con el informe final de auditoría.

4.1 GENERALIDADES DE AUDITORÍA

La auditoría es una función de dirección cuya finalidad es analizar y apreciar el control interno de las organizaciones, con vistas a las eventuales acciones correctivas para garantizar la integridad de su patrimonio, la veracidad de su información y el mantenimiento de la eficacia de sus sistemas de gestión.

La función de auditoría debe ser independiente; no tiene carácter ejecutivo ni son vinculantes sus conclusiones, la empresa decide cuáles serán las acciones pertinentes.

La auditoría tiene como finalidad evaluar el uso adecuado de la información dentro de los procesos de la empresa, y la emisión oportuna de los resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados en el funcionamiento de la empresa.

La auditoría surgió a partir de que el comercio fue tomando un crecimiento bastante amplio, fue entonces que se generó la necesidad de revisiones para asegurarse el adecuado manejo de los procesos de las empresas comerciales.

La auditoría como profesión fue reconocida por primera vez bajo la ley británica de sociedades anónimas de 1862 y el reconocimiento general tuvo lugar durante el período de mandato de la ley “Un sistema ordenado y normalizado de contabilidad era deseable para guía adecuada de información y para la prevención del fraude. *(Cashin, J. Neuwirth, P. Levy, J. Mainou Abad, J. (1999)).*

También reconocía “Una aceptación general de la necesidad de efectuar una versión independiente de las cuentas de las pequeñas y grandes empresas”. Desde 1862 hasta 1905, la profesión de la auditoría creció y floreció en Inglaterra, y se introdujo en los Estados Unidos hasta 1900. En Inglaterra siguió haciéndose hincapié en cuanto a la detección del fraude como objetivo primordial de la auditoría.

4.1.1 **Tipos de Auditoría**

Siendo la auditoría una parte tan importante para el buen funcionamiento de la empresa, ha sido necesario dividirla y especializarla según el tipo de área a trabajar, para lograr un mejor análisis de dicho entorno.

Dentro de los diferentes tipos de auditorías existen:

- **Auditoría Externa:** Una auditoría externa es aquella que es realizada por una firma externa de profesionales con el propósito de evaluar los estados financieros de una empresa. Se trata de un procedimiento de uso común cuando se quiere comprobar que una empresa se maneja financieramente de forma honrosa.1

- **Auditoría Financiera:** La auditoría financiera tiene como objeto la revisión de los estados financieros por parte de un auditor del que preparo la información contable y del usuario, con el fin de establecer sus puntos para

[1] Concepto extraído de http://economiaes.com/presupuesto/externa-auditoría.html.

dar a conocer resultados de su examen, a fin de aumentar la utilidad que la información posee. *Sierra, E.(2006)*

- **Auditoría Fiscal:** Es un proceso que consiste en la obtención y evaluación de evidencias acerca de los hechos vinculados a los actos de carácter tributario.[2]

- **Auditoría Integral:** Es el examen crítico, sistemático y detallado de los sistemas de información financiero, de gestión y legal de una organización, realizado con independencia y utilizando técnicas específicas, con el propósito de emitir un informe profesional sobre la razonabilidad de la información financiera, la eficacia eficiencia y economicidad en el manejo de los recursos y el apego de las operaciones económicas a las normas contables, administrativas y legales que le son aplicables, para la toma de decisiones que permitan la mejora de la productividad de la misma. *Zamarrita, E (2002)*

- **Auditoría Interna o de Campo:** La auditoría interna es un proceso cuya responsabilidad es parte de la Alta Gerencia de las compañías, y se encuentra diseñado para proporcionar una seguridad razonable sobre el logro de los objetivos de la organización.

- **Auditoría Interna o Auditoría contable financiera**: Tiene como objeto averiguar la exactitud, integridad y autenticidad de los estados financieros, expedientes y demás documentos administrativo-contables presentados por la dirección, así como sugerir las mejoras administrativo-contables que procedan.

- **Auditoría Informática:** Se refiere a la revisión práctica que se realiza sobre los recursos informáticos con que cuenta una entidad con el fin de emitir un informe o dictamen sobre la situación en que se desarrollan y utilizan estos recursos. *Bautista, J (2007).*

[2] Concepto extraído de: http://definicion.de/auditoría-fiscal/

4.1.2 **Auditoría Informática**

En la actualidad el costo de los equipos de cómputo han disminuido, y su potencia, rendimiento y seguridad han venido siendo inversamente proporcionales a los costos, esto quiere decir que a menor precio mayor capacidad de procesamiento, esto es posible porque si es cierto que se paga menos por un equipo de cómputo, su rendimiento es mayor gracias al avance de la tecnología.

Las nuevas herramientas con las que contamos como Internet, bases de datos, herramientas multimediales, hacen posible el fácil acceso a una gran cantidad de información en poco tiempo; aunque el costo de los sistemas completos es demasiado elevado, así mismo la manejabilidad y seguridad son igual de elevados.

Uno de los grandes y comunes problemas de los centros de cómputos es que estos carecen de una buena organización en el cableado, esto debería ser al contrario para que estos centros cumplan con las expectativas y exigencias de las empresas.

Además de la falta de organización, está la rapidez abrumadora con que estos equipos se renuevan o cambian de características afectando áreas claves de la informática en la empresa, tales como base de datos, aplicaciones, redes y en fin los sistemas de información en si, además de que se necesita para administrar bien los centros de cómputos una planeación estratégica y corporativa que permita a las empresas ir de la mano con las tecnologías de la información.

Estos factores han aumentado considerablemente la complejidad de los problemas así como la toma de decisiones respecto a las tecnologías de la información, pensamientos como el centrarse en los equipos y no en la información han traído como consecuencia el fracaso de grandes centros de cómputos, ya que sin la información adecuada una empresa no puede trabajar correctamente.

Otra deficiencia en los centros de cómputo es el desconocimiento en el adecuado empleo de herramientas administrativas, esto repercute en el área de informática, en el mal control de los usos de la información y de los recursos de la misma.

Los sistemas de información se han proliferado y así los problemas que estos poseen, por esto existe la auditoría en informática y es conveniente precisar y aclarar la función de esta en la organización, además de la profundidad de la realización que es totalmente dependiente de las características y número de equipos de cómputo que se tengan.

Antes de definir auditoría informática, se abordará el concepto de informática que se define como una automatización de la información por su procedencia en francés, aunque no existe una sola concepción de lo que es informática.

Aunque este se fue transformando con los años, por ejemplo 1966 la academia francesa describió la informática como la ciencia del tratamiento sistematizado y eficaz de la información, en 1975 la IBI dijo que era la aplicación racional y sistemática de la información para el desarrollo social, económico y político, la misma IBI para ese tiempo dijo que la informática es la ciencia de la política de la información y así sucesivamente.

4.1.3 **Tipos de Información**

La información al ser un bien tan preciado y delicado ha llegado al punto de ser secreta en algunos casos, por tener tanto rango, también se le ha dado niveles a la información, el primer nivel es el de técnico que considera eficacia y capacidad de los canales de transmisión, el segundo nivel es el semántico que se ocupa de la información por su significado, el tercero es el pragmático que es el que considera al receptor en un contexto y el cuarto evalúa la información desde un punto de vista ético y a quien se le difunde la información o su destino.

A medida que las distintas empresas crecen, sus áreas internas también, es por esta razón que se ha tenido que evaluar el funcionamiento de dichas áreas

mediante el uso de normas establecidas y revisadas por comités expertos en estas áreas.

Después de implementadas estas normas, el siguiente paso es revisar que sean cumplidas y si existen cambios en dichas normas para implementarlas, en las nuevas empresas se debe enterar a los encargados de áreas de que dichas normas existen, este es el trabajo de un auditor, dar a conocer y mantener las normas establecidas y si no se cumplen presentar los fallos y al mismo tiempo plantear las soluciones más aterrizadas a la empresa.

Dentro de las áreas que componen una empresa hoy en día, quizás la más importante sea la de informática, así que no es de extrañarse que tenga muchas normas y que sean exigentes al manejar el elemento más importante de toda organización, la información.

La información es el activo más importante de la empresa, por esto las mismas han buscado la mejor forma de protegerla y administrarla, no es sorpresa que se establezcan una serie de normas para esto; así como la tecnología es cambiante estas normas también, ya que tienen que adecuarse a las nuevas tecnologías y también a los ámbitos de cada una de estas.

Así como existen tantos recursos tecnológicos existen necesidades en las empresas y tantos equipos como servicios, entonces hay que hacer una revisión constante de que cada recurso este en el área indicada, cubriendo el servicio adecuado.

Además de esto la auditoría informática contempla ¿Cómo estos equipos se administran?, ¿Porque están ahí? ¿Quién decidió ponerlos ahí? ¿Con qué propósito? Y más importante ¿Deberían de estar ahí?, son algunos puntos principales de la auditoría informática.

Se contempla la parte lógica, el manejo en sí de la información y las herramientas adecuadas para administrarlas, en otras palabras el software que se ocupa o el conjunto de software utilizado para realizar esta función.

A grandes rasgos esto es lo que contempla la auditoría informática, más adelante entraremos de lleno a definiciones más concretas de la auditoría informática, sus fases y objetivos.

Tomando en cuenta los aspectos planteados y la interrelación de trabajo de los distintos software, así como la finalidad, ya sea recopilar, procesar, almacenar y buscar la información que se necesite o sea común al objetivo de la empresa podemos definir lo que es auditoría informática.

4.1.4 **Definición de auditoría informática**

Se define auditoría informática como una función que ha sido desarrollada con el propósito de proteger los activos de los sistemas de cómputo, mantener la integridad de los datos y así alcanzar la organización eficaz y eficiente.

Según Iturmendi, J.J (1994) define auditoría informática como “un conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un sistema informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existente en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente”.

También se puede decir que, es la revisión y evaluación de controles, sistemas procedimientos de la información de los equipos de cómputo, su utilización, eficiencia y seguridad.

4.1.5 **Objetivo de la auditoría informática**

El objetivo que la auditoría informática persigue es la evaluación de un sistema informático para emitir una opinión sobre la fiabilidad y exactitud de los datos procesados, así como detectar y corregir errores encontrados y asegurar la continuidad del soporte automatizado de la gestión y por último elaborar un informe de recomendación y de plan de acción.

4.1.6 **Alcance de la auditoría informática**

Así como el resto de las auditorías, la auditoría informática tiene su alcance definido, este alcance debe de delinear con precisión el entorno y los límites que van a desarrollarse en la auditoría informática, este alcance es complementario con los objetivos de la auditoría informática.

El alcance ha de figurar expresivamente en el informe final de modo que pueda perfectamente determinar, no solamente hasta qué punto ha llegado la auditoría, sino cuales materias fronterizas han sido omitidas.

4.1.7 **Factores influyentes en la auditoría informática**

A la hora de realizar una auditoría informática hay que tener en cuenta ciertos factores que pudieran ser decisivos a la hora de los resultados, dichos factores son: la necesidad de controlar el uso evolucionado de las computadoras, controlar el uso de la computadora, que cada día se vuelve más importante y costosa, el abuso en las computadores, valor del software y del hardware y personal y por último la toma de decisiones incorrectas.

4.1.8 **Fases de la auditoría**

Para que los resultados de una auditoría sean óptimos, esta deberá estar basada en alguna metodología ampliamente conocida para la realización de auditorías. En general las fases en que se desarrolla toda auditoría son:

Planeación: Aquí se debe planificar como realizar la auditoría, con los pasos a seguir, además de tener claro las herramientas a ocupar para la recolección, procesamiento y presentación de los datos necesarios para la auditoría, cabe destacar que el planeamiento está estrictamente ligado a los objetivos específicos de la auditoría.

Ejecución: En esta fase se plantea el trabajo a realizar, recopilando y analizando los datos, es decir, tomar la información y procesarla de acuerdo a los objetivos de la auditoría.

Informe de la auditoría: Aquí se presentan de forma clara, coherente y entendible las conclusiones de la auditoría, que dicho sea de paso es el resultado del procesamiento de la información y se compone de las sugerencias realizadas en base a lo observado y a las reglas aplicadas para enmarcar a la auditoría (estándares).

4.1.9 **Finalidad de la auditoría**

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 en los servicios que proporcionan los sistemas computacionales de la empresa.

4.1.10 **Control interno y auditoría informática**

Este es el seguimiento a las recomendaciones emitidas en la auditoría, es revisar si se están cumpliendo a cabalidad lo que se implementó con el fin de reducir los errores y que estos no persistan o estén apareciendo y desapareciendo.

Estos están estrechamente ligados con el control interno de la empresa que es el plan de organización de todos los métodos y procedimientos que son relativos y que están directamente relacionados con salvaguardar los activos y la confiabilidad de los registros financieros.

Además del control interno, también existe el control interno informático que es el que controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijadas por la dirección de la organización y la dirección de informática.

4.1.11 **Tipos de controles internos**

Los controles informáticos se dividen en las siguientes categorías:

- ✓ **Controles preventivos:** para tratar de evitar el hecho, como por ejemplo que un software de seguridad impida los accesos no autorizados al sistema.
- ✓ **Controles defectivos:** cuando fallan los preventivos para tratar de conocer cuanto antes el evento.
- ✓ **Controles correctivos:** facilitan la vuelta a la normalidad cuando se han producido incidencias.

4.1.12 **Técnicas para la auditoría informática**

Existen muchas herramientas para la ejecución de una auditoría informática, estas ayudan a la gestión de examinar que tan eficientes y eficaces son los controles del área evaluada, entre las herramientas más usada para auditar están:

- Cuestionarios
- Entrevistas
- Formularios Checklist
- Formularios Virtuales
- Pruebas de consistencias
- Inventarios y valorizaciones
- Reporte de bases de datos y archivos
- Reporte de estándares

- Software de interrogación
- Fotografías o tomas de valor
- Diseños de flujos y de la red de información
- Planos de distribución e instalación
- Certificados, garantías, otros del software
- Historia de cambios y mejoras

4.1.13 Principales pruebas y herramientas para efectuar una auditoría informática

Al elaborar una auditoría informática el auditor puede realizar las siguientes pruebas:

- **Pruebas clásicas:** Consiste en probar las aplicaciones/sistemas con datos de prueba, observando la entrada, la salida esperada, y la salida obtenida. Existen paquetes que permiten la realización de estas pruebas.

- **Pruebas sustantivas:** Aportan al auditor informático las suficientes evidencias y que se pueda formar un juicio. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican así mismo la exactitud, integridad y validez de la información.

- **Pruebas de cumplimiento:** Determinan si un sistema de control interno funciona adecuadamente según la documentación, según declaran los auditados y según las políticas y procedimientos de la organización.

4.2 COBIT 4.1

4.2.1 Definición

COBIT es un acrónimo formado por las siglas derivadas de Control Objetives for Information and Related Technology (Objetivos de Control para la Información y Tecnologías Relacionadas). *ISACA, org. (2007)*

Este conjunto de objetivos representa el producto de un proyecto de investigación desarrollado por la Information System Audit and Control Fundation (ISACF) que fue publicado inicialmente en el año de 1996.

Como su nombre lo indica, COBIT es un conjunto de objetivos de control aplicables a un ambiente de tecnologías de información que lograron definirse gracias a un trabajo de investigación y búsqueda de consenso entre la normatividad de distintos cuerpos colegiados, estándares técnicos, códigos de conducta, prácticas y requerimientos de la industria y requerimientos emergentes para industrias específicas (desde la banca hasta la manufactura). Este extenso trabajo de investigación realizado por equipos de expertos de América, Europa y Oceanía, dio como resultado un grupo estructurado de objetivos de control que al ser compatibles con las principales normas a nivel internacional, cuenta con una aceptación implícita como un estándar global en términos de control interno en tecnologías de información.

4.2.2 Misión

La misión de COBIT es: “investigar, desarrollar, publicar y promover un conjunto internacional, autorizado y actual de objetivos de control en tecnologías de información generalmente aceptados por el uso cotidiano de gerentes de organizaciones y auditores”.

Entonces, el propósito de COBIT es proporcionar una guía estándar que tenga una aceptación internacional sobre los objetivos de control que deben existir en un ambiente de tecnología de información para asegurar que las organizaciones logren los objetivos de negocio que dependen de un adecuado empleo de dicha tecnología.

4.2.3 **Estructura**

COBIT logra un primer acercamiento entre los mundos de los negocios y del control de tecnología de información, mundos que históricamente aparecían distantes uno del otro, aunque la necesidad de interacción fuese evidente.

La estructura de COBIT se fundamenta en la idea de que los recursos de TI deben ser utilizados en forma adecuada mediante la ejecución de procesos de trabajo para satisfacer los requerimientos de (información del) negocio que existen en las organizaciones.

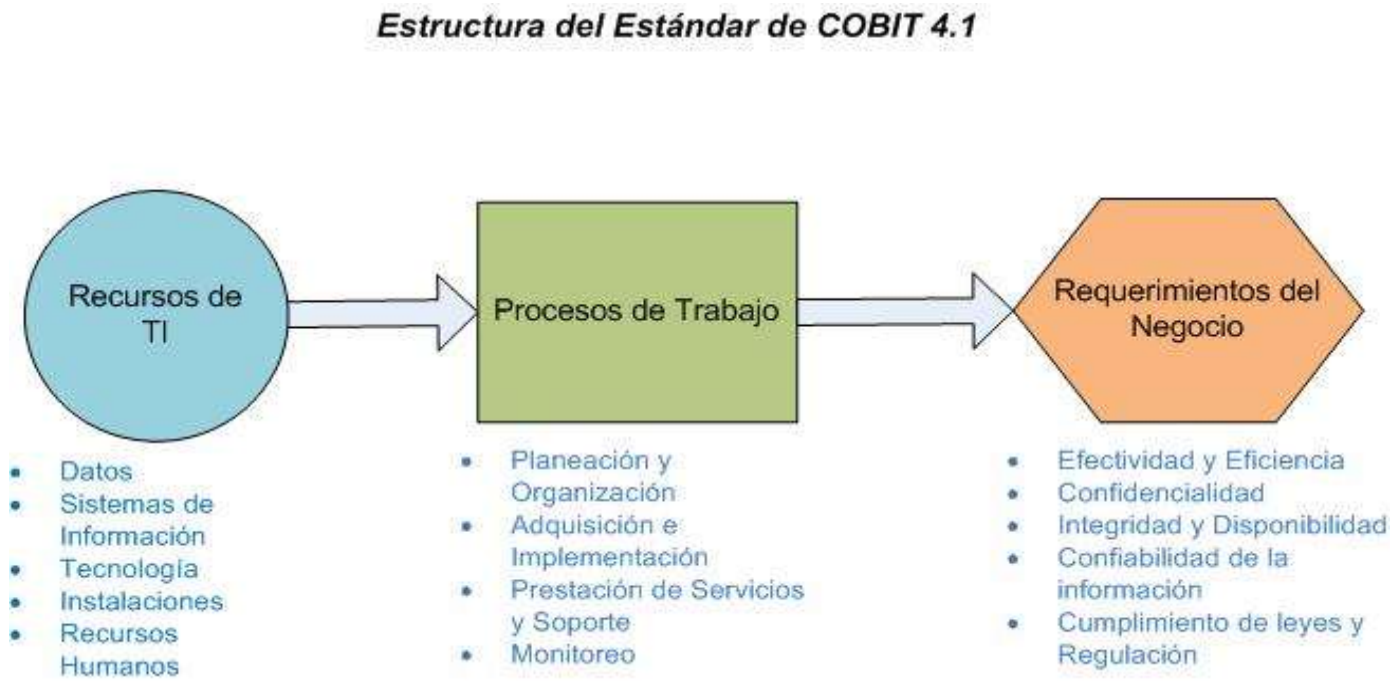


Figura 1. Esquema de estructura del estándar COBIT 4.1

a) Recursos de TI

La clasificación que propone COBIT sobre los recursos de tecnología de información es la siguiente:

Datos: Incluye a los objetos de información en su sentido más amplio, considerando información interna y externa, estructurada y no estructurada, gráfica, sonidos, etc.

Sistemas de información: Este concepto se entiende como los sistemas de información (aplicaciones) que integran tanto procedimientos manuales como procedimientos programados (basados en tecnología)

Tecnología: Incluye hardware, sistemas operativos, sistemas de administración de base de datos, equipos de redes y telecomunicaciones, video conferencia, etc.

Instalaciones: Incluye los recursos necesarios para alojar y dar soporte a los sistemas de información.

Recursos Humanos: Este concepto incluye, habilidades, conciencia y productividad del personal para planear, adquirir, prestar servicios, proporcionar soporte y monitorear los sistemas y servicios de información.

4.2.4 **Procesos de Trabajo**

COBIT clasifica los procesos de trabajo en tres niveles jerárquicos, dominios, procesos y actividades o tareas. Los cuatro dominios definidos se estructuran de acuerdo con el esquema que se utiliza para representar el ciclo de vida de administración de recursos:

Planeación y organización: *Planning and organization* (PO)

Adquisición e implementación: *Acquisition and implementation* (AI)

Entrega de servicios y soporte: *Delivery and support* (DS)

Monitoreo: *Monitoring* (M).

Estos dominios a su vez se subdividen en procesos:

1) Planeación y Organización (PO)

PO1: Definir un plan estratégico de sistemas.

PO2: Definir la arquitectura de información.

PO3: Determinar la dirección tecnológica.

PO4: Definir la organización y sus relaciones.

PO5: Administrar las inversiones en TI.

PO6: Comunicar la dirección y objetivos de la gerencia.

PO7: Administrar los recursos humanos.

PO8: Asegurar el apego a disposiciones externas.

PO9: Evaluar riesgos.

PO10: Administrar proyectos.

PO11: Administrar calidad.

2) Adquisición e Implementación (AI)

AI1: Identificar soluciones de automatización.

AI2: Adquirir y mantener software de aplicaciones.

AI3: Adquirir y mantener la arquitectura tecnológica.

AI4: Desarrollar y mantener procedimientos.

AI5: Instalar y acreditar sistemas de información.

AI6: Administrar cambios.

3) Prestación de Servicios y Soporte (DS)

DS1: Definir niveles de servicio.

DS2: Administrar servicios de terceros.
DS3: Administrar desempeño y capacidad.
DS4: Asegurar la continuidad de servicio.
DS5: Garantizar la seguridad de sistemas.
DS6: Identificar y asignar costos.
DS7: Educar y capacitar usuarios.
DS8: Apoyar y orientar a clientes.
DS9: Administrar la configuración.
DS10: Administrar problemas e incidentes.
DS11: Administrar la información.
DS12: Administrar las instalaciones.
DS13: Administrar la operación.

4) Monitoreo (M)

M1: Monitorear el proceso.
M2: Evaluar lo adecuado del control interno.
M3: Obtener aseguramiento independiente.
M4: Proporcionar auditoría independiente.

Posteriormente y como producto de un análisis más profundo, COBIT define las actividades o tareas en que se descompone cada uno de los 34 procesos e identifica los objetivos de control que deben existir en cada uno de ellos, tal como se muestra en el siguiente ejemplo:

DS. Prestación de servicios y soporte *(dominio)*
DS2. Administrar servicios de terceros *(proceso)*
2.3. Contrato con terceros *(actividad o tarea)*

Objetivo de control: “La Gerencia debe definir procedimientos específicos para asegurar que un contrato formal es definido y acordado para cada relación de servicios con un proveedor”.

Requerimientos de negocio

Por lo que respecta a requerimientos de negocio COBIT, se orienta en forma exclusiva a requisitos relacionados con la información. En un primer análisis presenta la siguiente clasificación:

Requerimientos de calidad:

- Calidad.
- Costo
- Prestación de servicio.

Requerimientos de confianza:

- Efectividad y eficiencia de operaciones.
- Confiabilidad de la información.
- Cumplimiento de leyes y regulaciones.

Requerimientos de seguridad de la información:

- Confidencialidad.
- Integridad.
- Disponibilidad.

De acuerdo con esta clasificación preliminar y mediante un análisis de los conceptos que integra y de las áreas comunes de interés que se presentan entre los mismos, COBIT resume los requerimientos (de información) del negocio en las siguientes siete categorías:

Efectividad: Se refiere a que la información debe ser relevante y pertinente para los procesos de negocio así como ser proporcionada en forma oportuna, correcta, consistente y utilizable.

Eficiencia: Se refiere a proveer la información mediante el empleo óptimo (la forma más productiva y económica impuestas en forma externa) de los recursos.

Confidencialidad: Se refiere a la protección de la información sensitiva contra la divulgación no autorizada.

Integridad: Se refiere a lo exacto y completo de la información así como a su validez de acuerdo a los valores y expectativas de la organización.

Disponibilidad: Se refiere a la accesibilidad de la información cuando sea requerida por los procesos de negocio ahora y en el futuro. También se relaciona con la salvaguarda de los recursos necesarios y las capacidades asociadas a los mismos.

Cumplimiento: Se refiere al cumplimiento de leyes, regulaciones y compromisos contractuales a los cuales está comprometida la organización, por ejemplo; criterios de negocio.

Confiabilidad de la información: Se refiere a proveer la información apropiada para que la administración opere la organización y cumpla con sus responsabilidades de informes financieros y de cumplimiento normativo.

5. Marco Metodológico

5.1 TIPO DE INVESTIGACIÓN

El enfoque metodológico propuesto para la realización de la auditoría fue un enfoque cualitativo ya que los pasos a seguir y los resultados de la ejecución de la misma se hicieron mediante un plan de trabajo flexible y con criterio humano. Como parte del proceso que se llevó a cabo se utilizó el lineamiento del estándar COBIT 4.1 para reforzar el procedimiento que se llevó a cabo al momento de la ejecución.

Como guía, para el desarrollo de la auditoría a la empresa **Almacenes Americanos S.A**, se empleó la metodología **MAI** (Metodología de Auditoría Informática), para la cual toda auditoría informática debe realizarse en las siguientes fases:

1. **Preliminar**

En esta fase se dieron los primeros pasos de la auditoría, es la realización de un diagnóstico general de la gerencia y de las áreas de la entidad, se requirió de poco tiempo para la realización de la misma ya que a través de esta se pretendía únicamente determinar los puntos débiles y fuertes del área de informática, desde el punto de vista de la alta gerencia y de los usuarios de cada área.

2. **Justificación**

En esta fase el auditor se enfocó en el desarrollo de un documento, para la aprobación del proyecto. También se definieron las áreas y componentes de informática que fueron evaluados con lo que se logró conseguir el compromiso del

personal de informática, de los usuarios y demás involucrados para participar cuando se necesitó de su participación.

3. **Adecuación**

En esta etapa el trabajo se enfocó en el análisis, adecuación y actualización detallados de todos los elementos definidos en la etapa anterior y que fueron evaluados en la auditoría informática.

Una vez terminada esta fase se tuvo el proyecto bien especificado y listo para ejecutarlo en las siguientes fases.

4. **Formalización**

Las etapas anteriores brindaron en conjunto, al auditor, un panorama de la situación de la empresa y de la función de informática; en ellas se detectaron las debilidades y fortalezas más relevantes, también se definió la planeación y proyección de las áreas que requerían ser auditadas, y se documentaron las adecuaciones.

En esta etapa correspondió a la alta dirección dar su aprobación y apoyo formal para el desarrollo del proyecto de auditoría, de manera que quedaran claro los límites y el acuerdo entre la empresa y auditores acerca de la auditoría.

5. **Desarrollo**

En esta etapa, los auditores en informática ejercieron su función de manera práctica, es decir, comenzaron a ejecutar sus tareas con profesionalismo, ética personal y aplicando sus conocimientos y experiencias, de acuerdo con el plan aprobado en la etapa anterior; con el fin de obtener un producto final de calidad y beneficios tangibles para el negocio.

5.2 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

En función del logro de los objetivos de esta auditoría, se emplearon instrumentos y técnicas orientadas a obtener información relevante, estos fueron recolectados a través de los siguientes instrumentos:

- **Cuestionarios:** Los cuestionarios son una serie de preguntas ordenadas, que buscan obtener información de parte de quien las responde, para servir a quien pregunta o a ambas partes.

- **Entrevistas:** Es una de las actividades personales más importantes del auditor; en ellas se reúne más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

- **Observación:** Es el registro visual de lo que ocurre en una situación real, clasificado y consignando los datos de acuerdo con algún esquema previsto y de acuerdo al problema que se estudia.

- **Hoja de Procesamiento de Datos (Word):** Este software sirvió de apoyo para la redacción del informe final de la auditoría, así como recomendaciones, hallazgos y conclusiones.

6. Desarrollo

El proceso de auditoría aplicado a la empresa **Almacenes Americanos S.A**, se desarrolló empleando la metodología MAI, la cual provee una serie de fases como guía para la realización de todo el proceso de auditoría, para seleccionar el área a auditar, se evaluó los diferentes departamentos de la empresa, seleccionándose el área donde se manejan los procesos informáticos.

A continuación se describe el desarrollo de la auditoría a la empresa Almacenes Americanos S.A, a través de la metodología MAI:

6.1 **PRELIMINAR**

La empresa Almacenes Americanos S.A es una empresa de giro aduanero, los servicios que estos ofrecen son:

- Liquidación de pólizas
- Desaduanaje de mercancías
- Gestión aduanera de importaciones y exportaciones
- Gestión de exoneraciones
- Asesoría técnica aduanera

La empresa cuenta con dos áreas principales que son el área de almacén fiscal y el área de agencia aduanera, siendo esta última donde se manejan las operaciones esenciales de los procesos informáticos, aquí se manipulan los dos sistemas utilizados para la gestión de los distintos servicios que la empresa brinda, de esta área se alimentan las demás áreas, a través de la red interna que les brinda conexión a Internet e intercomunicación entre los sistemas. ***(Ver anexo 1 Organigrama Empresarial)***

Esta área cuenta con cinco empleados, quienes hacen uso de los equipos que se encuentran en el departamento, entre ellos se encuentra el jefe de operaciones quien está a encargo del control de uso de equipos y software.

6.2 JUSTIFICACIÓN

Con la ejecución de la auditoría a la empresa **ALMACENES AMERICANOS S.A** se evaluará la eficiencia del manejo de la información y los procesos de la empresa, lo cual requiere vigilar los procesos de recopilación, proceso y almacenamiento de la información dentro de la empresa, todo esto mediante el uso de la tecnología informática; en toda entidad este proceso es vital para el buen funcionamiento de la misma.

Tomando en cuenta la evaluación preliminar en la empresa se definió como área para la ejecución de auditoría, el área de agencia aduanera, que es donde se manejan las operaciones referentes a los procesos informáticos de la entidad.

Plan de Auditoría

Área auditar	Objetivos	Componente	Riesgo
Seguridad Lógica	Comprobar la existencia de normativas y procedimientos que resguarden el acceso a los datos y los permisos de acceso a personal autorizado.	1 - Acceso de los usuarios a sistemas, sistemas operativos y bases de datos.	Alto
		2 – Acceso de los usuarios a programas y archivos	Alto
		3 – Disposición de sistemas alternos en caso de fallos.	Alto
		4- Existencia de software de protección (antivirus, firewall.)	Alto
		5- Control de acceso de los usuarios a los servicios de Internet.	Medio

Seguridad Física	Evaluar la protección física de datos, programas, instalaciones, equipos, red y personal, de la empresa.	1 – Control de accesos de los usuarios a los equipos 2- Informes de accesos y visitas a las instalaciones. 3- Inventario de equipos y software. 4- Revisión de la red (Factor Ambiental, Físico y Humano) 5- Controles para la instalación y uso de dispositivos externos.	Alto Alto Medio Alto Alto
Respaldos y plan de contingencia	Verificar la existencia de respaldos de la información vital para el funcionamiento de la empresa, tanto físico como digital y que cumplan los requisitos adecuados.	1 - Respaldo de información critica 2- Plan de Continuidad 3- Plan de Contingencia 4-Plan de Mantenimiento de Hardware y Software	Alto Alto Alto Medio
Documentación de Hardware y Software.	Corroborar la existencia de documentación de todo lo adquirido por la empresa en materia de informática: manuales, facturas, contratos, además de documentación detallada de los sistemas que la empresa ha adquirido.	1. Disposición de manuales de usuario y de instalación de los sistemas. 2. Existencia de documentos de adquisición de equipos y software y contratos legal de proveedor de Internet y red (ISP). 3- Documentación de los sistemas utilizados para los servicios de la empresa.	Medio Alto Medio

6.3 ADECUACIÓN

Para la realización de esta auditoría se utilizarán diversas técnicas, por medio de las que se pretende recopilar la información necesaria para el desarrollo de la misma, y posteriormente el procesamiento de esta información brindará resultados para poder crear el informe final de la auditoría.

Entre estas técnicas están:

- Cuestionarios
- Entrevistas
- Observación
- Hoja de Procesamiento de Datos (Microsoft Word)

Las áreas a evaluar fueron analizadas mediante los procedimientos del Estándar de COBIT 4.1 el cual establece cuatro dominios. Debido a que la empresa Almacenes Americanos S.A está en proceso de desarrollo, el análisis de esta auditoría se basará en los siguientes dominios: **Adquisición e implementación (*Adquisition and implementation* (AI)), Entrega de servicios y soporte (*Delivery and support* (DS))**, así mismo de estos dos dominios no se usarán todos los subprocesos.

Guías de Auditorías

1. **Componente:** Acceso de los usuarios a sistemas, sistemas operativos y bases de datos.

Guía de Auditoría	
Dominio	**Prestación de Servicios y Soporte (DS)**
Proceso	**DS5: Garantizar la seguridad de sistemas.**
Objetivo de Control	Verificar la implementación de controles adecuados para los accesos de los usuarios.

No.	Procedimiento
1	Solicitar listado de usuarios que tienen acceso a los sistemas usados en los equipos
2	Corroborar si existe en cada equipo una cuenta de usuario en el sistema operativo para cada persona.
3	Verificar cuantos de los usuarios tiene login y password para ingresar a sistemas de gestión de aduanas y bases de datos.

2. **Componente:** Acceso de los usuarios a programas y archivos

Guía de Auditoría	
Dominio	**Prestación de Servicios y Soporte (DS)**
Proceso	**DS11: Administrar la información.**
Objetivo de Control	Verificar la aplicación de normas acceso de los usuarios a la modificación de archivos y manipulación de programas no propios del trabajo.
No.	**Procedimiento**
1	Mediante la observación identificar si los usuarios tienen acceso a la información almacenada en los equipos sin ninguna restricción.
2	Comprobar la existencia de medidas de restricción a los usuarios en el uso de archivos en las Pc's y así mismo de la manipulación y ejecución de programas ajenos al giro de la empresa.

3. **Componente:** Disposición de sistemas alternos en caso de fallos.

Guía de Auditoría	
Dominio	**Prestación de Servicios y Soporte (DS)**
Proceso	**DS4: Asegurar la continuidad de servicio.**
Objetivo de Control	Obtener un plan de contingencia (Si es que existe), en caso de que los sistemas principales fallaran.
No.	**Procedimiento**
1	Aplicar entrevista al encargado del área para conocer con que tipos de medidas cuentan, en caso de fallar

	uno de los sistemas.
2	Verificar la existencia de servidor alterno donde se almacene la información de clientes y gestiones diarias.

4. **Componente:** Existencia de software de protección (antivirus, firewall.)

Guía de Auditoría	
Dominio	**Prestación de Servicios y Soporte (DS)**
Proceso	**DS3: Administrar desempeño y capacidad.**
Objetivo de Control	Evaluar el tipo de software y licencias obtenidas, su desempeño y que sean acorde con el tipo de empresa.
No.	**Procedimiento**
1	Asegurar mediante la observación directa la existencia de software de protección en cada uno de los equipos.
2	Si existe el software verificar si se encuentra actualizado.

5. **Componente:** Control de acceso de los usuarios a los servicios de Internet.

Guía de Auditoría	
Dominio	**Prestación de Servicios y Soporte (DS)**
Proceso	**DS9: Administrar la configuración.**
Objetivo de Control	Revisar la implementación de controles para el uso de Internet.
No.	**Procedimiento**
1	Mediante entrevista al encargado del área, se pretende conocer si en la empresa hay un reglamento de uso del servicio de Internet, para los usuarios que acceden a los equipos.
2	En caso de que existan reglas para el uso, verificar mediante la observación si dichas reglas son las correctas para el óptimo uso de dicho servicio.

6. **Componente:** Control de accesos de los usuarios a los equipos

Guía de Auditoría	
Dominio	**Adquisición e Implementación (AI)**
Proceso	**AI3: Adquirir y mantener la arquitectura tecnológica.**
Objetivo de Control	Verificar los normativos de uso y acceso a los equipos.
No.	**Procedimiento**
1	Solicitar al encargado del área la lista de equipos que se usan, cuantos usuarios las usan y cuantas horas al día son usados estos equipos.

7. **Componente:** Informes de accesos y visitas a las instalaciones.

Guía de Auditoría	
Dominio	**Prestación de Servicios y Soporte (DS)**
Proceso	**DS12: Administrar las instalaciones.**
Objetivo de Control	Revisar el control de visitas a las instalaciones de informática (si existe).
No.	**Procedimiento**
1	Verificación de los sistemas y mecanismos de seguridad sobre el ingreso al área de operaciones mediante el proceso de observación directa.

8. **Componente:** Inventario de equipos y software

Guía de Auditoría	
Dominio	**Adquisición e Implementación (AI)**
Proceso	**AI3: Adquirir y mantener la arquitectura tecnológica.**
Objetivo de Control	Verificar si existe un inventario y corroborar la información del inventario con lo existente en la empresa.
No.	**Procedimiento**
1	Aplicar entrevista al encargado del área para conocer la existencia de inventario de equipos y software de respaldo en caso de que un equipo o programa falle.
2	En caso de que exista un inventario, verificar su existencia visitando el lugar de almacenamiento

	(bodega).

9. Componente: Revisión de la red (Factor Ambiental, Físico y Humano)

Guía de Auditoría	
Dominio	**Prestación de Servicios y Soporte (DS)**
Proceso	**Protección contra Factores Ambientales**
Objetivo de Control	Examinar la red física, la disposición de los equipos involucrados en esta y los usuarios que tiene contacto directo con ella.
No.	**Procedimiento**
1	Revisión mediante la observación directa de la instalación de la red y los equipos para ver si esta implementada de forma correcta.

10. Componente: Controles para la instalación y uso de dispositivos externos.

Guía de Auditoría	
Dominio	**Prestación de Servicios y Soporte (DS)**
Proceso	**DS9: Administrar la configuración.**
Objetivo de Control	Verificar si existe algún control para el uso de periféricos, las restricciones y su alcance.
No.	**Procedimiento**
1	Aplicar entrevista al encargado del área para comprobar si utilizan algún método en los equipos para restringir el acceso de dispositivos externos o bien si existe un reglamento para el uso de estos.

11. Componente: Respaldo de información crítica

Guía de Auditoría	
Dominio	**Prestación de Servicios y Soporte (DS)**
Proceso	**DS11: Administrar la información.**
Objetivo de Control	Verificar si existen respaldos en digital de la información vital de clientes y procesos importantes para la empresa.
No.	**Procedimiento**
1	Aplicar entrevista para conocer la existencia de respaldos de la información que usan en las gestiones diarias.
2	Si existen respaldos, verificar que tipo de respaldos son (digitales o físicos), si son digitales en que se almacenan (servidor alterno, discos, memorias u otros dispositivos externos).

12. Componente: Plan de Continuidad

Guía de Auditoría	
Dominio	**Prestación de Servicios y Soporte (DS)**
Proceso	**DS4: Asegurar la continuidad de servicio.**
Objetivo de Control	Comprobar la existencia de un plan de continuidad que se use en casos de desastre naturales o accidentes provocados por la naturaleza humana y que puedan detener totalmente las operaciones de la empresa.
No.	**Procedimiento**
1	Realizar entrevista a la encargada del área de mantenimiento para conocer si existe un plan de continuidad para estar listos ante un desastre natural o causado por la misma naturaleza humana y que pueda detener totalmente las operaciones.
2	Si este plan existe, solicitar detalles del mismo y de los pasos que se realizarían al momento de surgir un caso de estos que pueda detener las operaciones totales de las operaciones.

13. Componente: Plan de Contingencia

Guía de Auditoría	
Dominio	**Prestación de Servicios y Soporte (DS)**
Proceso	**DS4: Asegurar la continuidad de servicio.**
Objetivo de Control	Determinar si el plan de contingencia es lo suficientemente específico o detallado para poder continuar con las operaciones en la empresa y que además, dicho plan este acorde a lo que la empresa tiene en sus recursos (Si dicho plan existe).
No.	**Procedimiento**
1	Realizar entrevista a la encargada del área de mantenimiento, para conocer si existe un plan de contingencia al momento de un fallo.
2	Si existe el plan de contingencia, solicitar detalles de lo que se hace al momento de surgir un fallo que detenga parcialmente las actividades en la empresa.

14. Componente: Plan de Mantenimiento de Hardware y Software

Guía de Auditoría	
Dominio	**Adquisición e Implementación (AI)**
Proceso	**AI3: Adquirir y mantener la arquitectura tecnológica.**
Objetivo de Control	Revisar el plan de mantenimiento al software, si el periodo entre cada mantenimiento es el adecuado y si se hace el mantenimiento como se debe.
No.	**Procedimiento**
1	Comprobar la existencia de un plan de mantenimiento mediante entrevista a la encargada del área de mantenimiento.
2	Si este plan existe, conocer qué tipo de plan se tiene, y que detalles abarca el mismo para el mantenimiento de equipos y software en general de la empresa.

15. **Componente:** Disposición de manuales de usuario y de instalación de los Sistemas

Guía de Auditoría	
Dominio	**Adquisición e Implementación (AI)**
Proceso	**AI2: Adquirir y mantener software de aplicaciones.**
Objetivo de Control	Revisar los manuales de usuarios de los programas que están actualmente en uso y si estos manuales son los más actuales.
No.	**Procedimiento**
1	Solicitar los manuales de usuario de los sistemas que utilizan para la gestión de servicios que la empresa brinda.
2	Revisar los manuales para observar si son acordes a la versión del software que se está usando.

16. **Componente:** Existencia de documentos de adquisición de equipos y software y contratos legal de proveedor de Internet y red (ISP).

Guía de Auditoría	
Dominio	**Adquisición e Implementación (AI)**
Proceso	**AI3: Adquirir y mantener la arquitectura tecnológica.**
Objetivo de Control	Verificar las compras de equipos mediante documentos legales (facturas) y revisar el contrato de ISP (Internet service provider) para determinar lo estipulado en el contrato y verificar su correcto cumplimiento.
No.	**Procedimiento**
1	Solicitar al encargado del área de mantenimiento el registro o respaldo de facturas donde se demuestre la adquisición de equipos, software y servicio de Internet.

17. **Componente:** Documentación de los sistemas utilizados para los servicios de la empresa.

Guía de Auditoría	
Dominio	**Adquisición e Implementación (AI)**
Proceso	**AI2: Adquirir y mantener software de aplicaciones.**
Objetivo de Control	Determinar si existe la documentación de los sistemas adquiridos por la empresa y si esta posee todos los aspectos necesarios para poder dar mantenimiento al sistema en caso de ser necesario.
No.	**Procedimiento**
1	Mediante la técnica de la entrevista conocer si la empresa al adquirir un sistema obtiene la documentación (diagramas, arquitectura, código) de estos para poder ser modificados.

6.4 FORMALIZACIÓN

El proceso de realización de esta auditoría se acordó de manera formal con la alta dirección de la empresa Almacenes Americanos S.A, en una reunión donde se convino entre el gerente general y los auditores, el área a auditar, los límites y alcances de la misma, visitas y tiempo de evaluación. ***(Ver anexo 2, Carta de aprobación).***

6.5 DESARROLLO

Como resultado de aplicar las técnicas y herramientas en la auditoría de TI, se evidenciaron las siguientes situaciones:

Seguridad Lógica

Al evaluar los componentes descritos en seguridad lógica, se encontraron los siguientes hallazgos los que se describen a continuación:

Componentes:

1- Acceso de los usuarios a sistemas, sistemas operativos y bases de datos.

En el apartado de acceso de los usuarios a sistemas, sistemas operativos y bases de datos, se pudo evidenciar que los usuarios tienen libre acceso al sistema operativo de las computadoras a excepción de la computadora del encargado, esta tiene contraseña para acceder al sistema operativo windows y las demás no, aquí se evidenció que ninguna PC tiene contraseña de arranque y basta con encenderla para cargar el sistema.

En cuanto al acceso de los usuarios a sistemas se encontró que en la empresa se emplean dos sistemas de información, los que requieren contraseña para poder acceder. El primero es el sistema proporcionado por la Dirección General de Aduana Nicaragüense, que es el SIDUNEA WORLD, este es un sistema online, el cual requiere obligatoriamente de conexión a Internet para su uso, este sistema necesita de usuario y contraseña para el acceso, los permisos de acceso son proporcionados por la aduana a agentes aduaneros inscritos y con permiso legal otorgado por la misma aduana.

En la empresa existen dos empleados que tienen contraseña propia para el acceso a este sistema, los demás no tienen usuario ni contraseña y en caso de que estos utilizaran el sistema uno de los dos usuarios que cuentan con acceso ingresan al sistema para que ellos lo utilicen, sin darles a ellos la contraseña y el usuario, cabe destacar que como este es un sistema que no es de la empresa, solo se evaluó el resguardo de la contraseña de acceso, así como la cantidad de usuarios que lo usan y las actividades que se realizan en él, en lo cual se evidencio que este sistema es usado por las cinco personas que laboran en el área, solamente dos de

estas poseen acceso al sistema; este sistema se usa para poder registrar hacia la Dirección General de Aduanas las declaraciones que se ingresan en el sistema TCO que es el que la empresa utiliza para estas gestiones; las contraseñas son manejadas exclusivamente por los agentes aduaneros en el caso del SIDUNEA, para el TCO cada usuario tiene su contraseña y solamente el jefe de operaciones tiene la contraseña y usuario de administrador en el TCO.

El segundo sistema empleado es el TCO este es un sistema de gestión de operaciones aduaneras, este sistema fue comprado a terceros, y es administrado por el encargado de la división de operaciones. Para el acceso a este sistema se necesita usuario y contraseña, según la información obtenida cada empleado del área tiene su usuario y contraseña para acceder al sistema, es decir que son cinco los usuarios del sistema.

La aplicación correcta de los controles de acceso a los sistemas en una empresa es vital porque aumenta la seguridad e integridad de la información, se disminuye el riesgo de fraude y de filtración o alteración de la información, limitando enormemente la cantidad de usuarios y administradores de los puntos críticos de TI y mantener el control del flujo de la información.

2- Acceso de los usuarios a programas y archivos

En este aspecto se obtuvo información mediante observación y entrevistas, por lo que se pudo evidenciar que las políticas de la empresa establecen que los trabajadores que utilizan las computadoras únicamente poseen la potestad de hacer uso de los sistemas TCO, Sidunea World, la paquetería de herramientas ofimáticas Office y Outlook para el uso del correo

institucional. Tienen prohibido el uso de programas ajenos a la misión del negocio.

Estas prohibiciones son informadas a los empleados de forma verbal, por medio de la encargada de administración y del responsable del área de operaciones, además de mantener en lugares visible rótulos con el reglamento impreso.

Este control es sumamente importante ya que el empleador deja en claro a los empleados cuales son responsabilidades, derechos y restricciones en la empresa, este control mal empleado podría causar serios daños en los equipos, software y demás elementos relacionados con TI.

3- Disposición de sistemas alternos en caso de fallos.

En cuanto a la disposición de sistemas alternos en caso de fallos, se determinó que la empresa no cuenta con sistema alterno, tampoco tienen plan de respaldo en caso de fallas en el sistema principal. Cuando existen fallos en alguno de los sistemas de gestión aduanera recurren al proveedor de Internet o al técnico de mantenimiento, pero esto se hace solo si existe un fallo.

La utilización de sistemas alternos es vital para la prevención de caídas de servicio por largos períodos de tiempo, si una empresa no tiene sistemas alternos para funcionar en caso de que el sistema principal presente algún inconveniente, la empresa podría detener parcial o totalmente sus operaciones, lo que se traduce en pérdidas, las que pueden ser cuantiosas para la empresa.

4- Existencia de software de protección (antivirus, firewall.)

Al revisar la existencia de software de protección se encontró que el antivirus utilizado en todos los equipos de la empresa es el Eset Nod 32 Versión 5.2.9 con licencia por un año, la licencia fue proporcionada por la empresa subcontratada para el mantenimiento de las computadoras en la empresa, también el firewall en uso es el firewall nativo del sistema operativo Windows XP y en el caso de la computadora que actúa como servidor Windows 7.

La existencia de software de protección actualizada es indispensable para la integridad y manejo de la información de la empresa, informáticamente hablando es importante contar con software que sea capaz de proteger la información digital de la empresa, este software se encarga de que la información no sea sustraída por terceros o dañada por algún software malicioso.

5- Control de Acceso de los usuarios a los servicios de Internet.

Cuando se revisó el control de acceso de los usuarios a los servicios de Internet se evidenció que solo las computadoras de los encargados de áreas tienen acceso a Internet, las demás computadoras solo están conectadas a la red de la empresa, pueden verse entre ellas, pero no tienen acceso a Internet.

El acceso a Internet se restringe mediante la configuración de cada PC, en el centro de redes de Windows se cambia las configuraciones para decidir qué dirección IP tiene acceso y cual no, esto lo aplica la empresa de soporte Datatex, mediante indicaciones de la alta gerencia de la empresa, quien decide los permisos de acceso a Internet, para lo cual se toma en

cuenta el cargo y función de los empleados, siendo así los jefes de departamentos los únicos con acceso a Internet, el resto de equipo solo tiene acceso a la red local.

Mantener el control de los permisos de acceso a internet, disminuye los riesgos que puedan afectar la integridad de la información, además que garantiza que la comunicación a través de dicho enlace sea utilizado para los fines y objetivos de la empresa.

Seguridad Física

Al evaluar los componentes descritos en seguridad física, se encontraron los siguientes hallazgos, los que se describen a continuación:

Componentes:

6- Control de accesos de los usuarios a los equipos.

En el control de accesos de los usuarios a los equipos informáticos, se evidenció que solo los usuarios que trabajan en el área de operaciones tienen acceso a los equipos, exceptuando al personal que hace mantenimiento a los equipos, que es personal externo a la empresa.

El uso de controles para el acceso a equipos, evita la exposición tanto de la información como de los equipos a riesgos provocados por accidentes o acciones mal intencionadas. Dando mayores garantías de la disponibilidad e integridad de la información.

7- Informes de accesos y visitas a las instalaciones.

En los informes de accesos y visitas a las instalaciones, se encontró que la empresa no lleva registro de control de ingreso al edificio, las notificaciones para el ingreso se hacen de manera verbal y no hay ningún soporte.

Además al ingresar a la empresa no se solicita ninguna identificación únicamente preguntan hacia donde se dirige y a quien busca, en el caso de las personas que llegan a la empresa a realizar mantenimiento a las PC llegan debidamente identificados a la empresa y aunque no existe un plan de mantenimiento, la encargada del área de administración lleva un control de lo que los técnicos realizan en cada visita, así mismo se lleva un registro de cambio de equipos y piezas, así como del Hardware descartado.

Mantener un control de visitas y control de presencia de personal externo en una organización, es importante porque de esta manera se mantiene un ambiente seguro para el personal que labora en la empresa; así también se protegen los activos, la continuidad operacional y la propiedad intelectual.

8- Inventario de equipos y software

En el inventario de equipos y software, se evidenció que la empresa cuenta con un almacén donde se encuentran las computadoras y equipos electrónicos que ya no funcionan, tienen un inventario manual de estos equipos con un diagnóstico donde se detallan piezas dañadas y piezas en funcionamiento, entre estos están: Pc's, impresoras, sistemas operativos en uso, etc.

Existe una computadora utilizada por el jefe de operaciones que su plataforma es Windows 7, esta actúa como servidor para el sistema aduanero TCO, este tiene un arquitectura cliente-servidor, las demás máquinas de esta área funcionan como cliente.

Es importante tener inventario de hardware y software al día, así la empresa tiene control directo sobre sus activos de TI y sabe exactamente

con lo que cuenta, lo que almacena y lo que tiene que adquirir en caso de alguna modificación en TI.

9- Revisión de la red (factor ambiental, físico y humano)

La red está compuesta por cableado plano en su mayoría, el ISP que en este caso es Datatex, les proporciona un nodo de conexión satelital, con una antena ubicada en la parte este de la empresa, la cual se conecta a un router ubicado en el área de operaciones mediante un cable UTP categoría 5e, de aquí la red se divide en cuatro subredes que son, operaciones, administración, bodega y gerencia.

La auditoría se llevó a cabo en el edificio donde se encuentran las áreas de operaciones y administración; en el área de operaciones se encuentra el router de la empresa, ubicado en una repisa, fuera del alcance de los empleados, cercano al router se encuentra un tomacorriente, la conexión de la antena hacia el router es por el exterior; en esta conexión no existe ningún dispositivo que logre fijar y mantener la conexión estable, esto quiere decir que el medio por el que viajan los datos (Cable UTP cat. 5e) no está asegurado por ninguno de sus lados. En la red LAN las conexiones (cables UTP cat. 5e) van en canaletas y por encima del cielo falso de la oficina hasta llegar a la cercanía de las máquinas, donde se conecta directamente al puerto de red de las PC, ninguno posee un toma de datos, se pudo observar que el único estándar para cableado estructurado que se cumple en el proceso de transmisión de datos es EIA/TIA 569. También se observó que los equipos de comunicación no cuentan con las condiciones ambientales establecidas por los estándares.

Cabe destacar que en lo que respecta a la seguridad del área mediante cámaras de seguridad y extintores, únicamente existe un extintor por área y

no hay existencia de cámaras de seguridad para la protección de sus activos, esto es una debilidad que muestran en este aspecto.

La seguridad de la red es un factor importantes que cualquier administrador o instalador de red debe considerar, ya que se debe garantizar la máxima seguridad de los datos que serán transmitidos a través de ella, así como la capacidad de transmisión que la empresa requiera, así que se deber tomar en cuenta todos estos aspectos al momento de una revisión, la cual debe hacerse cada cierto período de tiempo según la empresa lo considere necesario.

10-Controles para la instalación y uso de dispositivos externos

En lo que se refiere a los controles para la instalación y uso de dispositivos externos, se descubrió que la empresa tiene una fuerte política de restricciones de uso en lo que concierne a sus equipos de informática, los puertos USB de las computadoras están bloqueados, no está permitido el uso de ningún dispositivo externo y si un trabajador tratara de utilizarlos, este sería sancionado por la empresa.

Los controles para instalación de hardware y software evitan que empleados descontentos cometan fraude, llevándose información confidencial o que instale software innecesario.

Respaldos y planes de contingencia

Al evaluar los componentes descritos en respaldos y plan de contingencia, se encontraron los siguientes hallazgos los que se describen a continuación:

Componentes:

11-Respaldo de información crítica

En los respaldos de información crítica, se encontró que se maneja un respaldo de la información de los clientes únicamente en físico, y están resguardados en las instalaciones de la empresa, no hay respaldo digitalizado de la información, la empresa no posee redundancia en este apartado.

El respaldo de la información crítica, es lo más importante de TI en una empresa, se necesita salvaguardar la información que la empresa posea, las empresas deben ser cautelosas con su información, para asegurar que sus operaciones no sean afectadas por accidentes o desastres. La existencia de respaldos actualizados puede ser la solución para una pronta recuperación de sus actividades comerciales.

12-Plan de Continuidad

En cuanto al plan de continuidad, la empresa no está preparada en caso de que algún desastre natural llegara a interrumpir sus acciones, la empresa no tiene contemplado que algo así pudiera interrumpir sus operaciones. Si hay algún fallo general, la empresa quedaría deshabilitada, no existe un plan de continuidad.

El plan de continuidad es necesario que sea funcional en una entidad ya que si ocurriera algún contratiempo de fuerza mayor como un desastre natural, la empresa no quedaría fuera de operaciones, por lo tanto no tendría pérdidas.

13-Plan de Contingencia

En casos de fallos de los sistemas de información el proceso que se lleva a cabo en la empresa es: Si falla el acceso al SIDUNEA WORLD a causa de la pérdida de conectividad a Internet, la empresa tiene convenios con algunas empresas aduaneras a nivel nacional para poder continuar las operaciones de la empresa, en el caso de que el TCO llegara a fallar, las gestiones que se realizan en este sistema se realizarían manualmente.

El plan de contingencia es importante ya que si ocurriera algún fallo que pueda interrumpir parcialmente las actividades de la empresa, la misma no quedaría fuera de operaciones, por lo tanto no tendría perdidas.

14-Plan de Mantenimiento de Hardware y Software

En el plan de mantenimiento se encontró que la empresa tiene un contrato de soporte que puede variar según la estación del año, en verano se realiza cada 3 meses y en invierno cada 6 meses, lo que indica que el mantenimiento se realiza 3 veces en el año, este mantenimiento se podría considerar como un mantenimiento preventivo; el mantenimiento correctivo solo se hace cuando alguna computadora presenta problemas; cabe destacar que este mantenimiento lo hace una empresa subcontratada como servicios profesionales, el mantenimiento del software solo es correctivo, solo se hace cuando el software funciona mal, este mantenimiento es realizado por personal externo que está contratado por la empresa para realizar mantenimiento del software de facturación y el de contabilidad. La empresa está clara que el mantenimiento preventivo es esencial para el buen funcionamiento de los equipos informáticos.

Es importante conocer lo que los técnicos encargados de los mantenimientos les hacen a las PC, para esto se necesita tener un plan de

mantenimiento, así si se realiza algún cambio de técnico en la empresa, tanto el técnico nuevo como los directivos de la empresa estarán al tanto de lo que hacía el técnico anterior y no se tendrán futuros inconvenientes.

Documentación de Hardware y Software

Al evaluar los componentes descritos en la documentación de Hardware y Software, se encontraron los siguientes hallazgos los que se describen a continuación:

Componentes:

15-Disposición de manuales de usuario y de instalación de los sistemas

En la disposición de manuales de usuario y de instalación de los sistemas, se encontró que en los dos sistemas que actualmente están en uso, que son SIDUNEA WORLD y TCO, existe documentación. En el caso del SIDUNEA WORLD que es un sistema gratuito que la aduana nicaragüense proporciona, toda la documentación correspondiente a dicho sistema se encuentra en la página gubernamental de la aduana nicaragüense, en cuanto al sistema TCO de gestiones aduaneras, la empresa mantiene documentación en cuanto al manual de usuario, pero no mantiene ni los instaladores, ni el manual de instalación, esto se debe a que la adquisición del software no ha sido concretada y por el momento el proveedor de dicho software ha llegado a la empresa únicamente a instalar el software y a dejar el manual de usuario.

Es importante para el administrador del sistemas como para los usuarios tener documentación de los sistemas de información, porque así es más fácil capacitar a los usuarios en el uso correcto y eficiente del software con ayuda del manual de usuario, al igual que si se requiere de instalarlo nuevamente se debe contar con un manual para que la instalación termine con éxito.

16-Existencia de documentos de adquisición de equipos y software y contratos legal de proveedor de Internet y red (ISP).

Al comprobar la existencia de documentos de adquisición de equipos y software y contratos legales de ISP, se encontró que la empresa cuenta con la documentación, resguardados por el área contable, en cuanto al contrato de ISP no fue mostrado solo se sabe que se contrató el ancho de banda y que el proveedor es Datatex. En cuanto al proveedor de equipos informáticos se conoció que la empresa trabaja siempre con la empresa COMTECH.

La implementación de este control en la empresa es importante, porque es necesario que la empresa posea los documentos legales de adquisición de equipos, ya que si se presenta algún defecto en algún equipo nuevo se debe tener la cobertura de la garantía, así como para posibles auditorías o investigaciones, con lo cual se pueda corroborar la adquisición legal de los equipos.

17-Documentación de los sistemas utilizados para los servicios de la empresa

En cuanto a la documentación de los sistemas utilizados para los servicios de la empresa, se evidenció que la empresa no posee documentación, esto se debe a que los sistemas utilizados por la empresa, son sistemas enlatados, es decir sistemas comprados y desarrollados por terceros, cabe destacar que la compra del sistema TCO aún no es total, solo se ha comprado la utilización del software, no se ha comprado los derechos de modificación del código del mismo, por lo tanto la empresa no posee la documentación, diagramas y jerarquías del software.

La falta de documentación de los sistemas en una empresa se podría traducir como un manejo ineficiente de los sistemas, por lo tanto no se podría explotar a toda su capacidad el software.

7. Informe de Auditoría

7.1 OBJETIVO

Realizar valoración de los resultados obtenidos en el proceso de auditoría en seguridad, aplicado a la empresa Almacenes Americanos S.A.

7.2 ALCANCE

La realización de esta auditoría se llevó a cabo en la empresa Almacenes Americanos S.A, en un período de 60 días, en el cual se abordó la evaluación del área de operaciones de la empresa, que como se explicó anteriormente es el área donde se llevan a cabo los procesos informáticos de la entidad. Se evaluó seguridad física, seguridad lógica, respaldos de datos, planes de mantenimiento, contingencia y continuidad, así como la documentación general y específica sobre equipos, sistemas y software utilizado en la empresa.

Debido al acuerdo entre la gerencia de la empresa y los auditores, no se evaluó mediante pruebas sustantivas la seguridad de la red y los sistemas de información, ya que para ellos, esto podría dar lugar a que los auditores tuvieran acceso a información valiosa y confidencial de la empresa; por la razón antes mencionada solamente se verificó el cumplimiento de las normativas internacionales en seguridad, las que se comprobaron generalmente utilizando la información obtenida en las entrevistas, cuestionarios y mediante la observación.

7.3 SITUACIÓN OBSERVADA (HALLAZGOS) Y RECOMENDACIONES

Área: Seguridad Lógica

Nombre del Componente:	Acceso de los usuarios a sistemas, sistemas operativos y bases de datos.
Hallazgo:	No existe validación alguna para acceder al Sistema Operativo o a los archivos de las Pc's, a excepción de la PC del encargado de Operaciones, la empresa no cuenta con base de datos de ningún tipo.
Recomendación:	Se recomienda poner contraseñas en el inicio del sistema operativo y en el BIOS de cada PC, actualmente no se cuenta con una base de datos en la empresa, pero al implementarse lo recomendable es tener un administrador que sea el responsable de la contraseña de la BD.

Nombre del Componente:	Acceso de los usuarios a programas y archivos.
Hallazgo:	No existe ninguna validación de usuario en las PC, se puede tener acceso a cualquier archivo sin necesidad de usuario y contraseña, también cada PC es usada por más de un usuario.
Recomendación:	Se recomienda que los archivos estén cifrados para los usuarios que no tienen acceso a ellos, poniendo contraseña a carpetas en Pc's donde se maneje información delicada de la empresa.

Nombre del Componente:	Disposición de sistemas alternos en caso de fallos.
Hallazgo:	Falta de un servidor para el sistema TCO, el que está instalado en una PC con mayores requerimientos que las demás Pc's para poder funcionar como servidor.
Recomendación:	Se recomienda mantener un sistema en caso de fallos, un sistema menos potente pero que trabaje similar al TCO ya que ese es el sistema de aforo.

Área: Seguridad Física

Nombre del Componente:	Control de accesos de los usuarios a los equipos.
Hallazgo:	Solo los trabajadores del área de operaciones tienen acceso a los equipos de esta misma área.
Recomendación:	Se recomienda mantener una lista para el control de quien acceda a los equipos, así como tener una lista de los usuarios autorizados de los equipos y el horario en el que estos tienen derecho a ocupar los equipos, en una mejor instancia mantener un control electrónico por medio de tarjetas que identifiquen a los empleados según cargo.

Nombre del Componente:	Informes de accesos y visitas a las instalaciones.
Hallazgo:	No existe un control tangible de quienes entran o salen del área de operaciones, que es donde se encuentran los procesos más críticos de la empresa, para poder entrar se necesita la autorización del gerente, pero el control es verbal, no se lleva registro o documentación de visitas, para acceder al centro.
Recomendación:	Se recomienda establecer un horario de visita a las instalaciones y mantener un control de parte del encargado para poder ingresar, así como revisión de

	las personas que quieran ingresar a las instalaciones, además del permiso del gerente, para que exista constancia física o digital de que personas entraron a las instalaciones y a qué hora.

Nombre del Componente:	Inventario de equipos y software
Hallazgo:	Falta de automatización de algunos procesos que podrían ser más rápidos y menos tediosos, como es el inventario de los equipos dados de baja y puestos en bodega, el control de estos se lleva a mano.
Recomendación:	Se recomienda que el inventario se lleve de manera digitalizada, actualmente se lleva de manera física, pero es más eficiente de manera digital, alojando todo el inventario en una pequeña BD en un servidor.

Nombre del Componente:	Revisión de la red (Factor ambiental, Físico y humano).
Hallazgo:	El cableado proporcionado por el ISP (Internet Service Provider) que en este caso es Datatex, que conforma la red entera posee muy poca estandarización, el cableado instalado es meramente plano compuesto casi en su totalidad por cable UTP cat. 5e.
Recomendación:	Se recomienda mejorar las condiciones del cable de red que conecta la antena satelital al router de la empresa, para que este no este suelto, se pretende que esto se realice por medio de cintas de seguridad, amarradas en la antena, también se recomienda cumplir con la norma de la ISO y mantener las conexiones y equipos de telecomunicaciones a más

	de 10 metros de distancia.

Área: Respaldos y Planes de Contingencia

Nombre del Componente:	Respaldo de Información crítica.
Hallazgo:	Falta de digitalización de sus documentos, existe respaldo solo en físico, por lo tanto, no están preparados para ninguna eventualidad.
Recomendación:	Se recomienda comprar un servidor para poder almacenar los datos críticos en una base de datos.

Nombre del Componente:	Plan de continuidad.
Hallazgo:	Carecen de planes de reanudación de operaciones y planes en caso de desastres. Como se puede observar esto es un punto de debilidad en la empresa porque mediante estos se asegura que la empresa seguirá ofreciendo su servicio sin importar las condiciones.
Recomendación:	Se recomienda crear planes en caso de fallas parciales o totales de los sistemas de la empresa, para poder garantizar el seguimiento de operaciones para la misma. Además se recomienda contar con un plan de contingencia para poder recuperar y reanudar sus operaciones sin importar los acontecimientos.

Nombre del Componente:	Plan de Contingencia.
Hallazgo:	Carecen de planes de reanudación de operaciones y planes en caso de fallo total o parcial de sus sistemas Como se puede observar esto es un punto de

	debilidad en la empresa porque mediante estos se asegura que la empresa seguirá ofreciendo su servicio sin importar las condiciones.
Recomendación:	Se recomienda tener un plan de mantenimiento, para mantener informado al personal encargado las tareas a realizar, para que tanto directivos como demás gente involucrada en el mantenimiento esté enterada de lo que se hace y se cercioren de que el mantenimiento se realiza de manera adecuada y a como establece el plan para mantener control y orden.

Nombre del Componente:	Plan de Mantenimiento de Hardware y Software.
Hallazgo:	No se cuenta con un plan sólido de mantenimiento de hardware, se realiza 3 veces durante el año, de dos maneras preventivas y correctivas y el de software solo de manera correctiva, ambos realizados por terceros.
Recomendación:	Se recomienda la creación formal de un plan de mantenimiento y establecer los procedimientos de las tareas a realizar. Planes y procedimientos que deberán ser dados a conocer a todos los empleados, a cerca del correcto uso de los equipos informáticos, para optimizar los servicios de mantenimiento contratados por la empresa, además se recomienda llevar un registro detallado de las actividades que se realizan en cada tarea.

Área: Documentación de Hardware y Software

Nombre del Componente:	Documentación de los sistemas utilizados para los servicios utilizados para los servicios de la empresa.
Hallazgo:	No existe ninguna documentación en cuanto a diagramas y/o esquemas de los servicios utilizados por la empresa, de red o de software.
Recomendación:	Se recomienda a la empresa diagramar y esquematizar el software que posea, así mismo realizarlo con su red en uso.

7.4 **CONCLUSIONES**

Como resultado de la auditoría podemos manifestar que se ha cumplido con evaluar cada uno de los controles plasmados en el plan de auditoría, la auditoría revelo que controles implementados no se aplicaron en forma adecuados. Evaluando el área importante de la empresa como es el de operaciones, se evidencia que falta un manejo más amplio y exhaustivo de las TIC, así mismo sucede con algunas áreas de la empresa que no está automatizadas, la auditoría realizada debe tomarse como una guía para llevar en perfecta armonía las TIC con la misión del negocio, siguiendo con los resultados de auditoria consideramos que la empresa no tiene implementado los controles necesarios para el resguardo de la información, de igual forma muchos de los procesos de la empresa deberían ser automatizados como: el proceso de inventario, el proceso contable.

La empresa actualmente se encuentra en vías de desarrollo, pero poseen planes futuros para aumentar y mejorar su capacidad en materia de TI, se tienen controles en algunas áreas estrictos y en otras áreas no tan estrictos, por el momento la empresa se encuentra en dirección junto a TI para satisfacer las necesidades del cliente, la automatización no es completa y la adquisiciones para la mejora de los servicios de TI está pensada muy en el futuro.

Adicionalmente se sugiere a la empresa, realizar las tareas de actualización y mantenimiento necesarias, con énfasis en el área de operaciones, las que son esenciales para el buen funcionamiento de la empresa y para el cumplimiento de los objetivos establecidos. Cabe destacar que es de gran importancia que la empresa contrate personal capacitado para el desarrollo de sus sistemas de información, es decir, que no adquieran sistemas enlatados, porque un sistema desarrollado internamente sería único y acorde a las necesidades de la organización.

8. Conclusión

Al evaluar las condiciones de la empresa, se determinó que la empresa Almacenes Americanos S.A, es perfectamente auditable en materia de informática. Una vez determinada la viabilidad de la auditoría informática, se acordó con la alta gerencia aplicar la evaluación en el área de operaciones, debido a que en esta se manejan los procesos informáticos de la entidad; seguidamente se procedió a crear un plan de auditoría para evaluar los controles que se plantearon, enfocados al área de operaciones.

El plan de auditoría ejecutado, tiene sus fundamentos en los dominios de COBIT 4.1; del cual se emplearon únicamente dos de los dominios, ya que son los que se adaptaban a los controles establecidos para la evaluación, estos dominios son: Adquisición e implementación (Adquisition and implementation (AI)), Entrega de servicios y soporte (Delivery and support (DS)), así mismo para el desarrollo de la auditoría se hizo uso de la metodología MAI (metodología de auditorías informática) la cual plantea que toda auditoría informática debe realizarse en las siguientes fases: Preliminar, Justificación, Adecuación, Formalización, Desarrollo. De esta forma se procedió a revisar los controles internos y la seguridad del área de operaciones, una vez finalizada la evaluación se realizó un informe con los hallazgos de cada punto auditado, y finalmente en base al informe de los hallazgos, se procedió a sugerir las recomendaciones finales para presentar el informe completo.

9. Recomendaciones

- Como primera recomendación de este trabajo de tesis. Se sugiere tomar en cuenta las recomendaciones planteadas en los diferentes controles auditados en el transcurso de la auditoría y que están debidamente documentados en este trabajo. Recomendaciones que deberán ser implementadas por los jefes de las áreas de operaciones y administración, en conjunto con la alta gerencia.

- Para los casos en que se comparte el equipo de cómputo. Se recomienda crear sesiones individuales para cada empleado, haciendo uso de usuarios y contraseñas para mantener la confidencialidad y seguridad de la información. Esta recomendación deberá ser ejecutada por el responsable de informática.

- El jefe del área de operaciones, deberá restringir y monitorear el uso de software en cada PC, para lo que se recomienda emplear un software de monitoreo.

- El jefe de operaciones, deberá estar pendiente de aplicar las actualizaciones en tiempo y forma a cada software instalado, ya sea de procesamiento o de protección de datos.

- La alta gerencia de la empresa, deberá mantener en un servidor alterno con el sistema TCO, lo que permitirá en caso de fallo del servidor principal, la continuidad de las operaciones de la empresa.

- Se recomienda a la alta gerencia y encargados de área, mantener un estricto control documentado de quienes entran y salen de las instalaciones.

- Se recomienda desarrollar un Sistema de Base de Datos donde se pueda llevar el inventario de todo lo que la empresa posee; sistema que deberá estar bajo la responsabilidad del área de administración, para el registro del inventario y su mantenimiento.

- Se recomienda a la alta gerencia rediseñar e implementar una restructuración de la red LAN de la empresa, aplicando las normas para cableado estructurado. Se deberá implementar un MDF, para garantizar la seguridad de los equipos de telecomunicaciones.

- Se recomienda a la alta gerencia, desarrollar planes de contingencia y de continuidad.

- Los responsables de las áreas de operaciones y administración deberá solicitar al equipo de mantenimientos realizar un plan de mantenimiento para las PC de la empresa.

10. Bibliografía

- Auditoría y Control de Sistemas e Informática. (2008). Consultado el 26 de septiembre de 2012 de *http://perso.wanadoo.es/idmb/a_ing/temas/auditoría_informatica.htm*

- Bautista, J. (2007). *Auditoría en Informática, [En Línea],* Disponible en http://fcasua.contad.unam.mx/apuntes/interiores/docs/98/8/audi_infor.pdf. [Consulta 27-09-2012]

- Cervantes, R. (2011). *Administración de centro de cómputo: Seguridad Lógica.*

- Coronel, K. (2012). *Auditoría Informática orientada a los procesos críticos de crédito generados en la Cooperativa de Ahorro Y Crédito "Fortuna" aplicando el marco de trabajo COBIT.* Ecuador.

- Del Peso Navarro, E. (2008). *Auditoría de Tecnologías y Sistemas de Información.* 2012 RA-MA, S.A. Editorial.

- Echenique, J. (2001).*Auditoría en Informática 2da Edición.* Mc Graw Hill. México.

- *Estrategia y Planificación TIC: Diagnóstico de la función informática.* (2008). Recuperado de www.ibermática.com

- Galvez, G. (2011). *Enfoque metodológico de la auditoría a las tecnologías de la información y las comunicaciones.* Comité de Investigaciones Técnico Científicos (CITEC).

- García, J. (2001). *Auditoría en Informática.* México: Mc Graw Hill/Interamericana Editores S.A de C.V.

- Hernández, H. (2004).*Auditoría en Informática Un enfoque metodológico y práctico.* Compañia Editorial Continental S.A de C.V. México.

- ISACA.org. (2007). *COBIT® 4.1. Estados Unidos de América.* IT Governance Institute

- ISACA.org. (2007). *COBIT Control Practices (Guidance to Achieve Control Objectives for Successful IT Governance).* United States of America: IT Governance Institute.

- Iturmendi, J.J. (1994). *Auditoría Informática en la empresa.* Madrid: Thompson Paraninfo S.A

- Cashin, J. *Neuwirth, P. Levy, J. Mainou Abad, J. (1999). Enciclopedia de la auditoría, 1ª Edición,* Editorial Oceano, Pág 40.

- *Normas para la seguridad del software. (2007). [En Línea].* Documento Disponible en:icicm.com/files/NormasCalSegSoftware.doc [Consulta 30-09-2012]

- Piatinni, M. (2001). *Auditoría informática: Un enfoque práctico.* Alfaomega, 2001 Editorial.

- Piatinni, M. (2007). *Gobierno de las Tecnologías y Sistemas de Información.* Madrid: RA-MA editorial.

- República, C. G. (Julio, 2009). *Gubernamental, Manual de Auditoría.* Managua: Proyecto BID/CGR.

- *Soluciones en Ingeniería de Gestión, (2009),* [En Línea], Disponible en: http://es.scribd.com/doc/40028764/normas-calidad [Consulta 28-09-2012]

- Sierra, E., García-Martínez, R., Hossian, A., Britos, P. and Balbuena, E. 2006. *Providing Intelligent User-Adapted Control Strategies in Building Environments. Research in Computing Science Journal,* 19: 235-241.

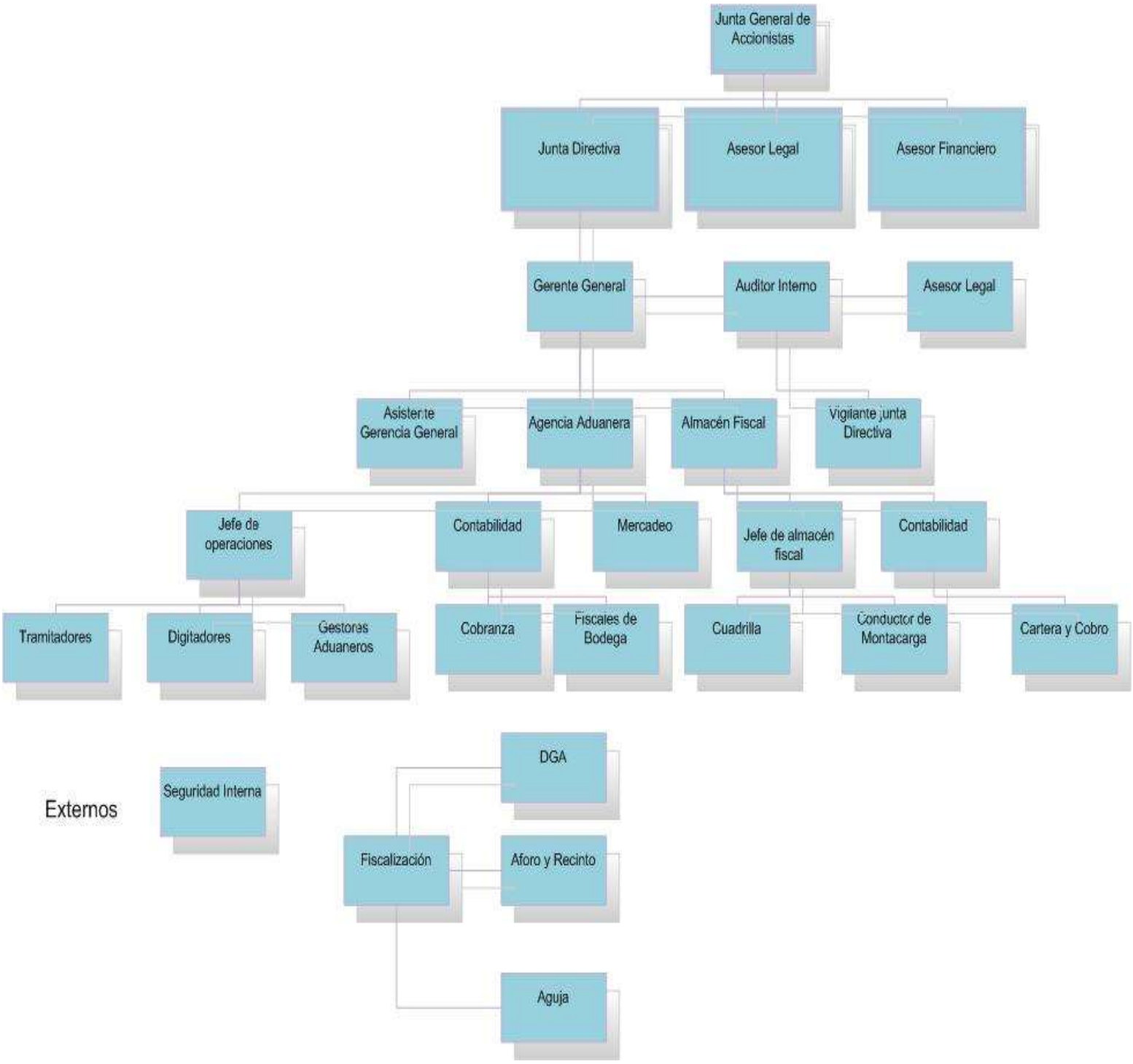
- Thomas, A, Douglas, I. (2001). *Auditoría informática.* Paraninfo Editorial.

- Vilches, R. (2008). *Apuntes del estudiante de auditoría,* [En Línea], Disponibleen:http://www.gestiopolis.com/recursos4/docs/fin/apuestaud.htm [Consulta 28-09-2012]

- Zamarrita, E. (2002). *Sistemas Tutoriales de Auditoría.* Prentice Hall.

ANEXOS

1. ORGANIGRAMA EMPRESARIAL



2. CARTA DE APROBACIÓN

ALMACENES AMERICANOS, S.A.
Despacho del gerente general

Managua, 06 de Julio del 2012.

Msc
Carlos Leal Saballos
Coordinador Ingeniería en Sistemas y Tecnología de Información
UNIVERSIDAD CENTROAMERCIANA (UCA)
Su oficina.

Msc. Leal:

Acusamos recibido de su carta, con fecha de hoy 06 de Julio del año dos mil doce y con relación a su contenido damos nuestra anuencia para colaborar en los Estudios Monográficos de Hazell Sevilla Mercado y Cristhian Narváez Morazán, estudiantes del quinto año de la carrera Ingeniería en Sistemas y Tecnología de Información.

Sin más sobre el particular, me suscribo

Muy Atentamente,

Víctor M. Hernández Méndez
Gerente General

ALMACENES AMERICANOS S.A. GERENTE GENERAL ALMACENA Managua, Nic.

C/c: Archivo

3. CUESTIONARIO GERENTE GENERAL

NOMBRE DE LA INSTITUCIÓN:
_____
DIRECCIÓN: _____
AUDITORÍA A:
_____
FECHA DE INICIO: _____ FECHA DE FINALIZACIÓN: _____
NOMBRE DEL AUDITOR:
_____

Objetivo: Recolectar información general y específica sobre los diferentes aspectos sobre como se maneja TI en la empresa a auditar.

- ¿Conoce lo que es TI?

- ¿Cuánto invierten en TI al año?

- ¿Qué tan importante ha sido esa inversión? ¿Han sacado provecho de la inversión?

- ¿Tienen planes futuros para TI?

- ¿Tienen algún manual interno para el manejo de TI (uso de PC, de software, hardware)?

- ¿Piden reportes del uso de TI? ¿Que tan seguido?

- ¿Cómo controlan las TI en la empresa?

4. CUESTIONARIO JEFE DE ÁREA DE OPERACIONES

NOMBRE DE LA INSTITUCIÓN:
_____
DIRECCIÓN: _____
AUDITORÍA A:
_____
FECHA DE INICIO: _____ FECHA DE FINALIZACIÓN: _____
NOMBRE DEL AUDITOR:
_____

Objetivo: Obtener información critica de los procesos informáticos que se manejan en el área de operaciones.

- ¿Tienen respaldo de la información de sus clientes? ¿En qué manejan la información de sus clientes?

- ¿Tienen algún plan para restablecer las operaciones si algo llegara a fallar?

- ¿Conoce lo qué es software libre? (Si usan software libre) ¿Cuál usan?

- ¿Qué tipo de software usan (libre o con licencia)? (Si usan software con licencia) ¿Compraron la licencia?

- ¿Por qué usan ese software?

- ¿Tienen algún respaldo energético?

- ¿Alguna vez han experimentado fallas graves (no funcionan los sistemas o la red)? ¿Qué hacen en esos casos?

- ¿Tienen una guía para casos como los antes mencionados?

- ¿Cuántas personas tienen acceso a las PC? ¿Cómo se identifican?

- ¿Qué tan capacitados están en el manejo de las redes (Solución de problemas)?

- ¿Los equipos de telecomunicación son administrables? ¿Tienen contraseña? ¿Quién las maneja?

- ¿Cuánta gente tiene acceso a ellos? ¿Cómo se identifican?

- ¿Cuál es el uso diario que le dan a los equipos?

- Si tiene WIFI ¿Quiénes tienen acceso a el? ¿Por qué? ¿Cuáles son los requisitos para tener acceso a el? ¿Qué tipo de seguridad tiene?

- ¿Alguna vez han tratado de hackear la red? Si ha pasado ¿Qué hacen para evitarlo?

- ¿Tienen algún manual o plan en caso de falla de la red en medio de operaciones importante?

- ¿Quién toma las decisiones para modificar la red?

- ¿Tiene problemas relacionados al congestionamiento de la información?

- ¿Cada persona tiene una cuenta para iniciar sesión en las máquinas o no?

- ¿En el sistema que utilizan estos tienen usuario y password? ¿Alguna vez han tenido problemas en el sistema al momento de ingresar datos? ¿Qué hacen en casos como estos?

- ¿Permiten que los usuarios inserten memorias USB a los equipos? O ¿deben pedir permiso? O ¿no esta autorizado?

- El control de la información que se procesa en el sistema ¿se almacena en algún tipo de base de datos?

- ¿En qué software almacenan estos datos? (Excel, SQL, Access)

- ¿Poseen un respaldo o replica de los datos que almacenan en caso de que pueda suceder cualquier percance en otro servidor para poder recuperarlos?

- ¿Poseen los usuarios del sistema restricciones en el uso del sistema operativo? Es decir, ¿se les permite hacer todo o no?

- ¿Cada cuánto se actualizan el nivel de los sistemas operativos y en que se basa esa decisión?

- ¿Cómo deciden la adquisición de los paquetes de software?

- ¿Una vez instalado un nuevo software que procedimiento siguen para que los usuarios conozcan las nuevas facilidades soportadas?

5. CUESTIONARIO A ENCARGADA DE ADMINISTRACIÓN (INVENTARIO Y MANTENIMIENTO)

NOMBRE DE LA INSTITUCIÓN:
_____
DIRECCIÓN: _____
AUDITORÍA A:
_____
FECHA DE INICIO: _____ FECHA DE FINALIZACIÓN: _____
NOMBRE DEL AUDITOR:
_____

Objetivo: Obtener datos específicos de la realización de mantenimiento e inventario en la empresa.

- ¿Tienen alguna bodega donde mantengan equipos viejos o nuevos? ¿Qué hacen con los equipos dañados?

- ¿Tienen algún plan en caso de que algún equipo no funcione correctamente?

- ¿Tienen algún tipo de acuerdo con alguna compañía distribuidora de equipos de informática?

- ¿Cuál es su ISP (Internet Service Provider)? ¿Por qué lo eligieron?

- ¿Hace cuanto trabajan con el? ¿Miden la velocidad de transferencia de datos? ¿Es la misma que el ISP (Internet Service Provider) estipula en el contrato?

- ¿Ha tenido problemas con la red? ¿El proveedor alguna vez ha faltado a lo estipulado en el contrato? ¿Cada cuanto renuevan contrato con el?

- ¿Cuáles fueron los criterios para adquirir los equipos de telecomunicaciones?

- ¿Qué seguridad emplean para estos equipos? ¿Hay planes de ponerles más seguridad en el futuro?

- ¿Además de Internet que otros servicios les ofrece y como ha sido la calidad de los servicios adicionales?

- ¿Cada cuánto dan mantenimiento a la red?

- ¿Cuánto tiempo tiene la red actual? ¿Como empresa disponen de un plan informático?

- ¿Tienen un presupuesto designado directamente al mantenimiento de los sistemas que utilizan?

- ¿Existe una jerarquía de roles dentro del departamento?

- ¿Poseen los manuales de usuario, documentación final y código de los sistemas adquiridos?

- ¿Cuenta la empresa con las respectivas licencias y facturación del Software adquirido? (S.O, sistemas de aduana, Antivirus, etc.)

- ¿Está debidamente actualizado el software actual?

- ¿Quién le proporciona los servicios de mantenimiento al software? ¿Una empresa externa o una persona interna?

- ¿Las personas usuarias de los sistemas, tienen acceso a Internet libremente? O ¿utilizan los equipos únicamente para interactuar con el sistema que trabajan?

- ¿Con qué frecuencia de tiempo se le brinda mantenimiento al software?

- Cada 3 meses: _____
- Cada 6 meses: _____
- Anualmente: _____

6. EVIDENCIAS DE LA EMPRESA (LUGAR, EQUIPOS,PERSONAL, SISTEMAS)

Figura 1. Computadoras del área de operaciones

Figura 2. Impresora Multifuncional Xerox

Figura 3. Vista amplia de las Pc's del área de operaciones

Figura 4. Siduanea World Pantalla Inicial

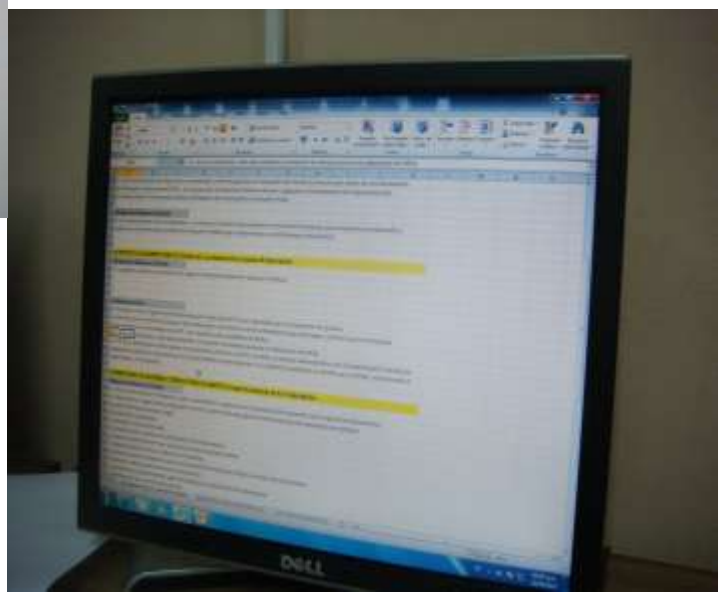


Figura 5. Correo institucional en Plataforma Outlook

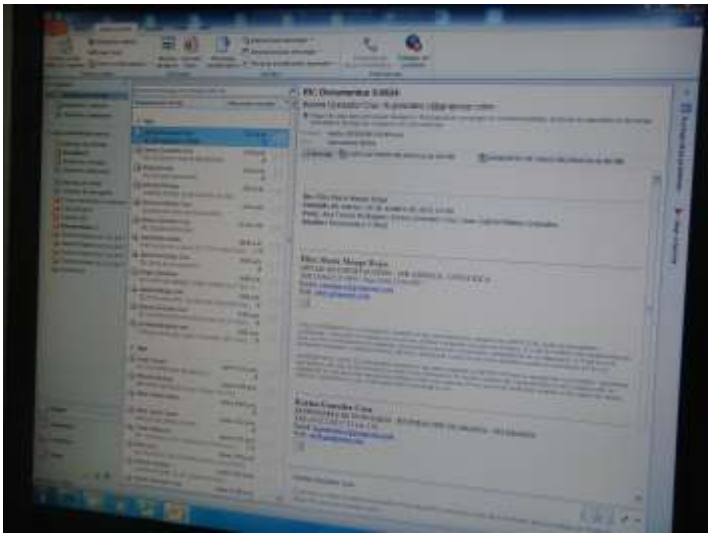


Figura 6. Muestra de como se realizan las gestiones en formato Excel

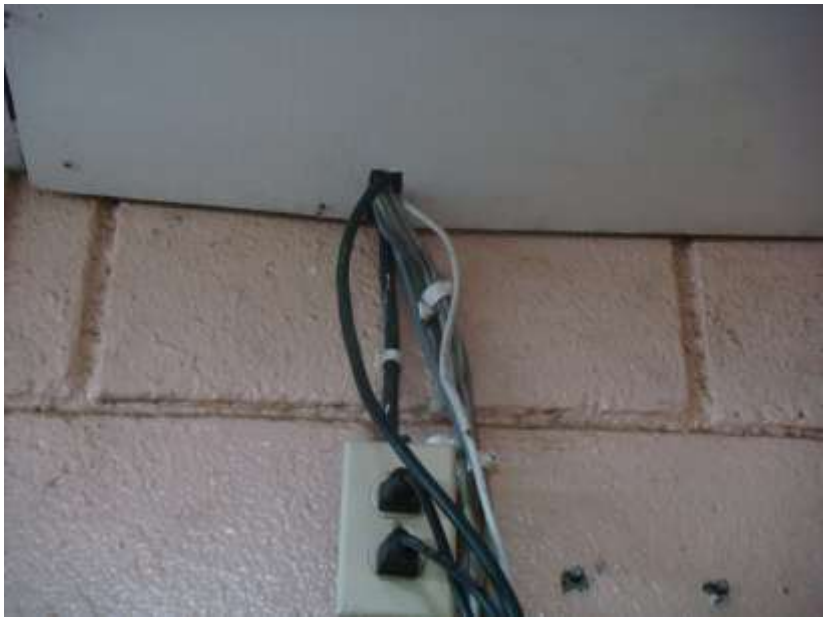


Figura 7. Parte externa del área de operaciones
donde se notan las conexión de la antena hacia el router

Figura 8. Muestra de como el
cableado esta protegido por las canaletas

Figura 9. Cableado que sale del router a las Pc's

Figura 10. Router D-Link

Figura 11. Vista amplia de la ubicación de router

Figura 12. Vista Cercana de Router

Figura 13. Antena de red

Figura 14. Conexión de antena hacia router

7. ESPECIFICACIONES DE LA APLICACIÓN WINAPPLIVE ®

WinAppLive es una aplicación que realiza auditoría, análisis, estadística y control de uso del software y las impresoras

La tarea de monitorear el equipamiento utilizado y medir los tiempos de forma clara y precisa le permitirá cuantificar costos, incrementar el rendimiento de su inversión, optimizar el uso de recursos, mejorar la gestión proporcionándole una visión de uso de forma clara y precisa.

La herramienta se puede utilizar en pequeños entornos (hogar) o en grandes organizaciones y está basada en una rápida y fácil implementación.

Ofrece respuesta a lo siguiente:

¿Cuánto tiempo se está insumiendo en tareas frente al PC?
¿Cómo se distribuye el tiempo de utilización del software?
¿Qué software está siendo más utilizando?
¿Cuánto está imprimiendo una persona o un área?
¿Qué impresora es la más utilizada por una persona o por un área?
¿Qué tiempo y que costo tiene el chat en mi organización?
¿Hay funcionarios que juegan en horario laboral?
¿Estarán utilizando programas para bajar música o software? - El ancho de banda siempre es insuficiente
¿En qué se está gastando el tiempo y los recursos?

Características:

- ✓ Fácil de instalar y de poner en ejecución.
  Auditoría y control del software que puede correr (entre periodos de tiempo).
- ✓ Auditoría y control de las impresiones realizadas.
- ✓ Administración de usuarios y grupos para todas las auditorías y controles.
- ✓ Un conjunto importante de reportes predefinidos

- ✓ Alarmas vía email (determinado por los umbrales).
- ✓ Interface de usuario 100% web
- ✓ Integración con Active Directory
- ✓ Corre en equipos independientes o en entornos de red.
- ✓ Compatible con Windows 2000, XP Home/Pro, Server 2003 todas la ediciones.
- ✓ Disponible en lenguaje ingles, español y portugués.
- ✓ Instalación remota desatendida en entornos de red o ejecución vía login script
- ✓ Mejoras y actualizaciones en línea desde Internet
- ✓ Modo invisible para el usuario final

Para correr necesita lo siguiente

Software

- Windows 2000 o superior
- IIS 5 o superior
- Internet Explorer 6 o superior
- Flash Player 5 o superior

Hardware

- No hay mínimos de Hardware el software está probado con el hard base de Windows 2000

Otros

- En entornos Corporativos contar con la contraseña del administrador
- Tener habilitados los puertos SMTP (25)