ESCUELA SUPERIOR POLITECNICA DEL LITORAL

CENTRO DE EDUCACION CONTINUA

Diplomado en Auditoría Informática

V PROMOCION

PROYECTO

Tesis Previo la Obtención del Diplomado en Auditoria Informatica

TEMA:

"Auditoría al Centro de Computo de Almacenes Carito en Base a la Metodología de Control Interno"

AUTORES:

María Fernanda Cortes Saavedra

Jessica Carolina Machuca De La Torre

Año 2011

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

CENTRO DE EDUCACION CONTINUA

DIPLOMADO EN AUDITORIA INFORMATICA

V PROMOCIÓN

PROYECTO

TESIS PREVIO LA OBTENCION DEL DIPLOMADO EN AUDITORIA INFORMATICA.

TEMA

"AUDITORIA AL CENTRO DE COMPUTO DE ALMACENES CARITO EN BASE A LA METODOLOGIA DE CONTROL INTERNO"

AUTORES

MARIA FERNANDA CORTES SAAVEDRA

JESSICA CAROLINA MACHUCA DE LA TORRE

AÑO 2011

TABLA DE CONTENIDO

CAPITULO 1

1. INTRODUCCION

La información de la empresa es uno de los activos más importantes que posee. Las organizaciones tienen que desarrollar mecanismos que les permitan asegurar la disponibilidad, integridad y confidencialidad en el manejo de la información debido a que está sujeta a muchas amenazas internas como externa.

Las amenazas y debilidades pueden afectar notablemente a la organización debido que se maneja información sensible como ventas, compras e inventario de textiles que se importan al por mayor y menor; por lo que es importante que la información siempre esté disponible y sea confiable.

Por eso se debe llevar un control en el departamento de TI de la organización, con el fin de relevar la consistencia de los sistemas de información y de control, las debilidades de seguridad en los programas y operaciones, y el cumplimiento de los reglamentos y normas prescriptas.

Para el desarrollo de la auditoría, se tiene que conocer y comprender cuáles son sus principales procesos, políticas o normativas que se maneja para resguardar la seguridad de la información, los objetivos de la empresa y del área de TI.

En base al levantamiento de información que se realizará mediante controles generales, utilizando entrevistas, cuestionarios y visitas técnicas, se podrá evaluar si los objetivos de TI están alineados a los objetivos del negocio y si están cumpliendo las políticas y procedimientos de seguridad adecuadamente prescritos.

Como resultado se generará una opinión técnica objetiva con respecto al nivel de seguridad de la información dentro del centro de cómputo, adicional a esto se detallará las debilidades encontradas y se emitirá las recomendaciones que contribuyan a mejorar los controles los controles generales.

1.1. ANTECEDENTES

La gerencia general del almacén, solicita una evaluación a los sistemas de información y el control interno del departamento de TI, para determinar si los controles utilizados son adecuados y asegurar el cumplimiento de las políticas y/o reglamentos incorporados en los sistemas.

Acorde a lo conversado con el Gerente General y Gerente de TI se acordó auditar las áreas que son más críticas para el negocio, debido a que se han presentado incidentes en el manejo de la información.

A continuación se describen las áreas de control a evaluar:

- Administración de la Seguridad Física y Lógica
- Adquisición, Desarrollo y Mantenimiento de los Sistemas
- Administración de Redes
- Administración de Base de Datos
- Administración de Operaciones

Se elaborará un informe final para indicar la criticidad de los situaciones encontradas en el transcurso del esta auditoría, al reunir evidencias que serán adjuntadas y se expondrá las conclusiones y recomendaciones a seguir.

1.2. OBJETIVO ESPECIFICO

El objetivo principal es emitir un informe objetivo detallado respecto al diseño y eficacia de los controles generales implementados dentro del centro de computo en el área de desarrollo, base de datos, seguridad y operaciones, a fin de informar al Gerente General si existe un control adecuado para la protección de la información y los activos de la organización; determinar la confidencialidad, integridad y disponibilidad de los datos y las responsabilidades que debe asumir cada uno de los empleados de la organización.

1.3. OBJETIVOS DETALLADOS

- Revisar y Evaluar los controles del departamento de TI de la organización a fin de garantizar que cumplan con los servicios.
- Evaluar el control de los activos, su mantenimiento y falla de los equipos.
- Evaluar los controles para los accesos físicos y lógicos del área del centro de cómputo.
- Evaluar los procedimientos de control de operación, analizar su estandarización y evaluar el cumplimiento de los mismos.
- Evaluar los procedimientos de adquisición, desarrollo y mantenimiento de las aplicaciones y su base de datos

CAPITULO 2

2. ENTENDIMIENTO DEL NEGOCIO

2.1. ANTECEDENTES

Esta empresa surge antes de las diversas necesidades del mercado, de encontrar textiles de excelente calidad, diseños novedosos, diversidad de productos para ambos sexos y a precios accesibles, todo esto es un conjunto; además de encontrarlo en un solo lugar, con instalaciones espaciosas, cómodas y aptas para recibir a sus clientes poder brindarles atención personal y especializada.

Tiene como principal actividad la venta de textil al por mayor y menor, la cual, para asegurarse de que los productos fueran del total gusto, exigencias y necesidades del público y además cumplirán con las principales normas y controles estadísticos de calidad, decidió establecer su propio diseño de producción, asesorada por fabricas del extranjero y contando con la dirección de expertos en la materia, constituyendo así una nueva e importante fuente de empleo en el país.

De esta manera La Empresa tiene sus dos primeros almacenes bajo el nombre "ALMACENES CARITO", con el compromiso de extenderse a las diferentes regiones del país. Así surgió esta compañía en constante crecimiento y totalmente comprometida con el consumidor.

2.2. MISION

Adquirir e innovar puntos de alta calidad, dando un servicio de excelencia, para satisfacer los requerimientos de nuestros clientes que cumpla con sus exigencias y necesidades y que al mismo tiempo nos permita competir en el mercado nacional, así como fomentar el desarrollo humano y profesional de nuestros colaboradores.

2.3. VISION

Ser la mejor empresa en su ramo de todo el Ecuador, así como extender nuestra cadena de tiendas por el resto del territorio, sin temor a los cambios y preocuparnos por el bienestar social aplicando nuestros conocimientos en beneficio de la sociedad.

2.4. CADENA DE VALOR

Logística Interna: Los insumos como textiles, hilos, moños, refuerzos y etiquetas se encuentran almacenados en una bodega a donde se dirige cada operaria para tomar el material que sea necesario para desempeñar su actividad.

Operaciones: La elaboración de los despachos está dividida en operaciones de corte, ensamblaje, revisión y empaque del producto para su posterior distribución a terceros o a clientes directos.

Logística Externa: Los tejidos que corresponden a pedidos elaborados por terceros o grandes empresas de marcas reconocidas son recogidos por estas inmediatamente el pedido se haya terminado. Las prendas que pertenecen a la empresa son llevadas a domicilio de quienes elaboren el pedido.

Mercadeo y Ventas: La empresa cuenta con publicidad en medios de comunicación, pero no cuenta con un departamento dedicado al mercadeo; son sus administradores (dueños de la empresa) quienes se han encargado de acreditarla a través de la excelente calidad y entrega oportuna.

2.5. PANORAMA ACTUAL

Actualmente la empresa cuenta con un 75% de productos importados y un 25% de productos nacionales, ofreciendo prendas de calidad media-alta a precios baratos, que se importan fundamentalmente de los países asiáticos. En el último año existe un aumento de 12,0% anual en ventas.

2.6. PRODUCTOS CLAVES

Productos y Servicios: Importador de productos textiles de alto valor agregado, bajo estándares internacionales de calidad.

2.7. CLIENTES

Nuestro principal clientes al por menor: Consumidor final debido a nuestras variedades en tejidos, calidades y precios.

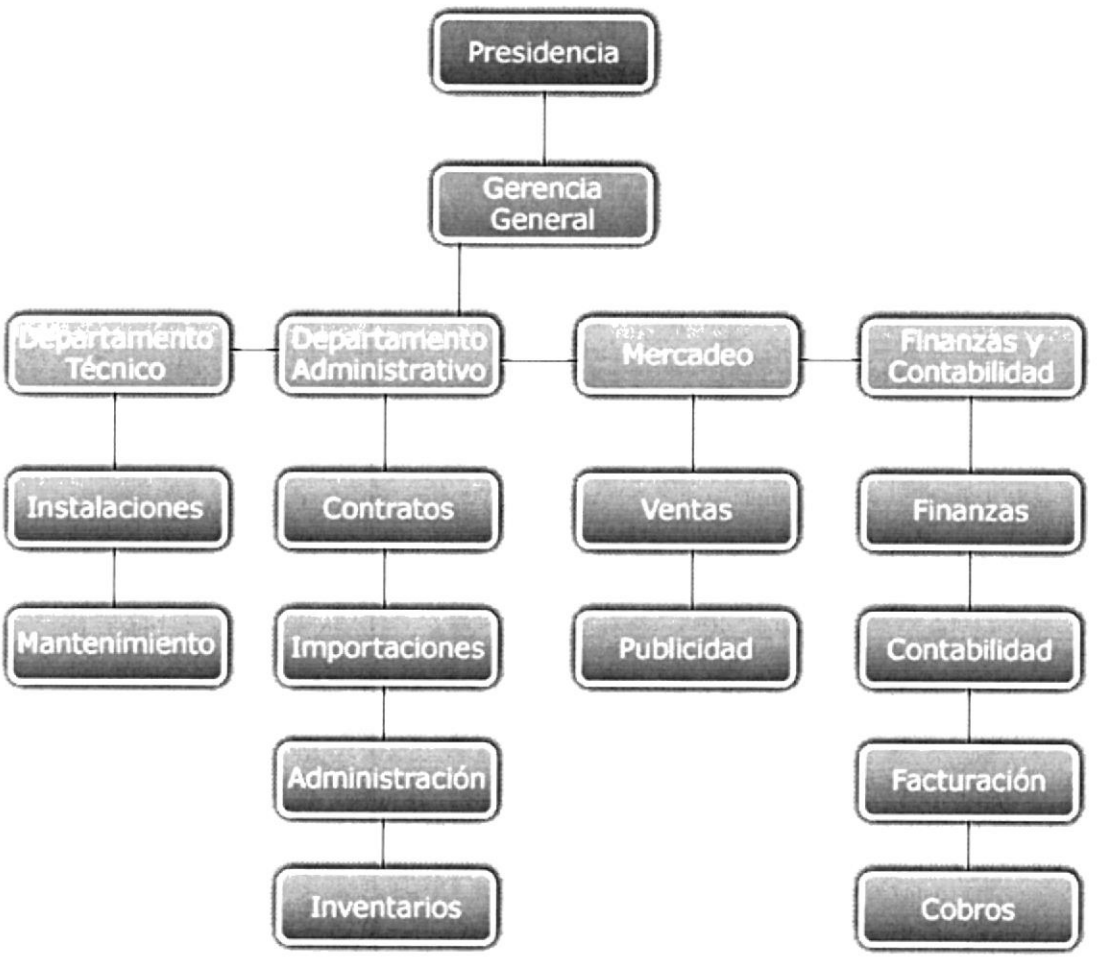
Nuestro principal clientes al por Mayor: Los confeccionistas de las diferentes regiones del país.

2.8. MERCADOS

La empresa tiene un gran mercado a nivel nacional, se tiene su matriz en la ciudad de Guayaquil y sucursales en diferentes ciudades: Guayaquil, Quito, Manabí, Cuenca, Ambato y Loja.

2.9. ESTRUCTURA ORGANIZACIONAL DE LA EMPRESA

La empresa está estructurada de la siguiente manera:



2.9.1. ESTRUCTURA DEL DEPARTAMENTO DE TI

El departamento de TI tiene dos personas que está distribuida de la siguiente manera:

El gerente de TI tiene comunicación directa con la gerencia, sus funciones no están definidas de manera formal pero se encarga de receptar las solicitudes de los usuarios sobre los diferentes problemas que se presentan a nivel tecnológico en la empresa, también se encarga de la administración la de la base de datos.

Mantenimiento de hardware

La persona encargada de esta área realiza el mantenimiento y configuración de los equipos, servidores y de la red, este trabajo lo realiza de forma empírica; realiza las reparaciones y resuelve problemas leves en los equipos y es responsable de las adquisiciones que se realizan.

Cuando se presentan fallas complicadas recibe ayuda técnica especializada; este servicio es realizado por personal externo, ellos también se encargan de realizar un mantenimiento completo a los equipos cada dos meses a pesar de no tener un contrato formal entre ambas partes.

Mantenimiento de software

En este departamento se tiene al asistente de TI como responsable de manejar los respaldos de la base de datos y archivos en general, y el gerente de TI como encargado de realizar cambios en las aplicaciones.

El asistente de TI realiza las configuraciones para la generación de respaldos automáticos, verificación de que estos respaldos se realicen de manera correcta y de proporcionar los respaldos para las diferentes pruebas que se ejecuten.

El gerente de TI realiza los cambios en la estructura de los reportes de ventas y reportes en general según los requerimientos que solicite el gerente general en ese momento, realiza los cambios porque es el único que maneja la herramienta que actualmente están utilizando en la empresa.

En caso que se presenten problemas o necesiten realizar cambios mas técnico en la aplicación o con la base de datos, el gerente de TI envía un correo a la persona que les vendió el sistema para que resuelva el inconveniente, esto lo puede realizar remotamente o asistiendo personalmente a la empresa.

INFORMACION DE AMBIENTE DE SISTEMA

El departamento de TI tiene como objetivo normar el adecuado uso y aprovechamiento de los recursos informáticos; la optimización de las actividades, servicios procesos y accesos a la información para la toma de decisiones, mediante el desarrollo, implantación y supervisión del correcto funcionamiento de los sistemas y comunicación.

CAPITULO 3

3. PLAN DE AUDITORIA

3.1. ALCANCE DEL PROYECTO

La presente auditoria comprende fundamentalmente en la planificación, ejecución y evaluación de los controles generales implementados de los siguientes aspectos:

- Administración de la Seguridad Física y su entorno
  - Control del acceso físico al centro de cómputo
  - Ambiente del Centro de Cómputo
  - Control de acceso a equipos

- Administración de la Seguridad Lógica
  - Administración de cuentas
  - Autenticación de usuarios
  - Administración de Contraseñas
  - Registros de Auditoria

- Adquisición, Desarrollo y mantenimiento de los sistemas
  - Adquisición de Aplicaciones
  - Desarrollo y Cambios de Cambios
  - Mantenimiento de Aplicaciones

- Administración de Redes
  - Configuración y Diagrama de la Red
  - Políticas y procedimientos de mantenimiento y soporte de la red
  - Antivirus
  - Firewall
  - Monitoreo de la Red

- Administración de Base de Datos
  - Estándares definidos para el diccionario de datos

- Estructura de la Base de Datos
- Monitoreo del desempeño de la base de datos
- Permisos a nivel de base de datos (consulta, modificación, creación y eliminación de los registros)
- Cambios a la información y Niveles de aprobación.
- Disponibilidad de Respaldo

- Administración de las Operaciones
  - Segregación de funciones
  - Administración de las operaciones del departamento de TI
  - Capacidad de Almacenamiento y rendimiento
  - Políticas de Respaldos

3.2. PERIODO DE EVALUACIÓN

La auditoria se realizará en base a las evidencias y registros que se tiene en el último semestre del año (enero – julio del 2011), esta evaluación se realizará en el periodo agosto a septiembre del 2011.

3.3. RECURSOS

El personal involucrado en el desarrollo de la auditoria es de dos personas, las mismas que se comprometen a resguardar la información sensible del negocio.

Como requerimiento inicial para el desarrollo de la auditoria se va a solicitar información confidencial de los procedimientos y políticas mencionadas anteriormente en la metodología.

Las personas que se van a encargar del desarrollo de este trabajo serán:

- ING. MA. FERNANDA CORTÉS
- ING. JESSICA MACHUCA

3.4. PLAN DE TRABAJO

Se llevará a cabo la auditoría en la oficina matriz de la empresa de la ciudad de Guayaquil, se realizarán en cada etapa a ejecutarse las siguientes tareas:

1. Administración de la Seguridad Física

    a. Solicitud de políticas para el acceso a áreas seguras y centro de cómputo.

    b. Verificación de acceso solo a personal autorizado al centro de cómputo.

    c. Solicitud y Verificación del diagrama físico y lógico del centro de cómputo.

    d. Visita técnica para comprobación de seguridades físicas de las instalaciones del centro de cómputo.

    e. Visita técnica para comprobación de que existan medidas de prevención contra eventos de la naturaleza o producidos por el hombre.

    f. Verificación de inventarios de los equipos informáticos dentro de la organización.

    g. Entrevistas al personal encargado del centro de cómputo sobre manejo de equipos dentro y fuera de la organización.

    h. Entrevistas al personal para darle de baja a los equipos.

    i. Verificación de procedimientos de fallas de los equipos.

2. Administración de la Seguridad Lógica

    a. Verificación de no acceso de cuentas por defecto a nivel de base de datos, aplicaciones y sistemas operativos.

    b. Verificación de des-habilitación de cuentas por defecto a nivel de base de datos, aplicaciones y sistemas operativos.

    c. Solicitud y verificación de perfiles de usuarios, privilegios y roles actualizados a nivel de base de datos, aplicaciones, sistema operativos y redes.

    d. Solicitud de lista de acceso y políticas de control de acceso.

    e. Evaluación de las políticas de acceso y autenticaciones de las aplicaciones.

    f. Solicitud de políticas para la administración de contraseñas.

    g. Verificación de las políticas para cambios de contraseñas de cuentas genéricas y de usuarios.

    h. Verificación de las activaciones del logs de auditoría para aplicaciones y base de datos.

3. Adquisición, Desarrollo y Mantenimiento de los sistemas

    a. Solicitud de planificaciones de compra y/o desarrollo de los sistemas.

b. Solicitud de las licencias de software instaladas en los equipos.

c. Solicitud de formatos para requerimientos de cambios de programas, autorizaciones

d. Solicitud de los cambios realizados y reporte de pruebas

e. Identificación de los responsables para autorizar cambios a los programas

f. Metodología utilizada para la implementación de programas y control de cambios

g. Análisis del manejo de la información por parte del personal de desarrollo y producción

h. Inspección Técnica del ambiente de desarrollo, producción y pruebas de las aplicaciones.

i. Solicitud de Bitácoras de actualizaciones de las aplicaciones, sistemas operativos y base de datos principales.

j. Solicitud y Verificación de los programas instalados en los equipos

4. Administración de Redes

a. Solicitud del diagrama y configuraciones de red

b. Solicitud y verificación del listado de IP de la red

c. Entrevista para la verificación del cumplimiento de Políticas y procedimientos de mantenimiento y soporte de la red

d. Solicitud y Verificación de Incidentes o Fallas de la red

e. Verificación de que los programas y datos se encuentren conectado por medio de la red.

f. Verificación de que los recursos se encuentren asignados de manera correcta.

g. Solicitud y Verificación de la configuración del Firewall

h. Verificación de las actualizaciones del antivirus instalado

i. Evaluación del monitoreo de la red

5. Administración de Base de Datos

a. Solicitud del diccionario de datos

b. Verificación del Cumplimiento de los estándares definidos en el diccionario de datos

c. Solicitud del Diagrama de la estructura de la Base de Datos

d. Verificar la responsabilidad de control de la administración de la base de datos.

e. Solicitud de registros de errores para verificar desempeño de la base de datos.

f. Solicitud y Evaluación de los perfiles de usuario.

g. Solicitudes de cambios a la información, identificar niveles de aprobación.

h. Verificación de los niveles de aprobación.

6. Administración de las Operaciones

a. Solicitud del Organigrama del departamento de TI

b. Verificación de una correcta segregación de funciones en el departamento.

c. Verificación de la capacidad de almacenamiento de la base de datos

d. Verificación del rendimiento del procesador y porcentaje de disco duro utilizado

e. Solicitud de políticas de respaldos y recuperación de la información

f. Solicitar y revisar la bitácora de respaldos (acta de entrega y recepción)

En cada etapa se realizará un análisis de los datos relevados, hallazgos de debilidades y generación de recomendaciones que se las colocará en un Pre-informes realizado por el auditor al final.

Se tendrá una revisión del Pre-informe de las observaciones con el personal involucrado, para luego emitir un informe final con los compromisos adquiridos por el departamento.

3.5. FUENTES DE INFORMACIÓN

Se coordinará con el Gerente del departamento de TI la realización de las siguientes actividades:

- Solicitud de Manuales, políticas, estándares seguidos por la organización
- Organigrama del Departamento de TI y Funciones.
- Cuestionarios a ejecutarse para el personal
- Informes Realizados de Control de Cambios a los sistemas realizados
- Registros de los sistemas principales y/o accesos físicos y lógicos
- Entrevistas a realizar al personal (Ver anexo A)
- Visitas a las áreas seguras y centro de cómputo de la organización.

CAPITULO 4

4. ADMINISTRACIÓN DE LA SEGURIDAD FÍSICA

4.1. OBJETIVO

Evaluar que las personas que acceden al centro de cómputo cumplan con las políticas necesarias para el acceso y utilización de recursos.

4.2. CONTROL DE ACCESO FÍSICO AL CENTRO DE CÓMPUTO

El centro de cómputo se encuentra ubicado en el tercer piso del edificio en la oficina del Gerente de TI junto al departamento de contabilidad; no existen ventanas en la oficina y las paredes son la mitad de vidrio lo cual se puede ver al interior de la oficina. El área no tiene piso o techo falso.

El centro de cómputo no posee controles biométricos o puertas de acceso con tarjetas magnéticas, el personal no autorizado puede ingresar al departamento sin ninguna restricción o sin tener una persona que supervise su ingreso, la única seguridad que se tiene es una puerta que cuando no esta ninguna de las personas encargadas del centro de cómputo se cierra con llave y la llave la dejan en recepción.

No se tiene políticas y procedimientos formales para el acceso a personal interno o externo al centro de cómputo.

La empresa cuenta con guardias de seguridad; en horarios laborables se ubican en el interior y exterior de la misma.

4.3. AMBIENTE DEL CENTRO DE CÓMPUTO

El centro de cómputo no dispone de planes o herramientas para las seguridades de los equipos o información ante eventos de la naturaleza o producido por el hombre.

- **Alarmas de Fuego**: no se tiene instalado alarmas contra fuego o incendios en el centro de cómputo, lo cual es necesario en caso de existir un conato de incendio.
- **Extintores**: no se tienen instalados extintores en el centro de cómputo, ni áreas seguras de la organización.
- **UPS**: se tiene el uso de UPS para servidores con una duración de tres minutos, pero no para las demás equipos.

- **Descargas de tierra:** para los equipos de la organización no se tienen las líneas de potencia aterrizadas, esto es necesario en caso de variaciones de poder.
- **Generador de energía**: se tiene un generador que hay que conectar manualmente y solo permite que funcionen las cajas para facturar a los clientes, las demás áreas quedan fuera de servicio.
- **Luz de Emergencia**: no se tiene una luz de emergencia en caso de que si existe un corte de luz se active automáticamente.

El centro de cómputo cuenta con un aire acondicionado central apropiado para los servidores.

4.4. CONTROL DE ACCESO A EQUIPOS

Para el cumplimiento de los objetivos del negocio, el departamento de TI ha definido la siguiente arquitectura de servidores:

Servidor	Sistema Operativo	Ubicación	Información
Servidor de Aplicaciones y Base de Datos	Ubutu (Linux)	Centro de Cómputo (Matriz)	Todas las aplicaciones utilizadas en la organización y base de datos. Carpetas compartidas por departamento con sus respectivos permisos de usuario.
Servidor de Internet	Ubutu (Linux)	Centro de Cómputo (Matriz)	Firewall y servidor de internet
Servidor de Aplicaciones y Base de Datos	Ubutu (Linux)	Centro de Cómputo (Sucursal)	Todas las aplicaciones utilizadas en la organización y base de datos. Carpetas compartidas por departamento con sus respectivos permisos de usuario.
Servidor de Internet	Ubutu (Linux)	Centro de Cómputo (Sucursal)	Firewall y servidor de internet

Actualmente se tienen 25 computadores distribuidos de la siguiente manera:

- 15 en la Matriz
- 10 en la Sucursal

Los computadores personales son clones y cada usuario es responsable de su equipo. El departamento de TI asigna los equipos a cada usuario que ingresa a la empresa, pero no existe un procedimiento formal para designación de equipos.

No se tiene el diseño del diagrama físico y eléctrico de la red del centro de cómputo ubicado en la matriz y en la sucursal, motivo por el cual al instalar o colocar un equipo compartido se lo realiza de forma empírica sin un estudio previo.

Los servidores no se apagan en horarios no laborables permanecen encendidos las 24 horas del día aunque durante la noche, no existen procedimientos en lotes que se realicen de manera automática a nivel de aplicativos, solo los procesos de respaldos.

No se tiene documentada las configuraciones de los servidores, en caso de que se des-configure los equipos se comunica a la empresa que realizó la instalación de los servidores.

Los servidores no se encuentran en un gabinete cerrado con llave, tampoco los equipos de red instalados, por este motivo cualquier persona no autorizada puede tener acceso a ellos.

A excepción de los equipos portátiles, el computador personal no debe moverse o re-ubicarse sin el consentimiento y autorización del gerente del departamento; en caso de moverlo fuera de las instalaciones, deberá estar acompañado de una autorización firmada por el gerente del departamento.

Cuando un computador cambia de usuario primario, el departamento de TI realiza una inspección física del equipo para determinar que toda información confidencial ha sido eliminada.

Se tiene un inventario de los equipos informáticos que tiene la organización pero no están detallados y actualizados, se puede desconocer en algunas ocasiones la ubicación, estado y responsable de algún equipo.

Adicional no existen contratos de seguros de equipos en especial para equipos que soportan un proceso crítico del negocio como son los servidores.

FALLAS

Si el equipo ha sido dañado, perdido, robado o no está disponible por algún motivo para las actividades normales del negocio, el usuario debe informar al departamento de TI para la habilitación del equipo.

En caso de presentar una falla técnica en el equipo el usuario es el responsable de reportar al departamento de TI; una vez reportada la falla el encargado de mantenimiento de hardware realiza una inspección previa del equipo, si es una falla leve realiza la reparación, caso contrario se llama a la persona externa que apoya en el soporte y reparación del equipo.

No se tiene un plan de contingencia formal, en caso de haber una falla en el servidor principal se carga toda la información y se dirección a nivel de red a un computador personal; mientras tanto el departamento de facturación y cobros realiza su labor manualmente para al final del día ingresar los valores al sistema.

EQUIPOS DE BAJA

No existen procesos para manipular o dar de baja un equipo o periférico. Los computadores y dispositivos no se identifican si están dados de baja en el inventario, se los coloca en bodega para repuesto de los demás equipos.

DISPOSITIVOS EXTERNOS

Para el manejo de dispositivos externos no existen políticas para el uso y manipulación de estos dispositivos, debido a que los computadores tienen sellado con silicón los puertos USB para que no puedan colocar ningún dispositivo externo y no tienen habilitadas las disqueteras, ni CD o DVD.

4.5. DEBILIDADES Y RECOMENDACIONES

De la evaluación realizada según la metodología surgen las debilidades encontradas y a corregir y sugerencias a poder implementarse ante la ausencia o falta de los controles.

- **Situaciones o Hallazgo detectado**: Descripción de lo que se encontró en un determinado punto de la evaluación, según las pruebas, procedimientos o técnicas de evaluaciones utilizadas para hacer la revisión; cada una de estas desviaciones es parte importante del documento.
- **Impacto**: descripción del impacto en el negocio si se lleva a materializar la situación encontrada.
- **Nivel de Riesgo**: Evaluación de la auditoría acorde al Anexo B.

- **Recomendaciones**: sugerencias del auditado o del auditor para solucionar las desviaciones reportadas. Casi siempre corresponde una solución para cada una de las causas reportadas.

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
Acceso físico al centro de Cómputo			
No se tienen políticas o procedimientos formales para el acceso de personal interno o externo al centro de cómputo.	Personal no autorizado puede ingresar al departamento sin ninguna restricción atentando a la integridad, confiabilidad y disponibilidad de la información	M	Se sugiere tener políticas de acceso para personal interno o externo.
Se evidenció que los servidores y equipos de red se encuentran ubicados en una pequeña mesa en la oficina del Gerente de TI, si no está ninguna persona dentro de la oficina se cierra con llave la puerta y se la deja en recepción.	Personal no autorizado puede ingresar a la oficina del Gerente de TI y acceder a los servidores atentando a la integridad, confiabilidad y disponibilidad de la información.	A	Se sugiere destinar un área de la empresa que sea exclusiva para ubicar los servidores, el switch central y demás equipos de tecnología informática. Esta área debe de cumplir con las medidas ambientales para el buen funcionamiento de los equipos y sobre todo cumplir con las medidas de seguridad necesarias para que personal no autorizado no tenga acceso a esta área.
Durante la visita técnica se comprobó que se puede ingresar a la Oficina donde se encuentra los servidores sin ninguna restricción, incluso durante la entrevista el Gerente de TI tuvo que salir a atender un llamado abandonando la oficina.	Personal no autorizado puede ingresar al departamento sin ninguna restricción.	M	Se sugiere implementar controles para el acceso de personal interno y externo no autorizado al centro de cómputo.

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
Ambiente del Centro de Cómputo			
Se evidenció que no se tiene instalado extintores en el centro de cómputo, se pudo observar que si hay extintores en el primero y segundo piso.	Al ser una empresa que vende productos altamente inflamables como las telas y otros derivados de esta se corre el riesgo de que se produzca un incendio pueden dañarse o perderse los equipos informáticos y la información que contienen.	A	Se recomienda implementar planes o mecanismos para la prevención de incendios.
Control de Acceso a Equipos			
Se evidenció que no se tiene una descripción de las configuraciones del servidor, solo la empresa que realizó la instalación tiene la configuración de los servidores de las aplicaciones e internet.	Se tiene dependencia por terceros en caso de necesitar una restauración de las configuraciones del servidor.	M	Se sugiere tener un procedimiento para la restauración de las configuraciones del servidor que contemple: • Detalle técnico de los servidores. • Configuración a nivel de Hardware y Software. • Responsable de estas actualizaciones.
	Se dificulta conocer la configuración exacta y actual de cada servidor, y de esta forma se obstaculiza la tarea del mantenimiento.		
	En caso de falla se puede tener una interrupción de las operaciones críticas de la organización.		
Se evidenció que los equipos dados de baja son enviados a bodega sin verificar que la información de ese equipo ha sido eliminada.	Al no tener precauciones al eliminar la información de un equipo que se da de baja, puede quedar expuesto información confidencial a personal no autorizado siendo un peligro para la empresa.	B	Se sugiere tener una política para limpiar el disco de todo software o información que se tenga de un equipo antes de darle de baja o asignárselo a otra persona.

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
Durante la entrevista al Gerente de TI se evidenció que no se tienen diagramas físicos de redes, electrónicos o planos del centro de cómputo.	Se tiene el riesgo de no tener un control adecuado en servicios de hardware en un futuro crecimiento afectando el performance que se tiene en las redes o equipos compartidos.	B	Se sugiere realizar planos físicos o electrónicos de las redes de datos, centro de cómputo para la matriz y sucursal con un responsable en la actualización de estos diagramas.
Se evidenció que no se tiene un plan de contingencia formal, en caso de haber una falla en los servidores, en caso de haberla se utilizaría un computador común.	Al levantar el ambiente de producción en forma empírica con un computador de no similares características se corre el riesgo de no tener las aplicaciones 100% operativa o dificultades en su ejecución.	M	Se sugiere tener un plan de contingencia básico que contemple lo siguiente: • Plan de respaldo: contramedidas necesarias durante la materialización de una amenaza. • Plan de emergencia. Contempla las contramedidas necesarias durante la materialización de una amenaza. • Plan de recuperación. Contempla las medidas necesarias después de materializada y controlada la amenaza. • Responsable/ Persona que lo reportó
	Interrupción del servicio de manera continúa al no tener un plan de contingencia a seguir.		Tener un equipo de similares características para en caso de falla del servidor principal se realice en este equipo el levantamiento de los servicios críticos de la empresa.

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
No existe un inventario detallado de los equipos de equipos.	No se tiene un control de las características y estado de los equipos que se encuentran instalados en cada departamento de la organización.	B	Se recomienda tener un inventario detallado de los equipos, donde se incluya: • Hardware: dispositivos instalados en cada máquina, número de serie, y demás datos sobre procesadores, tarjetas, teclados, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, servidores, routers, bridges. • Software en los equipos: programas fuente, programas objeto, utilerías, programas de diagnóstico, sistemas operativos, programas de comunicaciones, números de licencias. • Datos o principales archivos que contienen los equipos. • Configuración de los equipos (y sus archivos de configuración). •Ubicación de los equipos (departamento). • Responsable

4.6. CONCLUSIONES

En el siguiente cuadro se muestra la evaluación por las secciones descritas acorde al alcance definido:

Proceso	Efectividad sobre el objetivo de Control
CONTROL DE ACCESO FÍSICO AL CENTRO DE CÓMPUTO	NO CUMPLE
AMBIENTE DEL CENTRO DE CÓMPUTO	NO CUMPLE
CONTROL DE ACCESO A EQUIPOS	NO CUMPLE

Como resultado de la auditoría se concluye que los controles internos **NO SON ACEPTABLES,** personal no autorizado puede acceder al centro de cómputo sin ninguna restricción lo que puede ocasionar que se atente contra la seguridad de la información y de los equipos; adicional no se tiene un buen ambiente de control para eventos producidos por la naturaleza o por el hombre, esto pone en riesgo la continuidad del negocio; para el control de acceso a equipos se lo realiza de manera no formal pero no se tienen procedimientos definidos por lo que cumple parcialmente el objetivo de control evaluado.

Se debe considerar la implementación de controles aceptables a mediano plazo acorde a la evaluación de la auditoría realizada. Los controles han sido evaluados en base a su diseño y eficiencia.

CAPITULO 5

5. ADMINISTRACIÓN DE LA SEGURIDAD LÓGICA

5.1. OBJETIVO

Evaluar los controles de accesos de los usuarios a las aplicaciones y a los datos que éstas gestionan, a fin de verificar la confidencialidad, integridad y disponibilidad de la información al cumplir con las políticas de acceso de la empresa.

5.2. ADMINISTRACIÓN DE CUENTAS

No se tiene un procedimiento formal para la creación de cuentas de usuario de los aplicativos, Red y Base de datos, cuando un empleado ingresa a la empresa el Gerente de TI crea su usuario y le asigna dependiendo del departamento al que pertenecen los permisos respectivos.

Las aplicaciones no realizan validaciones de intentos fallidos por usuario.

Las cuentas de usuarios son creadas a cada usuario por cada departamento para el ingreso de las aplicaciones y registro de las transacciones.

Se tienen deshabilitadas las cuentas genéricas para el acceso tanto para los sistemas operativos, aplicaciones, redes y base de datos de la organización.

Existen cuentas de usuarios administradores con la cual la persona encargada puede ver la información de todos los módulos que tiene el sistema y la base de datos, este usuario puede ingresar desde cualquier computador y acceder a toda la información.

No existe en el sistema una lista de control de acceso que se pueda identificar los tipos de usuarios a las aplicaciones y base de datos.

5.2.1. PERMISOS DE USUARIO

El departamento de TI no realiza una revisión periódica los derechos de acceso a los usuarios, perfiles y permisos asignados. Los permisos se asignan por medio de configuración a los aplicativos para que los usuarios puedan ingresar a los módulos asignados y carpetas compartidas.

5.2.2. INACTIVIDAD DE CUENTAS

En algunos computadores no se tiene habilitado el bloqueo del computador por inactividad, se pueden tener sesiones abiertas por parte del personal debido a que los servidores están encendidos las 24 horas del día.

Las cuentas de usuarios que permanecen varios días sin actividad no pasan a un estado de suspensión automática.

5.2.3. BAJAS DE CUENTAS

No existe un procedimiento formal para dar de baja a un usuario. Las cuentas de usuario no se eliminan de la aplicación, se actualiza en la base de datos la fecha de anulación que corresponde a la fecha de salida del usuario de la empresa; de esta manera las transaccionales realizadas por esta cuenta quedan almacenados en el base y no es posible repetir los ID de usuarios anteriores a los nuevos empleados.

5.3. AUTENTICACION

Para la autenticación del usuario a nivel de aplicaciones y de red se realiza de la siguiente manera:

1. Ingreso de Nombre de usuario (a completar por el usuario)
2. Ingreso de Contraseña (a completar por el usuario)
3. Verificación de la autenticidad de la identificación
4. Validación si las credenciales aportadas son suficientes para dar acceso al usuario.

Cuando un usuario quiere autenticarse en el sistema "SPACE" se presenta en el campo de contraseña el carácter asteriscos, pero si se da click con el mouse la aplicación revela la contraseña ingresada por el usuario.

Los datos de autenticación de los usuarios de las aplicaciones se almacenan en la base de datos del sistema sin ninguna encriptación; esta información puede ser visualizada si se tiene la contraseña de la base de datos.

5.4. ADMINISTRACIÓN DE CONTRASEÑAS

Cuando un empleado ingresa a la compañía se genera de forma manual la contraseña en la base de datos por el Gerente de TI, luego de creada la cuenta con la contraseña se la da al empleado para su ingreso al sistema.

El gerente de TI crea la contraseña del usuario de manera directa a la base de datos con al menos 7 caracteres en una combinación de números, caracteres especiales,

letras mayúsculas y minúsculas; adicional no se usa salvo que estén acompañados de caracteres adicionales no relacionados los nombres propios, ubicación geográfica, número de placa del automóvil, número de identificación, del seguro social y fechas de cumpleaños.

A los servidores, equipos de red y base de datos se puede ingresar con una clave universal, no se han cambiado las claves a pesar que se tiene conocimiento, por este motivo personal no autorizado puede que acceda a programas no autorizados e incluso puede visualizar las claves de los demás usuarios.

La contraseña dada por el Gerente de TI no puede ser modificada, las aplicaciones no permiten realizar cambios de contraseñas.

Debido a que no se tiene definido políticas para cambios de contraseña de manera automática, no existe un historial de contraseñas.

Si un usuario bloquea u olvida su contraseña debe avisar al departamento de TI, el cual cambiará la clave directamente en la base de datos e informará cual es la nueva clave al usuario.

5.5. REGISTROS DE AUDITORIA

No se tienen activados los registros de auditoría para las aplicaciones y base de datos de manera que se puede dar seguimiento al tipo de transacción realizada, accesos a recurso por fecha y usuarios, a pesar que se posee un registro de transacciones para la eliminación de facturas.

5.6. DEBILIDADES Y RECOMENDACIONES

De la evaluación realizada según la metodología surgen las debilidades encontradas y a corregir y sugerencias a poder implementarse ante la ausencia o falta de los controles.

- **Situaciones o Hallazgo detectado**: Descripción de lo que se encontró en un determinado punto de la evaluación, según las pruebas, procedimientos o técnicas de evaluaciones utilizadas para hacer la revisión; cada una de estas desviaciones es parte importante del documento.
- **Impacto**: descripción del impacto en el negocio si se lleva a materializar la situación encontrada.
- **Nivel de Riesgo**: Evaluación de la auditoría acorde al Anexo B.
- **Recomendaciones**: sugerencias del auditado o del auditor para solucionar las desviaciones reportadas. Casi siempre corresponde una solución para cada una de las causas reportadas.

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
Administración de Usuarios			
Durante la revisión se comprobó que el personal de TI tiene activado el acceso a todas las opciones del sistema principal.	Al tener acceso todo el personal a información confidencial o sensitiva de la empresa existe la posibilidad de que peligre la integridad de la información al aumentar el riesgo de un posible fraude o cometer errores.	A	Se sugiere limitar los accesos al personal de TI, dejando activos solamente las opciones que son de su competencia. Se recomienda tener un solo responsable usuario administrador tanto para los aplicativos como para la base de datos.
Durante la revisión de cuentas de usuarios se comprobó: • No se tiene políticas o procedimientos formales para la creación de cuentas de usuarios en los aplicativos y base de datos. • No se lleva a cabo una revisión periódica ni control sobre las cuentas de los usuarios o permisos que se tienen asignados.	Se posibilita que por error o negligencia la cuenta o los permisos de algún usuario sean modificados, permitiendo a usuarios no habilitados accedan a información sensible.	M	El departamento de TI debe establecer políticas para la creación de cuentas de usuario que incluyan: • Perfil de Usuario • Modificaciones de cuentas • Des-habilitación de cuentas. • Responsable de los cambios Se recomienda realizar un control de las cuentas de usuarios de manera periódica, que contenga: • Se encuentren activas solo las cuentas en uso. • Tipos de permisos que los usuarios poseen sobre los mismos. •Las contraseñas se cambien periódicamente.
No se tiene una lista de control de acceso de los usuarios a las aplicaciones.	Al tener una lista de usuarios a las aplicaciones existe la posibilidad que personal que ya no labore en la empresa acceda a las aplicaciones atentando contra la integridad de la información.	A	Se sugiere realizar una lista de acceso de los usuarios que se tienen a nivel de aplicación, base de datos y redes.

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
El encargado de hardware puede ingresar con su usuario desde cualquier equipo de la empresa tanto en la matriz como en la sucursal, además de tener la posibilidad de abrir varias sesiones del sistema al mismo tiempo.	El encargado de hardware puede dejar una sesión abierta en cualquier computador, lo que permite a cualquier usuario que acceda a esta terminal realizar cambios en los perfiles de usuarios y sus permisos, entre otras actividades.	M	Se recomienda que el encargado de hardware no tenga la posibilidad de tener más de una sesión abierta.
No existe en la empresa un procedimiento formal para efectuar las bajas de los empleados del sistema.	Se corre el riesgo que puedan ingresar a las aplicaciones con la clave de los empleados próximos a desvincularse de la empresa.	B	Se sugiere establecer políticas para la administración de cuentas que incluya el procedimiento de desvinculación de personal saliente.
Se observó que no se tiene un control de bloqueo automático en las aplicaciones para los usuarios que tienen varios días de inactividad o se encuentran de vacaciones.	Genera la posibilidad de que alguna persona no autorizada tenga acceso a una cuenta de usuario que no le corresponde, permitiendo ver información sensible o confidencial.	B	Se sugiere inhabilitar estas cuentas cuando entre a un periodo de tiempo determinado o por vacaciones, con esta ultima previa coordinación con el jefe del departamento de recursos humanos.
Se evidenció que en los servidores se encuentran activadas las sesiones de administrador durante las 24 horas del día.	Cualquier persona que consiga ingresar al centro de cómputos podría acceder a los datos y a la configuración de los servidores.	B	Se recomienda usar el usuario administrador en caso que fuera necesario realizar una tarea específica.

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
Autenticación			
Cuando un usuario quiere autenticarse en la aplicación se presenta en el campo de contraseña el caracter asterisco, pero si se da click con el mouse el sistema revela la contraseña ingresada.	La información sensible puede no ser íntegra ni confiable debido a que personal puede ver la contraseñas de otros y tener acceso a los aplicativos para modificación de información o consultas no autorizadas.	A	Se recomienda modificar el aplicativo de manera que no puede revelarse la contraseña al dar click derecho.
Administración de Contraseñas			
Durante la revisión se comprobó que a pesar de tener una cuenta administrador para la base de datos, servidores y redes es una clave universal.	Al no tener una clave universal para cuentas administradores se tiene el riesgo que personal adivine la contraseña y pueda acceder a la información sensible.	A	Se sugiere cambiar las claves de todas las cuentas administradores de manera periódica con un máximo 6 caracteres, incluyendo mayúsculas y símbolos como @#$, a fin de no permitir tener una contraseña universal para acceso a las aplicaciones.
Se evidenció que no se tiene procedimientos para cambios de contraseñas en un determinado periodo de tiempo.	Personal adivine la contraseña y pueda acceder a la información sensible de la empresa.	B	Se sugiere implementar un procedimiento para el cambio de contraseña con lo siguiente: • Expiración de Contraseñas: activación de la configuración de cambio de contraseñas en un periodo de tiempo determinado, en especial para cuentas administradoras o privilegiadas. • Historial de Contraseñas: implementar un mecanismo para permitir un control histórico de contraseñas a fin de impedir ingresar una contraseña anteriormente usada.

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
Se evidenció que la clave en la base de datos del sistema no cumple con la política establecida por el administrador.	Personal adivine la contraseña y pueda acceder a la información sensible de la empresa.	A	Se sugiere cumplir las políticas establecidas para la asignación e ingreso de contraseñas y documentarlas.
Registros de Auditoria			
Se evidenció que no se tiene activados los registros de auditoría de la base de datos, se tiene registros de transacciones de eliminación de factura.	Se dificulta la verificación de las transacciones que se realizan en especial del DBA.	B	Se sugiere establecer políticas de auditoría a nivel de base de datos que contemplen: • Configuración de las pistas de auditoría que se tiene en la base de datos en especial para los usuarios administradores o cuentas superusuario. • Registro de las pistas de auditoría que se generen en el sistema. • Responsable.

5.7. CONCLUSIONES

En el siguiente cuadro se muestra la evaluación por las secciones descritas acorde al alcance definido:

Proceso	Efectividad sobre el objetivo de Control
ADMNISTRACION DE CUENTAS	NO CUMLE
AUTENTICACION DE USUARIOS	NO CUMPLE
ADMINISTRACIÓN DE CONTRASEÑAS	NO CUMPLE
REGISTROS DE AUDITORIA	NO CUMPLE

Como resultado de la auditoría se concluye que los controles internos **NO SON ACEPTABLES,** personal no autorizado puede acceder a las aplicaciones y a los datos que éstas gestionan debido a que no se tienen políticas para roles ni perfiles de usuario, se tienen contraseñas no complejas lo que compromete la confidencialidad, integridad y disponibilidad de la información.

Se debe considerar la implementación de controles aceptables a mediano plazo acorde a la evaluación de la auditoría realizada. Los controles han sido evaluados en base a su diseño y eficiencia.

CAPITULO 6

6. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

6.1. OBJETIVO

Evaluar el procedimiento de adquisición, desarrollo y control de cambios de las aplicaciones; a fin de verificar su correcto funcionamiento en un ambiente de desarrollo y producción adecuado.

6.2. ADQUISICIONES

La organización cuenta con la aplicación adquirida con su respectivo código fuente llamada "SPACE", esta aplicación está desarrollada en lenguaje visual FoxPro bajo una arquitectura cliente-servidor.

La aplicación "ALMACENES CARITO" está compuesta por los siguientes módulos:

Aplicación	Sistema Operativo	Base de Datos	Proceso del Negocio que Soporta	Volumen de transacciones anuales
Módulo de Administración	Linux	MySQL v5.1.55	Administra la organización de la empresa y los números puntos de ventas en las oficinas.	1400000
Módulo de Inventario y Facturación	Linux	MySQL v5.1.55	Administra los productos que se tiene en inventario y se comercializa.	200000
Módulo de Cotizaciones y Pedidos	Linux	MySQL v5.1.55	Cotizaciones a clientes, pedidos de productos de existencia.	34000
Módulo de Clientes y Proveedores	Linux	MySQL v5.1.55	Administra toda la información de cuentas por cobrar o pagar de clientes y proveedores.	10000

Módulo de Contabilidad	Linux	MySQL v5.1.55	Administra toda la información generada de forma independiente como balance general, estado de pérdidas y ganancias y demás estados financieros.	100000
Módulos de Bancos	Linux	MySQL v5.1.55	Control de cuentas bancarias, cheques y otros depósitos.	15000

Se tienen programas básicos como DIM y EXCEL 2007 para manejar la información relacionada con el cumplimento de leyes tributarias.

El software instalado en los computadores no se encuentra licenciado, se tienen licencias solo de Microsoft Office 2003 de los antiguos equipos.

No existen procedimientos para evaluación del aplicativo a adquirir en base a los requerimientos de la empresa.

6.3. DESARROLLO Y CONTROL DE CAMBIOS

No hay estándares definidos o procedimientos a seguir con respecto a la instalación, documentación y actualización de las aplicaciones en los equipos de la empresa. El Gerente de TI realiza una instalación básica y configuración del sistema operativo, actualizar o instalar los sistemas operativos, antivirus y aplicaciones en los computadores.

No se realiza una definición y análisis de requerimientos de los usuarios previamente a la implementación; tampoco existe un modelo conceptual para realizar modificaciones en las aplicaciones.

No existe un cambio de requerimientos formal, para los cambios pequeños se tiene como responsable al encargado de software. Cuando se piden cambios complejos se contrata a la empresa externa que desarrollo el modulo que se desea modificar.

No se tiene un control de cambios en los programas fuentes, la persona encargada de software saca una copia de la carpeta física del código fuente en su computador y realiza los cambios solicitados; una vez realizado el cambio se sube la versión directamente al servidor y/o computadores de los usuarios.

Los cambios de las aplicaciones a producción se realizan en la noche o en la mañana para no afectar el trabajo, se sale del aplicativo en todos los computadores para subir los cambios realizados para luego continuar de manera normal con las operaciones.

Las pruebas de los cambios realizados se colocan en una carpeta física en el computador de la persona encargada de software.

No se tiene un registro y control de aceptación de cambios a las aplicaciones solicitados por el usuario.

El departamento de TI no tiene una separación de infraestructura de desarrollo, pruebas y producción; se tiene un computador común para el desarrollo y ejecución de pruebas.

6.4. MANTENIMIENTO

No se realizan mantenimientos para eliminar archivos temporales; tampoco existen políticas o procedimientos para mantenimiento de aplicaciones y Base de Datos.

Existen programas no autorizados instalados en los equipos de los usuarios, el departamento de T.I. no lleva un control del software instalado en los equipos

No se tiene un registro de los parches o actualizaciones instaladas en el Sistema Operativo y Base de Datos utilizadas en la empresa.

6.5. DEBILIDADES Y RECOMENDACIONES

De la evaluación realizada según la metodología surgen las debilidades encontradas y a corregir y sugerencias a poder implementarse ante la ausencia o falta de los controles.

- **Situaciones o Hallazgo detectado**: Descripción de lo que se encontró en un determinado punto de la evaluación, según las pruebas, procedimientos o técnicas de evaluaciones utilizadas para hacer la revisión; cada una de estas desviaciones es parte importante del documento.
- **Impacto**: descripción del impacto en el negocio si se lleva a materializar la situación encontrada.
- **Nivel de Riesgo**: Evaluación de la auditoría acorde al Anexo B.
- **Recomendaciones:** sugerencias del auditado o del auditor para solucionar las desviaciones reportadas. Casi siempre corresponde una solución para cada una de las causas reportadas.

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
Adquisiciones			
No se tienen licencias de Software instalado como Office 2007 y Windows XP en los equipos de la empresa.	No se tiene soporte o actualizaciones del software no licenciado dentro de la empresa. Al no tener licenciado el software, están expuestos a tener fuertes sanciones legales que pueden ser motivos de encarcelamiento al representante legal de la empresa y multas.	A	Licenciar el software que se tiene en los equipos de la empresa.
No existe un procedimiento para adquisiciones o compra de software de manera formal acorde a los requerimientos de la organización.	Al no evaluar un software que se requiere comprar se pone en riesgo que no cumplan con los requerimientos planteados por el usuario.	M	Se sugiere tener un procedimiento de adquisiciones de software que contemple: • Objetivo por el cual se deba comprar la herramienta. • Análisis costo-beneficio • Justificativo de compra. • Tiempo de garantía • Mantenimiento • Capacitación de la herramienta.

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
Desarrollo y Control de Cambios			
En la entrevista con el Gerente de TI se evidenció que no se tiene un análisis de los requerimientos de los usuarios previamente a la implementación.	Al no tener un análisis de requerimiento puede que no se cumplan con las solicitudes de los usuarios.	B	Se sugiere establecer políticas para la definición de requerimientos dentro de la metodología de desarrollo.
Se evidenció durante la revisión realizada en el departamento de TI no existe un ambiente separado de desarrollo y pruebas, en un computador se hace la implementación y pruebas con el usuario.	Se corre el riesgo de tener errores de procesamiento en la información y fraudes.	A	De ser posible se debe tener un ambiente separado para pruebas y desarrollo, el cual debe contemplar el ambiente de pruebas tenga los requerimientos mínimos como el de producción adicional la instalación solo del release.
Se evidenció que no existen manuales técnicos o manuales de usuario actualizados para el manejo de las aplicaciones que se manejan en la organización.	Operación inadecuada del aplicativo por parte de los usuarios, debido al desconocimiento de funcionalidades.	B	Se sugiere tener documentación actualizada de las aplicaciones: • Manuales de Usuario del Sistema o Módulo. • Manuales Técnicos

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
Se evidenció que no existe un procedimiento para la administración de cambios principales o críticos de la empresa, solo se realizan los cambios sin registrarlos o comunicarlos internamente.	Los cambios críticos no son realizados a tiempos, debido a que no existe un control o prioridad. Al no tener un procedimiento descrito formal para control de cambios, existe el riesgo de que un cambio no difundido o registrado pueda afectar las aplicaciones o interfaces críticas de la organización involucrando la integridad y confiabilidad de los datos.	M	Se recomienda que se tenga un procedimiento de control de cambio, que se tome en cuenta: • Prioridad de Cambios Críticos. • Análisis de la Solicitud del Usuario. • Registro de cambios de requerimientos y verificación de estos por parte de QA antes de llevarlo a producción. • Firma de la persona responsable del cambio y Usuario Final para constancia de conformidad del cambio realizado. • Responsable del cambio.
Durante la revisión se constató que no hay un control de fechas, versiones de los programas fuente y ejecutables, al realizar el cambio se saca una copia de la carpeta donde se modifica el código sin documentarlo y posteriormente se lo envía a producción.	No se garantiza que los programas que se encuentran en el ambiente de producción reflejen los cambios realizados por la persona encargada de software. Al revisar versiones anteriores no se tiene documentado los cambios realizados en esa versión.	M	Se debe realizar control de los cambios del código fuente que contemple los siguientes aspectos: • Definición del número de versiones anteriores de los programas que deben ser almacenadas. • Definición del responsable encargado de la realización de los cambios. • Documentación del código. • Realización de copias de respaldo de las versiones anteriores en dispositivos externos.

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
No existen estándares o procedimientos definidos para la instalación y actualización de las aplicaciones en los equipos	La aplicación instalada puede que no funcione correctamente	B	Se recomienda diseñar estándares y procedimientos para la instalación y actualizaciones de las aplicaciones que se tiene en la organización.
Durante la entrevista se evidenció que no se tiene un procedimiento formal de pase de desarrollo a producción.	Es importante tener definida de forma clara las actividades a realizar debido a que son dos ambientes distintos y el comportamiento del sistema puede no ser el mismo.	B	Se sugiere tener procedimientos o actividades para que las aplicaciones pasen de desarrollo a producción con un responsable.
No existe una documentación de solicitud de cambios, ni registro de aceptación de los usuarios.	No se tiene un historial de cambio realizados en las aplicaciones, ni quien las implementó.	B	Se sugiere establecer un procedimiento que incluya un formato de Solicitudes de Cambios de Usuarios y documento de aceptación de cambio por parte del usuario.
Mantenimiento			
Durante la entrevista realizada Gerente de TI se evidenció que no existe un registro o bitácora de los parches instalados en las aplicaciones, sistemas operativos o base de datos principales.	Al no tener un control de los parches instalados, puede que las aplicaciones o base de datos funcionen de diferente manera en producción o causen errores de ejecución por parches.	M	Se sugiere tener un registro para la actualización de los parches de seguridad que contenga: • Ultimo parche de seguridad instalado en el sistema • Fecha de la instalación • Responsable de la instalación. • Aplicaciones que afecten esta instalación. • Computadores a instalar. • Ubicación física del parche.

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
Existen instalado programas no autorizados en los respectivos puestos de trabajo, a pesar que tienen deshabilitados los dispositivos externos y sin acceso a internet.	La instalación indiscriminada de aplicaciones puede traer problemas en relación a las licencias de los programas y virus.	B	Se recomienda tener como política la notificación al usuario que se encuentra prohibida la instalación de cualquier software en los equipos. Adicional se deben tener medidas de control e infracciones necesarias.
	Pérdida de productividad del empleado y de recursos, debido a que pueden instalarse juegos y otros programas ajenos a la empresa.		Se sugiere que se designe un persona para realizar verificaciones periódicas en los equipos, identificando así los nuevos productos que han sido instalados.
No se realiza un control de eliminación de archivos temporales de los equipos	Se tiene la utilización de recursos físicos como espacio en disco.	B	Se debe tener un procedimiento que de manera periódica se eliminen los archivos temporales de los equipos.

6.6. CONCLUSIONES

En el siguiente cuadro se muestra la evaluación por las secciones descritas acorde al alcance definido:

Proceso	Efectividad sobre el objetivo de Control
ADQUISICIONES	NO CUMPLE
DESARROLLO Y CONTROL DE CAMBIOS	NO CUMPLE
MANTENIMIENTO	NO CUMPLE

Como resultado de la auditoría se concluye que los controles internos **NO SON ACEPTABLES,** el Departamento de TI no cuenta con un ambiente adecuado para el control de cambios y pruebas por lo que surge la dependencia hacia el personal y no se garantiza que los programas que se encuentran en el ambiente de producción reflejen los cambios realizados en los fuentes, esto puede ocasionar errores de procesamiento de información y posibles fraudes. Al no tener licenciados los programas que utiliza el computador para su funcionamiento como el sistema operativo Windows XP puede ser motivo de fuertes sanciones legales que pueden llevar a la cárcel al gerente general y pagar una multa muy alta.

Se debe considerar la implementación de controles aceptables a mediano plazo acorde a la evaluación de la auditoría realizada. Los controles han sido evaluados en base a su diseño y eficiencia.

CAPITULO 7

7. ADMINISTRACIÓN DE REDES

7.1. OBJETIVO

Evaluar la red y comunicaciones que se encuentra implementada para que los programas, datos y equipos estén conectados entre sí; así como el mantenimiento y soporte de la red.

7.2. CONFIGURACIÓN Y DIAGRAMA DE RED

La comunicación entre la matriz y sucursal no se tiene de manera directa, son redes independientes en los dos edificios donde funciona.

Para la matriz y sucursal se tiene la siguiente estructura:

- 01 Switch: para la administración de la red interna, se encuentra conectado el servidor y los computadores de toda la oficina a esta red.
- 01 Router: se tiene para suministro de internet.
- 01 switch: este no se encuentra conectado a nada, se encuentra en el rack como respaldo en caso de fallas o se dañe el principal.

La instalación del cableado fue realizada de forma práctica por la persona encargada de hardware, es decir no se tuvo un asesoramiento técnico; adicional no se tiene diagrama de los puntos de red que se tienen en la oficina matriz o sucursal. Al instalar los puntos de red se tomó en cuenta de no pasar por los cables de corriente eléctrica para no provocar interferencias, daños o cortes.

No se tiene una descripción formal de la configuración de la red, tampoco se tiene un diseño estructural de la misma; sin embargo la red se encuentra configurada de tal manera que los usuarios solo pueden tener acceso a la información y los recursos que el administrador le asigne.

Para la conexión de red entre los computadores utilizan una red de área local (LAN) se tiene una arquitectura cliente servidor, de esta manera se comparten recursos.

Se utiliza una red Ethernet para proporcionar una velocidad mayor en la transferencia de datos entre 10 y 100Mbps. El protocolo que se utiliza es el TCP/IP por medio de este se asigna a los equipos la dirección IP en un rango de determinado.

FALLAS EN LA RED

Cuando hay un corte de luz se deja de trabajar online, se enciende el generador de energía, mientras tanto las cajas continúan facturando manualmente.

En caso de falla de red por los equipos, se tiene considerado de igual manera facturar de forma manual y una vez restaurado el sistema las facturas o cobros realizados son ingresados.

Cuando un usuario por medio de la aplicación está realizando una operación y si se desconecta o falla la red se pierde los paquetes de datos enviados, se debe realizar nuevamente la operación una vez habilitada la red.

7.3. POLÍTICAS DE MANTENIMIENTO Y SOPORTE DE RED

No se tiene políticas para mantenimiento, uso y soporte de la re, el encargado de la red no realiza un estudio de escalabilidad al momento de colocar un recurso.

7.4. FIREWALL

El firewall utilizado en la empresa es el que viene instalado en el sistema operativo Ubuntu. El ufw está habilitado y configurado por defecto, aceptando todas las conexiones salientes y rechazando todas las conexiones entrantes.

Se tiene restricción para mensajería instantánea (Microsoft Messenger, aMSN, yahoo).

7.5. ANTIVIRUS

Los computadores personales tienen instalado la versión actual del software antivirus instalado AVG gratuita; las actualizaciones del antivirus son bajadas de forma automática por el internet y por control del departamento de TI, en el caso de los equipos que no tiene acceso a internet el encargado de Hardware realiza las actualizaciones de manera manual.

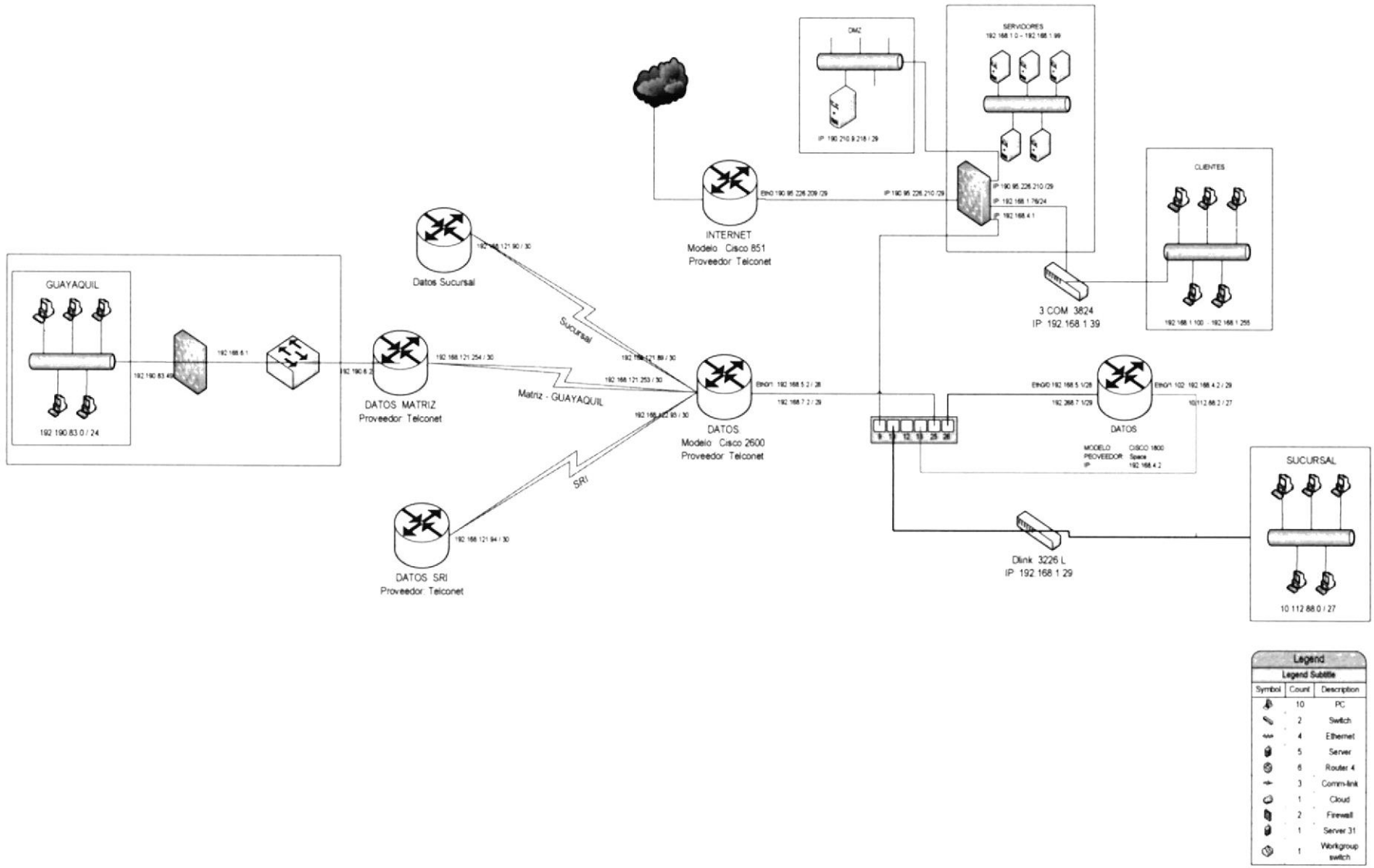
Se realizan escaneos periódicos buscando virus en los servidores y computadores de la oficina principal y sucursal; sin embargo no se realizan escaneos para la base de datos y redes de sistema. Se han tenido problemas de virus en la sucursal llegando a infectar la base de datos y red del edificio.

Cuando se sospecha de una infección o el software antivirus señale que existe una infección, el usuario debe comunicar inmediatamente al departamento TI.

7.6. MONITOREO DE LA RED

El departamento de TI no dispone de herramientas destinadas exclusivamente para prevenir o monitorear la red, el encargado de hardware no realiza un monitoreo de tráfico de la red, intentos de acceso a recursos no autorizados por usuarios.

No hay un control con respecto a la negación de servicios para el tráfico de la red, cantidad de archivos abiertos y cantidad de usuarios conectados.


DMZ
IP 190.210.9.218 / 29
SERVIDORES
192.168.1.0 - 192.168.1.99
CLIENTES
192.168.1.100 - 192.168.1.255
INTERNET
Modelo Cisco 851
Proveedor Telconet
Eth0 190.95.226.209 /29
IP 190.95.226.210 /29
IP 190.95.226.210 /29
IP 192.168.1.76/24
IP 192.168.4.1
3 COM 3824
IP 192.168.1.39
Datos Sucursal
192.168.121.90 / 30
Sucursal
192.168.121.89 / 30
GUAYAQUIL
192.190.83.0 / 24
192.168.6.1
192.190.83.49
192.190.6.2
DATOS MATRIZ
Proveedor Telconet
192.168.121.254 / 30
192.168.121.253 / 30
Matriz - GUAYAQUIL
192.168.121.93 / 30
DATOS
Modelo Cisco 2600
Proveedor Telconet
Eth0/1 192.168.5.2 / 28
192.168.7.2 / 29
Eth0/0 192.168.5.1/28
192.168.7.1/29
Eth0/1.102 192.168.4.2 / 29
10.112.88.2 / 27
DATOS
MODELO CISCO 1800
PROVEEDOR Speca
IP 192.168.4.2
SRI
192.168.121.94 / 30
DATOS SRI
Proveedor Telconet
Dlink 3226 L
IP 192.168.1.29
SUCURSAL
10.112.88.0 / 27
Legend
Legend Subtitle
Symbol
Count
Description
10 PC
2 Switch
4 Ethernet
5 Server
6 Router 4
3 Comm-link
1 Cloud
2 Firewall
1 Server 31
1 Workgroup switch

7.7. DEBILIDADES Y RECOMENDACIONES

De la evaluación realizada según la metodología surgen las debilidades encontradas y a corregir y sugerencias a poder implementarse ante la ausencia o falta de los controles.

- **Situaciones o Hallazgo detectado**: Descripción de lo que se encontró en un determinado punto de la evaluación, según las pruebas, procedimientos o técnicas de evaluaciones utilizadas para hacer la revisión; cada una de estas desviaciones es parte importante del documento.
- **Impacto**: descripción del impacto en el negocio si se lleva a materializar la situación encontrada.
- **Nivel de Riesgo**: Evaluación de la auditoría acorde al Anexo B.
- **Recomendaciones:** sugerencias del auditado o del auditor para solucionar las desviaciones reportadas. Casi siempre corresponde una solución para cada una de las causas reportadas.

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
Configuración y Diagrama de red			
En la actualidad no se cuenta con un diagrama de configuración de redes ni de cómo se encuentra diseñada.	Crecimiento desordenado de la red. No se tiene una ubicación exacta de los equipos en la red	B	Se debe de realizar un esquema del diagrama de configuración de red y como está diseñada
Políticas y procedimientos de mantenimiento y soporte de la red			
No se tiene políticas o procedimientos formales para la planificación de los mantenimientos de la red.	Deterioro de equipos y canales de comunicación.	A	Establecer un plan de mantenimiento y niveles de soporte de la red, que contemple: • Limpieza de los componentes. • Ordenamiento de la red. • Actualización de software de los dispositivos de red. • Reparaciones o cambios de elementos del canal de comunicación. • Responsable • Periodicidad
No se tiene una lista de IP disponible de la red.	Al no tener una lista de IP el encargado de la red no tiene conocimiento que equipo tiene asignada una determinada IP o que IP se encuentra disponible en la red.	B	Se recomienda realizar una lista de IP de la red y a qué equipo se encuentra asignado.

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
Monitoreo			
No se tiene herramientas destinadas para el monitoreo de la red.	Intentos de accesos no autorizados y amenazas de intrusos en la red.	M	Se recomienda realizar un monitoreo de la red donde se contemple: • Verificación de detección de Intrusos. • Negación de Servicios • Sniffing • Responsable
Antivirus			
No se tiene procedimientos formales en caso de que los equipos se infecten de virus.	Al no tener un procedimiento para la eliminación de virus puede que no se elimine el virus completamente del equipo y pueda contagiar a los demás por medio de la red.	M	Establecer procedimientos a seguir en caso que se encuentre un virus en el sistema, verificando: • Escaneo de Disco Duro. • Dispositivos de entrada para saber fuente de virus. • Determinar la fuente. • Comprobar si se eliminó completamente el virus.
Se evidenció que el antivirus instalado no se encuentra licenciado.	Limitaciones en el software por ser una versión gratuita.	A	Se recomienda tener una versión licenciada del antivirus para una protección del equipo y redes de manera optima.

7.8. CONCLUSIONES

En el siguiente cuadro se muestra la evaluación por las secciones descritas acorde al alcance definido:

Proceso	Efectividad sobre el objetivo de Control
CONFIGURACION Y DIAGRAMA DE RED	NO CUMPLE
POLITICAS Y PROCEDIMIENTOS DE MANTENIMIENTO Y SOPORTE DE RED	NO CUMPLE
ANTIVIRUS	NO CUMPLE
MONITOREO	NO CUMPLE

Como resultado de la auditoría se concluye que los controles internos **NO SON ACEPTABLES,** la red implementada funcionan pero no se tiene un control en la configuración y mantenimiento de equipos conectados generando una exposición a la disponibilidad a los recursos.

Se debe considerar la implementación de controles aceptables a corto plazo acorde a la evaluación de la auditoría realizada. Los controles han sido evaluados en base a su diseño y eficiencia.

CAPITULO 8

8. ADMINISTRACIÓN DE BASE DE DATOS

8.1. OBJETIVO

Evaluar la integridad, confiabilidad y disponibilidad de la información y estructura de la base de datos, a fin de que funcione correctamente y no alteren los procedimientos de la empresa.

8.2. DESCRIPCION DE LA BASE DE DATOS

La base de datos que manejan esta creada en MySQL versión 5.1.55, es una base de datos relacional multiusuario que almacena 50 millones de registros, la base de datos que utiliza la aplicación se llama SPACE en esta se almacena toda la información de las ventas, facturación, control de empleados, para acceder a ella hay una clave universal y se encuentra a cargo del Gerente de TI.

No se tiene el diseño del modelo entidad relación de la base de datos que utilizan los aplicativos, tampoco se tiene un estándar ni una descripción del diseño de tablas o nomenclatura utilizada de la base de datos.

No existe un control de acceso a los datos críticos de las aplicaciones de la empresa, el personal puede visualizar la información ingresada a la base de datos por ejemplo las contraseñas de los usuarios por no estar encriptadas.

Las únicas personas que pueden tener acceso a los archivos de la base de datos son el administrador y todo aquel que opere el servidor de aplicaciones (es decir las personas que tengan acceso físico al equipo).

Cuando algún usuario elimina una transacción por medio del aplicativo, los registros de la base de datos no se borran físicamente sino que son marcados como borrados, esto quiere decir que se realiza una eliminación lógica. De esta forma siempre permanecen los registros de las transacciones realizadas y que usuario realizó la acción, sin embargo no se tienen un registro desde que computador se realizó la operación.

No se realiza un monitoreo constante de los recursos utilizados por la base de datos en el servidor

El encargado de los respaldos de la base de datos realiza la restauración de la en el servidor ubicado en la oficina matriz del respaldo generado en la sucursal, de forma que se tiene un compilado de toda la información.

Cuando se realiza el respaldo a la base de datos se revisa que se genere el archivo del respaldo, pero no se realizan pruebas para saber si los datos se respaldaron correctamente.

8.3. DEBILIDADES Y RECOMENDACIONES

De la evaluación realizada según la metodología surgen las debilidades encontradas y a corregir y sugerencias a poder implementarse ante la ausencia o falta de los controles.

- **Situaciones o Hallazgo detectado**: Descripción de lo que se encontró en un determinado punto de la evaluación, según las pruebas, procedimientos o técnicas de evaluaciones utilizadas para hacer la revisión; cada una de estas desviaciones es parte importante del documento.
- **Impacto**: descripción del impacto en el negocio si se lleva a materializar la situación encontrada.
- **Nivel de Riesgo**: Evaluación de la auditoría acorde al Anexo B.
- **Recomendaciones:** sugerencias del auditado o del auditor para solucionar las desviaciones reportadas. Casi siempre corresponde una solución para cada una de las causas reportadas.

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
Diccionario de datos			
Se constató que no existe un diccionario de datos.	La persona encarga de realizar los cambios en la estructura de la BD o modificaciones de los aplicativos se tardará más de los previstos al no tener una descripción formal del diccionario de datos.	B	Se recomienda que se diseñe un diccionario de datos que contemple: • Descripción de las Entidades • Características de las Entidades. • Relación entre entidades
Se constató que no se tiene estándares para la creación de tablas y campos en la base.	Al no tener estándares definidos se dificulta la modificación o desarrollo de las aplicaciones.	B	Definir estándares para la creación de tablas y campos.
Estructura de la Base de Datos			
Se verificó que no se tiene un diseño de diagrama de E-R de la base de datos.	No se tiene conocimiento de las tablas relacionadas y tipo de relación, esto puede dificultar el manejo de la base de datos.	B	Se sugiere realizar el diseño del diagrama E-R con sus respectivas entidades y relaciones.
Monitoreo y Desempeño			
No se realiza un Monitoreo constante de los recursos utilizados por la base de datos en el Servidor.	Caídas y lentitud permanente durante el procesamiento de transacciones. Inadecuada capacidad del equipo donde se encuentra instalada la base de datos.	B	Establecer monitoreos constantes en base: • Espacio disponible en la BD • Espacio de Memoria • Espacio de disco duro • Nivel de procesamiento del servidor.

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
Permisos a Nivel de Base de Datos			
Se evidenció que la administración de la base de datos la realizan 2 personas: el Gerente de TI y el asistente; cualquiera de los dos puede realizar actualizaciones, consultas, inserción y eliminación de la información; adicional pueden realizar modificaciones en la estructura de la base.	Al no estar definidas formalmente las funciones del personal de TI no se tiene un control de las actividades realizadas en la BD, pudiendo afectar la integridad y confiabilidad de la información.	A	Definir un manual de funciones y responsabilidades del personal del departamento de TI El departamento de TI debe activar los registros de auditoría y designar una persona que sea la encargada de administrar la base de datos y de resguardar la información que en ella se almacena.
Se evidenció que las claves de los usuarios almacenadas en la base de datos no se encuentran encriptados.	Al no tener encriptadas las claves existe el riesgo que personal no autorizado tenga acceso a la información confidencial.	A	Se debe implementar mecanismos de encriptación para las contraseñas almacenadas en la base de datos.
Cambios a la información y Niveles de aprobación.			
No se tiene un control de cambios definidos formalmente, cada vez que necesitan realizar un cambio el gerente de TI o el asistente pueden realizar los cambios según la necesidad que tengan en ese momento.	Se tiene el riesgo de que se realicen cambios inadecuados a la base de datos lo que puede ocasionar fraude, puede afectar los diferentes módulos existentes.	A	Se recomienda definir una metodología para una buena administración de cambios que contemple: • Solicitud del cambio. • Niveles de Autorización del cambio. • Responsable del Cambio

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
Disponibilidad de Respaldos			
Se constató que los respaldos no se están realizando correctamente en el Virtual Box debido a que al hacer la auditoría se solicito el respaldo del 22 de Agosto y no se encontró el respaldo correspondiente.	En caso de falla a los servidores o a la base de datos, el encargado no podría realizar una restauración de la misma al no tener disponibilidad de la información.	A	Se debe realizar una verificación y prueba diaria de los respaldos al realizarlos.

8.4. CONCLUSIONES

En el siguiente cuadro se muestra la evaluación por las secciones descritas acorde al alcance definido:

Proceso	Efectividad sobre el objetivo de Control
CUMPLIMIENTO DE LOS ESTANDARES DEFINIDOS PARA EL DICCIONARIO DE DATOS	NO CUMPLE
DISEÑO DE LA ESTRUCTURA DE LA BASE DE DATOS	NO CUMPLE
PERMISOS A NIVEL DE BASE DE DATOS	NO CUMPLE
CAMBIOS A LA INFORMACION Y NIVELES DE APROBACION	NO CUMPLE
DISPONIBILIDAD DE RESPALDOS	NO CUMPLE

Como resultado de la auditoría se concluye que los controles internos **NO SON ACEPTABLES,** debido a que se atenta con la integridad, confiabilidad y disponibilidad de la información al poder añadir datos no validos o eliminar información relevante para la empresa atentando contra la continuidad del negocio y exponiéndola a posibles fraudes.

Se debe considerar la implementación de controles aceptables a corto plazo acorde a la evaluación de la auditoría realizada. Los controles han sido evaluados en base a su diseño y eficiencia.

CAPITULO 9

9. ADMINISTRACIÓN DE OPERACIONES

9.1. OBJETIVO

Evaluar la organización de las operaciones dentro del departamento de TI, la asignación de tareas, rendimiento de los recursos y respaldos de la información; a fin de tener un ambiente adecuado.

9.2. ADMINISTRACIÓN DE OPERACIÓN DEL DEPARTAMENTO DE TI

El centro de cómputo no cuenta con procedimientos formales de operaciones realizadas por el departamento de TI, no se tiene una metodología para el manejo diario de actividades.

Una de las tareas del área de operaciones es el soporte de usuarios en la matriz y sucursal de la empresa, cuando se presenta un problema el usuario notifica al departamento de TI para que personal disponible revise el incidente reportado.

Existe una planificación anual que la realiza el Gerente de TI y es aprobado por el Gerente General de la empresa; para las actividades diarias no existen coordinaciones entre el personal.

9.3. SEGREGACION DE FUNCIONES

En el departamento de TI no se tiene designaciones de tareas de manera formal, un empleado puede realizar la totalidad de una actividad que puede iniciar desde la solicitud de un cambio, modificar el código fuente, realizar las pruebas y puesta en producción, por lo que no existiría un verificación real del cambio.

No existe una persona encargada de la seguridad de la información dentro de la organización.

9.4. CAPACIDAD DE ALMACENAMIENTO Y RENDIMIENTO

No se tiene un control de almacenamiento y rendimiento para:

- Transacciones almacenadas en la base de datos para verificar si existe un desbordamiento de datos.
- Fallas que se produzca o tiempos de respuesta en los aplicativos.
- Cuellos de botella en la red o pérdidas de comunicaciones.
- Tiempo de respuesta de los equipos para verificar rendimiento y espacio disponible.

9.5. POLÍTICAS DE RESPALDO

El Gerente de TI es el encargado de realizar los respaldos, se tiene tres formas el manejo de los respaldos: disco duro externo, DVD y VirtualBox; los respaldos realizados en el disco duro y DVDs se encuentran en la misma oficina donde se encuentran los servidores en la principal y en la sucursal.

El VitrtualBox ha sido configurado de tal manera que los respaldos se ejecutan automáticamente, esta información se mantiene durante 15 días en el contenedor luego de este tiempo se reinicia.

Se tiene un quemador de DVD conectado directamente al servidor que realiza las copias de manera automática, se debe tener precaución al efectuar los respaldos por este medio debido a que si se encuentra lleno el DVD se borra automáticamente y se carga la información del día.

El respaldo de la base de datos se realiza 2 veces en el día: una al medio día y a la media noche, ambos son copias completas a la base de datos y sin encriptación.

El disco duro externo que se lo tiene para respaldos es de 1 TeraByte, se encuentra conectado directamente al servidor de aplicaciones para la obtención automática del respaldo. En este disco se tiene los respaldos históricos realizados por carpetas de la oficina matriz y sucursal.

El departamento de TI no verifica si se han realizado correctamente los respaldos hechos, adicional no se ejecutan pruebas de recuperación total o parciales periódicamente.

Los respaldos de los computadores de cada usuario se realizan en la compartición lógica que se tiene en su mismo equipo.

9.6. DEBILIDADES Y RECOMENDACIONES

De la evaluación realizada según la metodología surgen las debilidades encontradas y a corregir y sugerencias a poder implementarse ante la ausencia o falta de los controles.

- **Situaciones o Hallazgo detectado**: Descripción de lo que se encontró en un determinado punto de la evaluación, según las pruebas, procedimientos o técnicas de evaluaciones utilizadas para hacer la revisión; cada una de estas desviaciones es parte importante del documento.
- **Impacto**: descripción del impacto en el negocio si se lleva a materializar la situación encontrada.
- **Nivel de Riesgo**: Evaluación de la auditoría acorde al Anexo B.
- **Recomendaciones:** sugerencias del auditado o del auditor para solucionar las desviaciones reportadas. Casi siempre corresponde una solución para cada una de las causas reportadas.

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
Segregación de Funciones			
Se evidenció durante la revisión realizada en el departamento de TI no se tiene una segregación de funciones adecuada debido a que el mismo encargado es quien diseña, desarrolla y prueba con el usuario.	Al no haber responsabilidades puntuales asignadas a cada empleado puede generarse duplicación de tareas, lo que genera una pérdida de productividad.	A	Se recomienda tener una definición de funciones para los diferentes roles que se tiene en el departamento de TI.
No existe un empleado designado como responsable de la seguridad y manejo de incidentes de la información.	Al no tener una persona encargada de la seguridad de la información la integridad, confiablidad y operatividad de la misma puede ser alterada en forma intencional o accidental por fallas de los equipos, software o acción de un virus informático.	A	Se sugiere tener un empleado a cargo de la seguridad del sistema que tenga funciones de coordinación de las tareas de seguridad y cumplimiento de las políticas dentro de la organización. El encargado de la seguridad de la información no debe ser parte del departamento de TI y garantizar la independencia necesaria respecto de las áreas usuarias.
Capacidad de Almacenamiento y Rendimiento			
No se tiene un control de almacenamiento y rendimiento a nivel de equipos, aplicativos, redes y base de datos.	• Desbordamiento de datos. • Fallas y tiempos de respuesta en los aplicativos. • Cuellos de botella en la red. • Pérdidas de comunicaciones en la red.	M	Se recomienda medir la capacidad de los equipos y servidores a nivel de memoria, procesador y espacio en disco.

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
	• Alto Tiempo de respuesta de un equipo.		
Administración de Operaciones			
No se encuentran documentados formalmente los procedimientos de las operaciones realizadas por el departamento de TI ni metodología para el manejo diario de actividades.	Al no tener los procedimientos o una metodología de trabajo, una tarea puede tardar más tiempo en ejecutarse.	B	Se sugiere documentar los procedimientos y diseñar metodologías para las operaciones diarias del departamento. Se recomienda realizar planificaciones de actividades de manera periódica asignándole a cada tarea un responsable, tiempo de ejecución y recurso necesario para su cumplimiento; adicional se debe tener una verificación y evaluación del cumplimiento de estas planificaciones.
Políticas de Respaldos			
Se realizan respaldos de los archivos de cada usuario en los propios computadores en una partición lógica.	Al realizar un respaldo en el mismo computador original no tiene garantía en caso de daño de la partición del disco duro.	B	Se sugiere a los usuarios tener habilitados dispositivos para la realización de respaldo de información sensible de la empresa. Se debe tener una carpeta encriptada en el servidor para guarda los respaldos no compartidos para los demás usuarios.

Hallazgo	Impacto	Nivel de Riesgo	Recomendación
No existe un procedimiento formal para la generación, restauración y prueba de los respaldos.	Puede afectar la integridad y disponibilidad de la información al querer restaurar la base de datos, ya que no se realizan pruebas de que los respaldos se hayan generado correctamente.	A	Se sugiere que exista un procedimiento escrito y formal de política de respaldo, que contenga las recomendaciones : • Responsable de la generación de las copias de seguridad, restauración y prueba. Los respaldos deben ser probados para verificar que se hayan realizado correctamente. • Descripción del procedimiento de generación de respaldo.
	Puede afectar directamente a la continuidad del negocio		• Los archivos de respaldo deberían tener una contraseña que los proteja ya que contienen información confidencial.
Se realizan respaldos de los archivos de cada usuario en los propios computadores en una partición lógica.	Al realizar un respaldo en el mismo computador original no tiene garantía en caso de daño de la partición del disco duro.	B	Se sugiere a los usuarios tener habilitados dispositivos para la realización de respaldo de información sensible de la empresa. Se debe tener una carpeta encriptada en el servidor para guarda los respaldos no compartidos para los demás usuarios.
No se tienen un control para manejo de medios de almacenamiento, en ocaciones sino se cambia el disco (DVD) se borra la información respaldada.	Pérdida de información si no se cambia el DVD o en caso de que exista un desperfecto en el medio de almacenamiento y fallen los otros medios de respaldos	B	Se sugiere llevar un control sobre el manejo de medios de almacenamiento ya que el disco (DVD) es más vulnerable a daños.

9.7. CONCLUSIONES

En el siguiente cuadro se muestra la evaluación por las secciones descritas acorde al alcance definido:

Proceso	Efectividad sobre el objetivo de Control
SEGREGACION DE FUNCIONES	NO CUMPLE
ADMINISTRACION DE LAS OPERACIONES DEL DEPARTAMENTO DE TI	CUMPLE
CAPACIDAD DE ALMACENAMIENTO Y RENDIMIENTO	NO CUMPLE
POLITICAS DE RESPALDOS	NO CUMPLE

Como resultado de la auditoría se concluye que los controles internos **NO SON ACEPTABLES,** se pudo identificar que la mayoría de los controles para la administración del centro de cómputo no se cumplen debido a que no se tiene una separación de funciones entre el personal por lo que se podría generar una duplicidad de tareas y no hay un responsable directo en caso de problemas, ni se tiene una política de respaldo formal en caso que se necesite restaurar la base de datos no existiría la disponibilidad de información de la base de datos.

Se debe considerar la implementación de controles aceptables a mediano plazo acorde a la evaluación de la auditoría realizada. Los controles han sido evaluados en base a su diseño y eficiencia.

ANEXO A: ENTREVISTAS REALIZADAS

ADMINISTRACION Y ORGANIZACIÓN DE TI

Fecha: 12 de Agosto 2011

Entrevistado: Gerente de TI

Item	Pregunta	SI	NO	N/A	Observaciones
1	Existe una adecuada separación de funciones dentro del sector Control de Datos, bibliotecas de archivos, control impreso, montaje de trabajo?		X		
2	El organigrama funcional es adecuado para el tamaño del área?		X		
3	Se han definido políticas y procedimientos para cada una de las actividades del departamento de TI.		X		
4	Se desarrollan regularmente planes a corto, mediano o largo plazo que apoyen el logro de la misión y las metas generales de la organización?		X		
5	Durante el proceso de planificación, se presta adecuada atención al plan estratégico de la empresa?		X		
6	¿Las tareas y actividades en el plan tiene la correspondiente y adecuada asignación de recursos?		X		
7	¿Existen estándares de funcionamiento y procedimientos y descripciones de puestos de trabajo adecuados y actualizados?		X		
8	Existe un Plan de Trabajo que especifique tiempos, recursos, metas?		X		
9	Existe algún procedimiento para el personal que se incorpora en el departamento?		X		

Item	Pregunta	SI	NO	N/A	Observaciones
10	Los proyectos son previamente analizados y aprobados por la Gerencia?	X			

ADMINISTRACION DE LA SEGURIDAD

Fecha: 22 de Agosto 2011

Entrevistado: Gerente de TI

Mantenimiento de Software

Mantenimiento de Hardware

Item	Pregunta	SI	NO	N/A	Observaciones
SEGURIDAD LOGICA					
1	¿Existen controles, procedimientos y estándares de seguridad de acceso?	X			Pero no de manera formal
2	¿Se encuentran documentadas las obligaciones y funciones del personal del Departamento?		X		
3	Se han implantado contraseñas para garantizar la operación de la consola y equipo central al personal autorizado?	X			Pero son claves universales que puede una personal fácilmente adivinar.
4	Existe una persona responsable de asignar los perfiles y roles de usuario para acceder a las aplicaciones?	X			El encargado es el Gerente de TI.
5	En los sistemas están habilitadas para todas las cuentas de usuario las opciones que permiten establecer:				
	a. Un período máximo de vigencia de las contraseñas		X		La contraseña que se asigna al inicio en el sistema nunca la cambia el usuario, no hay esa opción.
	b. Un número máximo de intentos de conexión.		X		El sistema no valida intento inválidos por conexión
6	¿Existen procedimientos de asignación y distribución de contraseñas?	X			

Item	Pregunta	SI	NO	N/A	Observaciones
7	¿Los derechos de acceso concedidos a los usuarios son los necesarios y suficientes para el ejercicio de las funciones que tienen encomendadas?	X			
8	¿El sistema de autenticación de usuarios guarda las contraseñas encriptados?		X		Se pueden leer las contraseñas del personal en las tablas de la base de datos.
9	El usuario tiene conocimiento de una selección para selección y uso de contraseña de forma apropiada?(Ej: tenga máximo 6 caracteres, incluyendo min y símbolos @#$)	X			
10	¿Se verifican que los controles de acceso de cada aplicación funcionan de manera correcta?	X			
11	¿Dentro del sistema para conceder derechos de acceso son autorizadas por el dueño del proceso?		X		Es acorde a las funciones que realiza el encargado asigna acceso y perfil.
12	Se bloquea al tercer intento fallido para el acceso a los diferentes recursos?		X		
13	¿Se encarga alguien de verificar el registro de log de los intentos fallidos?		X		
14	¿Se desactivan las cuentas de las personas que se encuentran fuera de la organización por largo tiempo?		X		
15	¿Después de cuánto tiempo se dan de baja las cuentas de las personas que salen de la organización?				
16	¿Se verifica que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro? (autenticación)		X		

Item	Pregunta	SI	NO	N/A	Observaciones
17	El departamento de TI revisa periódicamente los derechos de acceso de los usuarios utilizando un proceso formal? Ej: Privilegios especiales cada 3 meses, normales cada 6 meses		X		
18	Se desactivan las cuentas genéricas para el acceso a las aplicaciones o/y DB?	X			
19	Se adopta la política de escritorios limpios para los documentos y medio de almacenamiento removibles?	X			
20	Se debe tener la política de bloqueo automático del computador en caso de estar inhabilitada por un periodo determinado?	X			Se tiene que se deshabilite con un periodo de inactividad de 15 minutos.
21	Se tienen restringido los recursos compartidos entre aplicaciones?	X			
22	Existen señales de alarma cuando se violan las políticas de seguridad implementadas en el sistema?		X		Existen log que se generan en el servidor y en la base, pero señales de alarmas no hay.
23	Se tienen restringidos los horarios de conexión a los usuarios?		X		El personal puede conectarse en cualquier momento sea en horas laborables o no, adicional puede dejar la sesión activa.
24	Las cuentas genéricas son usadas solo bajo circunstancias excepcionales, adicional se tiene cuentas de mantenimiento?	X			
25	Se restringe y controla el uso de programas utilitarios que podría superar al sistema y controles de la aplicación?	X			Se encontraron programas no autorizados instalados en los computadores.

Item	Pregunta	SI	NO	N/A	Observaciones
SEGURIDAD FISICA					
26	Existe controles biométrico o que tipos de seguridades como puertas de ingreso controlado para el acceso a las instalaciones sólo el acceso al personal autorizado?		X		
27	¿Existe un documento de autorización para el acceso al centro de cómputo?		X		
28	Se registra el acceso al centro de cómputo de personas ajenas?		X		
29	Se ha instruido al personal de sistemas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?	X			No se tiene un procedimiento formal, pero se tiene prohibido el ingreso de personal no autorizado.
30	¿Existe una persona responsable de la seguridad?		X		
31	Se controla el trabajo fuera de horario establecido, en especial cuando realizan horas extras?		X		
32	Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de la puerta del centro de cómputo		X		
33	Existe control de seguridad a terceros que está trabajando en un área segura (Ej: Personal no autorizado que ingresa al centro de cómputo, se lo acompaña en todo momento durante su visita)?		X		
34	Se retira los pases de empleado y de visita cuando se retiran de la institución?			X	
35	Existen políticas o procedimientos para el acceso físico y lógico a áreas seguras y centro de cómputo?		X		

Item	Pregunta	SI	NO	N/A	Observaciones
36	Existe una políticas para comidas, bebidas y no fumar cerca de los servicios de procesamiento de información?		X		
37	Existe un lugar destinado para el centro de computo (equipo de redes y servidores)?	X			Este lugar encuentra dentro de la oficina de la persona encargada del software, sin un gabinete cerrado con llave.
38	El centro de datos se encuentra aislado del acceso externo del edificio?		X		Se encuentra en el tercer piso de la matriz
39	Existe un sistema de acondicionamiento de aire apropiado en en centro de cómputo?	X			
40	Existen controles para minimización de riesgo de vibraciones, agua. Explosivos, fuego, radiación electromagnética, etc.?		X		
41	Se tienen extintores manuales de incendio dentro del centro de cómputo?		X		No se tienen el área extintores.
42	La ubicación de cada extintor está señalizada de tal forma que permite una fácil localización?		X		
43	Existen contratos de seguros de equipos actualizados, en especial para los activos críticos?		X		
44	Se tiene en el centro de cómputo cámaras de video para la vigilancia del departamento.		X		Se ha realizado varias veces la propuesta a gerencia pero no ha visto un costo - beneficio para dar el visto bueno.

Item	Pregunta	SI	NO	N/A	Observaciones
45	Existen políticas o procedimientos para el traslado de equipos o medios de almacenamiento fuera de las instalaciones (mantenimientos programados o visitas a otras instalaciones)?		X		No se tiene un procedimiento formal, pero se debe comunicar al jefe del departamento en caso de sacar un equipo fuera del área.
46	El mantenimiento es realizado solo por personal autorizado?		X		Se tienen una persona externa para los mantenimientos de los computadores (cada dos meses).
47	El cableado de energía y telecomunicaciones que llevan datos o sostienen los servicios de información son protegidos de la intercepción o daño?		X		Se ha instalado en forma empírica la red del sistema.
48	Los equipos se encuentra protegido con un sistema eléctrico backup, protector o supresor de picos eléctricos y otras interrupciones causadas por fallas en los servicios públicos?		X		Solo los computadores de escritorio tienen protección UPS
49	Las líneas de potencia se encuentran aterrizadas?		X		
50	Se tienen auditorias regulares para verificación de rotación o movimientos de activos de forma no autorizada?		X		El usuario asignado al equipo es el único responsable del activo.
51	Se tiene responsables asignados para la configuraciones de los equipos y hardware?	X			La persona encargada del Hardware es la que realiza las configuraciones básica del mismo, para lo demás se lo tiene a personal externo.

Item	Pregunta	SI	NO	N/A	Observaciones
52	Se tiene un inventario de activos importantes de cada sistema de información?		X		Se carece de un inventario físico de los activos de la información.
53	El centro de cómputo cuenta con diagramas físicos, eléctricos, de redes a la mano en forma física y digital?		X		

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTOS DE APLICACIONES

Fecha: 19 de Agosto 2011

Entrevistado: Mantenimiento de Software

Item	Pregunta	SI	NO	N/A	Observaciones
ADQUISICION					
1	Las aplicaciones desarrolladas o compradas por terceros cumplen con los requisitos de seguridad establecidos en la organización?		X		
2	¿Están identificados el software original y copia?		X		No de manera de listado pero se tiene conocimiento que el software que se tiene no es original.
3	Los programas que usan para el desarrollo son originales?		X		
4	Existe algún procedimiento para la adquisición de equipos.		X		Simplemente se llama a la persona externa para una cotización de un equipo.
5	Se tiene procedimientos o políticas la adquisición de actualizaciones de determinados paquetes de software?		X		
DESARROLLO Y CONTROL DE CAMBIOS					
6	El departamento de TI tiene implementado una metodología de software para el desarrollo de un proyecto?		X		
7	¿Se tiene documentados y actualizados todos los procedimientos de desarrollo?		X		
8	Se cumplen las políticas y estándares de programación definido		X		Debido a que no se tiene procedimientos.

Item	Pregunta	SI	NO	N/A	Observaciones
9	¿Existen manuales de usuario y manuales técnicos actualizados de los diferentes sistemas?		X		De manera parcial.
10	Se tiene los registros de la solicitud, cambios realizado y responsables de los cambios?		X		Se realizan los cambios de forma empírica sin ningún registro de la solicitud o aceptación
11	Se tiene separada la infraestructura de desarrollo, pruebas y producción para reducir el acceso no autorizado?		X		Desarrollo y pruebas se lo realiza en un mismo computador
12	Existe validaciones para los datos de entrada y salida de los sistemas para asegurar que son los correctos y apropiados?		X		Se lo realiza cada mes de manera manual se comparan los datos
13	Se realizan transacciones previamente ingresadas para verificar la validez de los resultados y comprobar validaciones?	X			Se lo realiza cada tres meses de manera manual se comparan los datos.
14	Existe un control apropiado para la detección ante posibles errores de procesamientos en las aplicaciones?		X		
15	Existen herramientas automatizadas y manuales para comprobar desbordamientos, SQL, etc.		X		
16	Existe un control criptográfico para información sensible de la organización? Ej: contraseñas, información sensible que se transmite en la red?		X		
17	Las pruebas de las aplicaciones se realiza con bancos de pruebas diseñados?		X		
18	Se tiene restringido el manejo del código fuente y el ambiente de desarrollo al personal?		X		

Item	Pregunta	SI	NO	N/A	Observaciones
19	Existen procedimientos definidos de puesta en producción de los sistemas, se realiza en horas no laborables?		X		No se tienen procedimientos definidos pero la puesto a producción se realizada antes de iniciar o finalizar la jornada laboral.
20	Se tiene un procedimiento de control de cambio establecido en la organización para el desarrollo o actualización de los sistemas?		X		Se realizan cambios a los fuentes acorde se necesite en el momento, pero no se tiene un control o procedimiento especifico solo la persona encargada sabe del cambio realizado.
21	Existe una evaluación del software a utilizar, considerando temas como interfaces, capacidad de trabajar en red, capacidad multiplataforma, entre otros?		X		
22	Se realiza un análisis de requerimientos y definición del problema?		X		
23	Se realiza un estudio de factibilidad del proyecto?	X			
24	Se establece un diseño del sistema en donde se incluye el modelo lógico, fisico y conceptual?		X		
25	Se llevan a cabo pruebas adecuadas durante el desarrollo y aceptación del sistema?	X			
26	Se deja evidencia de la aceptación del Usuario del sistema modificado o realizado?		X		
27	La alta Gerencia participa y revisa las aplicaciones desarrolladas?		X		
28	Los Usuarios participan en la fase de desarrollo de los sistemas?		X		

Item	Pregunta	SI	NO	N/A	Observaciones
29	¿El personal de área de desarrollo cuenta con la formación adecuada y son motivados para la realización de su trabajo?		X		
30	Se tienen sincronizados los relojes de todos los sistemas de procesamientos de información dentro de la organización?	X			Se graba toda la información con respecto a la fecha del servidor.
31	Se tiene un control y monitoreo de la información que maneja y desarrolla el personal subcontratado por la organización?		X		
MANTENIMIENTO					
32	Se lleva un registro de las fallas tanto de hardware como de software?			X	
33	Se realizan verificaciones a nivel de aplicativo cuando se cambia de sistema operativos en las computadores de escritorio?		X		
34	¿Existe una lista del software que utilizan en la organización?		X		

ADMINISTRACION DE RED

Fecha: 24 de Agosto 2011

Entrevistado: Mantenimiento de Hardware

Item	Pregunta	SI	NO	N/A	Observaciones
1	¿Existen registros de pruebas de compatibilidad de programas realizados en sedes remotas?		X		
2	¿Existen autorizaciones según el rol para desarrollar y modificar a los programas?		X		Solo se tiene de manera informal que cualquier cambio lo realiza el Gerente de TI.
3	Existe documentación completa de las configuraciones de las redes y sus esquemas dentro de la organización. (IP de cada equipo, configuraciones de router, personal encargado)?	X			Se lo tiene de manera informal, pero no se tienen diagramas de redes ni inventario de equipos.
4	¿Existe un proceso formal de control de distribución de los programas?		X		
5	¿Se dispone de un calendario de estos procesos automáticos?		X		Solo se tienen configurado los de respaldo.
6	¿Existen políticas para la administración de redes tanto en la matriz como en la sucursal?	X			Pero no de manera formal.
7	Existen procedimientos y responsable para la administración remota de los equipos?	X			El Gerente de TI es el responsable
8	¿Existe un proceso formal de ingreso de equipos a la red?				
9	¿Existe un ente encargado de dar manejar incidentes en la red?		X		No se realiza ningún tipo de verificación de red.
10	¿Las políticas establecidas están respaldadas por los directivos?			X	No hay políticas establecidas
11	¿Existe dominio en la red o se trabaja por grupos de trabajos?	X			

Item	Pregunta	SI	NO	N/A	Observaciones
12	¿Existe software especializado para monitoreo de la red?		X		
13	¿Existe registro de actualizaciones de equipos de red?		X		
14	¿La red inalámbrica esta habilitada con DHCP?			X	No se tiene una red inalámbrica
15	¿existe un Registro de log del sistema: Tanto de transacciones correctas e incorrectas?	X			
16	¿Se realizan transacciones previamente ingresadas para verificar la validez de los resultados y comprobar validaciones?	X			
17	Se manejan reportes de las alertas enviadas por el sistema?			X	No se tienen alertas del sistema, solo registro o log de transacciones.
18	Se Verificar plan de contingencia para transacciones realizadas?			X	
19	Existe procedimientos y responsable para la administración remota de equipos?	X			
20	Existe un registro de Log para lo referente a Firewall, Internet y Dominio?		X		
21	Revisión de contratos de servicios de terceros para redes de datos?			X	
PROTECCION CONTRA VIRUS					
22	¿Existen procedimientos para los archivos ejecutables o programas bajados?		X		
23	Se verifica el trafico de la red en busca de virus como por ejemplo: Email, Archivos adjuntos, FTP, etc ?		X		
24	¿Existen controles de detección, prevención y recuperación para protegerse de código malicioso (antivirus).	X			Se tiene instalado el AVS en versión gratuita.

Item	Pregunta	SI	NO	N/A	Observaciones
25	¿Existen políticas de actualización de antivirus, e activación periódica en las versiones instaladas en los computadores de los usuarios?		X		Se tienen activación periódica de las computadores, en caso de no tener acceso a internet los computadores existe responsables que lo realizan semanalmente. Pero no se tienen políticas formales.
26	Se verifican que los computadores de la organización se encuentre con la base de virus actualizada y licenciado?		X		Todo el software instalado no es licenciado.

ADMINISTRACION DE BASE DE DATOS

Fecha: 26 de Agosto 2011

Entrevistado: Gerente de TI

Mantenimiento de Software

Item	Pregunta	SI	NO	N/A	Observaciones
1	Tienen un DBMS y un administrador de la base de datos?	X			Se tiene la base de datos en MySQL versión 5.1.55.
2	Existen controles o procedimientos que identifiquen redundancia de datos?	X			
3	Se cuenta con un Diccionario de Datos?		X		
4	Se utiliza software que apoye a la seguridad de la Base de Datos?		X		
5	¿Está documentada la estructura y funcionamiento de la base de datos?		X		
7	Las funciones del DBA están debidamente detalladas y documentadas?		X		
8	Las Bases de Datos están diseñadas para Usuarios Múltiples?	X			
9	Tienen un servidor de base de datos?	X			La base de datos se encuentra en el servidor de aplicaciones.
10	Existen estándares para el diseño de la base de datos y su diccionario?		X		
11	Se realiza un monitoreo de los recursos utilizados por la Base de Datos en el servidor?		X		

Item	Pregunta	SI	NO	N/A	Observaciones
12	¿Existe un registro de acceso a los datos y transacciones realizadas?	X			Se tiene un registro en la base por usuario y tipo de acción realizada, sin embargo no se registra desde que computador realiza la operación.
13	Los datos son cargados correctamente a la interfaz grafica de la aplicación por la cual es utilizada?	X			
14	¿Existe personal restringido que tenga acceso a la base de datos?	X			Sin embargo la clave del administrador es una clave no compleja.
15	¿Existen logs que permitan tener pistas sobre las acciones realizadas sobre los objetos de la base de datos?	X			
16	Si existen estos logs:				
	a. Se usan los logs generados por el DBMS	X			
	b. Se usan los generados por el Sistema Operativo	X			Se tiene activados los log en el servidor
	c. Se han configurado estos logs para que solo almacenen la información relevante.		X		
	d. Se tiene un sistema de registro de acciones propio con fines de auditoría.		X		
17	¿Se verifica que el respaldo se haya realizado correctamente?		X		Solo se realiza el respaldo en cualquier dispositivo establecido.
18	¿El sistema administrador de base de datos depende de los servicios que ofrece el SO?		X		

Item	Pregunta	SI	NO	N/A	Observaciones
19	¿Cada qué tiempo se realizan los respaldos de la base de datos y en que dispositivo de almacenamiento se realiza ?	X			Se realiza 2 veces en el día: una al medio día y a la media noche, disco duro externo que funciona como respaldo es de 1 Terabyte.
20	¿Esta verificación se la realiza con transacciones reales?		X		
21	¿se realizan auditorias periódicas para los dispositivos de almacenamiento?		X		

ADMINISTRACION DE OPERACIONES

Fecha: 16 de Agosto 2011

Entrevistado: Gerente de TI

Mantenimiento de Software

Mantenimiento de Hardware

Item	Pregunta	SI	NO	N/A	Observaciones
1	Se tiene procedimientos descritos actualizados para la realización de operaciones dentro de la empresa como procesos bath?		X		
2	El software que se tiene instalado en los computadores se encuentra licenciado?		X		Ningún software se encuentra licenciado en la organización
3	El departamento de TI maneja los procesos bajos normas de internacionalmente reconocidas?		X		
4	Existe una segregación de funciones a niveles de autorización de cambios y de procedimientos?		X		
5	Existe una segregación de funciones para el desarrollo y pruebas del sistema?		X		
6	Existe una políticas para el uso del internet dentro de la organización?	X			
7	El departamento de TI revisa regularmente el cumplimento de las políticas del uso del internet?		X		
8	Existe la capacidad de monitoreo para el procesamiento y almacenamiento de los sistemas (Ej: Monitoreo de espacio en disco, RAM. CPU, servidores críticos)?	X			Se tiene en el servidor instalado un programa para el manejo de esto.
9	Existen evaluaciones periódicas al personal que nos presta un servicio crítico?		X		

Item	Pregunta	SI	NO	N/A	Observaciones
10	Existen criterios formales de aceptación de sistemas para actualizaciones y nuevas versiones para hacer cumplir los requerimientos por los que fue solicitado?		X		
11	Se encuentran claros y registrados los contratos de servicios de TI (SLA) y niveles de servicios que se proporciona por parte de terceros?			X	
12	Se revisa regularmente estos acuerdos de niveles de servicios?		X		No se tienen contratos firmados para tecnología en la organización.
13	Se tiene políticas para el uso de dispositivos externos como pen driver, DVD, CD, discos externos?	X			Se tienen deshabilitados los puertos USB del computador, no se tienen DVD o CD ROM en los computadores del personal.
14	Existe un procedimiento para la manipulación y control de los dispositivos externos?		X		
15	Existen procedimientos formales descritos para el manejo de eComerce de manera segura?			X	No se realiza comercio electrónico en la organización.
RESPALDO					
22	Existen procedimientos de respaldos para las aplicaciones y datos sensibles de la organización (tiempo y esquema)?	X			Los respaldos son por tres métodos: DVD, Disco Duro Externo y Virtual Box.
23	Existe un responsable asignado o convenios de respaldo con terceros?	X			El Gerente de TI es el que realiza los respaldos de información.

Item	Pregunta	SI	NO	N/A	Observaciones
24	Los respaldos realizados son probados diariamente?		X		Se realizan las copias pero no la comprobación de la copia.
25	Se tiene etiquetado de forma correcta e inventariado los dispositivos que son utilizados para respaldos?			X	
26	Se tiene el concepto de Encriptación de Copias de seguridad y archivos que contengan datos sensibles?	X			
27	Se envían fuera de la matriz o edificio central los dispositivos que son utilizado para respaldo?	X			Con el Virtual Box una copia de respaldo de los últimos 15 días
28	Existe una política de salida o copia de datos desde los equipos de escritorios de los usuarios de la organización?	X			

ANEXO B: EVALUACION DE LA AUDITORIA Y DEL INFORME DE LA AUDITORÍA

Evaluación de auditoria	Descripción
Alta	Elevado impacto negativo sobre el negocio. Se debe poner inmediatamente en conocimiento de la dirección.
Media	Impacto medio sobre el negocio. La dirección deberá tomar medidas a corto o mediano plazo.
Baja	La dirección deberá tomar medidas a mediano o largo plazo.

ANEXO C: INFORME DE AUDITORIA REALIZADA AL CENTRO DE COMPUTO

ENTIDAD: ALMACENES CARITO

FECHA DE CORTE: SEPTIEMBRE/2011

I. RESUMEN EJECUTIVO

Producto de la visita efectuada a la empresa con la finalidad de evaluar el diseño y eficacia de los controles generales implementados dentro del centro de computo en el área de desarrollo, base de datos, seguridad, redes y operaciones, se considera que controles **NO SON ACEPTABLES** lo cual representa un alto riesgo para:

- La administración del ambiente y acceso al centro de cómputo por personal no autorizado.
- Acceso a las aplicaciones, base de datos y redes mediante asignación de perfiles de usuario.
- Administración para control de cambios y pruebas de las aplicaciones existentes en el ambiente de producción.
- Disponibilidad de los recursos compartidos de red.
- Integridad, confiabilidad y disponibilidad de la información
- Operatividad en la administración del Centro de Cómputo

En el siguiente cuadro se muestra la evaluación por áreas:

Proceso	Efectividad sobre el objetivo de Control
ADMINISTRACION DE LA SEGURIDAD FISICA	NO CUMPLE
ADMINISTRACION DE LA SEGURIDAD LOGICA	NO CUMPLE
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	NO CUMPLE
ADMINISTRACION DE REDES	NO CUMPLE
ADMINISTRACION DE BASE DE DATOS	NO CUMPLE
ADMINISTRACION DE OPERACIONES	NO CUMPLE

Se debe considerar la implementación de controles aceptables a mediano plazo acorde a la evaluación de la auditoría realizada. Los controles han sido evaluados en base a su diseño y eficiencia.

II. PRINCIPALES HALLAZGOS Y RECOMENDACIONES.

Los hallazgos descritos a continuación son los considerados los más críticos para la empresa, debido a que pueden tener un impacto negativo dentro de la organización; esto se realizó en base a la evaluación de nivel de riesgos descritos en el anexo A.

1. ADMINISTRACION DE LA SEGURIDAD FÍSICA

1.1. ACCESO FÍSICO AL CENTRO DE CÓMPUTO

1.1.1. EL departamento de TI no tiene políticas o procedimientos formales para el acceso de personal interno o externo al centro de cómputo.

Recomendación:

- El departamento de TI debe establecer políticas de acceso al centro de cómputo para personal, a fin de restringir el acceso a personal no autorizado que pueda atentar con la integridad de la información.

1.1.2. Los servidores de Aplicación y Base de datos, y de Internet se encuentran ubicados en una pequeña mesa dentro de la oficina del Gerente de TI, atentando con la integridad, confiabilidad y disponibilidad de la información.

1.1.3. Personal no autorizado puede ingresar a la oficina del Gerente de TI sin ninguna restricción, debido a que en ocasiones el Gerente abandona su oficina para atender un llamado técnico.

Recomendación:

- Es conveniente que el área donde se encuentran los servidores, el switch central y demás equipamiento tecnológico crítico tenga una medida de seguridad extra, por medio del cual solo se permita el acceso a los administradores, para esto se sugiere destinar un área de la empresa que sea exclusiva para ubicar estos equipos.

- La gerencia de TI debe de implementar políticas para el acceso de personal interno y externo no autorizado en el centro de cómputo.

1.2. AMBIENTE DEL CENTRO DE CÓMPUTO

1.1.4. No se tiene instalado extintores en el centro de cómputo, a pesar de que se pudo observar que hay extintores en el primero y segundo piso; se corre el riesgo de que se produzca un incendio al ser una empresa que vende productos altamente inflamables como las telas puede dañarse o perderse los equipos informáticos y la información que contienen.

Recomendación:

- Se debe implementar planes y mecanismos para la prevención de incendios.

1.3. CONTROL DE ACCESO A EQUIPOS

1.1.5. Una empresa externa realizó la instalación y configuración de los servidores por lo que el departamento de TI no tiene una descripción de las configuraciones de los servidores, en caso de falla puede tener una interrupción de las operaciones críticas de la organización.

Recomendación:

- El departamento de TI debe tener implementar una política o procedimiento para la restauración de las configuraciones del servidor, en este se debe incluir:
  - Descripción técnica de los servidores utilizados en la matriz y sucursal.
  - Configuración a nivel de Hardware y Software.
  - Responsable de estas actualizaciones

1.1.6. La empresa no tiene un plan de contingencia formal, en caso de haber una falla en los servidores el Gerente de TI utiliza su computador como servidor alterno teniendo el riesgo de no tener los aplicativos 100% operativos o con dificultades en su ejecución.

Recomendación:

- El departamento de TI debe desarrollar un plan de contingencia básico en caso de que falle el servidor principal, en este se debe incluir:
  - Plan de respaldo: contramedidas necesarias durante la materialización de una amenaza.
  - Plan de emergencia. Contempla las contramedidas necesarias durante la materialización de una amenaza.
  - Plan de recuperación. Contempla las medidas necesarias después de materializada y controlada la amenaza.
  - Responsable/ Persona que lo reportó

- La empresa debe tener un equipo de similares características para en caso de falla del servidor principal se realice en este equipo el levantamiento de los servicios críticos de la empresa.

2. ADMINISTRACIÓN DE LA SEGURIDAD LÓGICA

2.1. ADMINISTRACION DE USUARIOS

2.1.1. El personal de departamento de TI tiene activado el acceso de todas las opciones del sistema y la base de datos, lo que permite ver toda la información de la organización aumentando el riesgo de cometer errores o posibles fraudes.

Recomendación:

- Se debe designar un solo responsable para la base de datos y aplicativos para que desempeñe el rol de administrador, a fin de no tener más de una persona con privilegios totales dentro de estas aéreas.

- Se recomienda limitar los acceso al personal del departamento de TI por roles para tener permisos solo opciones acorde sus actividades designadas acorde a la definición de funciones.

2.1.2. El departamento de TI no tiene políticas o procedimientos formales para la creación de cuentas de usuarios en los aplicativos y base de datos; no se lleva a cabo una revisión periódica ni control sobre las cuentas de los usuarios o permisos que se tienen asignados. Esto posibilita que por error o negligencia la cuenta o los permisos de algún usuario sean modificados, permitiendo a usuarios no habilitados accedan a información sensible de la empresa.

Recomendación:

- Se sugiere establecer políticas para la creación de cuentas de usuario que incluyan:
  - Perfil de Usuario
  - Modificaciones de cuentas
  - Des-habilitación de cuentas.
  - Responsable de los cambios

- Se recomienda realizar un control de las cuentas de usuarios de manera periódica, que contenga:
  - Se encuentren activas solo las cuentas en uso.
  - Nivel de permisos que los usuarios poseen sobre los mismos.

- Las contraseñas se cambien periódicamente

2.1.3. El departamento de TI no tiene una lista de control de acceso de los usuarios a las aplicaciones, base de datos y redes.

Recomendación:

- Se sugiere realizar una lista de acceso de los usuarios que se tienen a nivel de aplicación, base de datos y redes, a fin de tener un control de que personal autorizado tenga acceso a los recurso y aplicaciones de la empresa.

2.1.4. El encargado de hardware puede ingresar con su usuario desde cualquier equipo de la organización tanto de la matriz como de la principal sin restricciones de apertura de sesiones, esto puede permitir a un usuario atentar a la integridad y confiabilidad de la información si tiene acceso al equipo con la sesión abierta de administrador.

Recomendación:

- Se recomienda que se limiten las sesiones administradores y no se tenga la posibilidad de tener más de una sesión abierta tanto en la matriz como en la sucursal.

2.2. AUTENTICACIÓN

2.2.1. Cuando un usuario quiere autenticarse en la aplicación se presenta en el campo de contraseña el caracter asterisco, pero si se da click con el mouse el sistema revela la contraseña ingresada.

Recomendación:

- Se recomienda modificar el aplicativo de manera que no se puede revelar la contraseña al dar click derecho sobre el campo de contraseñas.

2.3. ADMINISTRACIÓN DE CONTRASEÑAS

2.3.1. Las contraseñas de cuentas administradores para la base de datos, servidores y redes son claves universales, el usuario puede adivinar la contraseña y acceder a información sensible atentando contra la integridad y disponibilidad de la información.

Recomendación:

- El departamento de TI dentro de sus política de cambios de contraseñas debe incluir el cambio periódico de claves para cuentas administradores con

un máximo de 6 caracteres incluyendo una combinación de mayúsculas, minúsculas y símbolos como @#&$, a fin de no permitir tener una contraseña universal para acceso a las aplicaciones, adicional que se cambien de manera periódica las contraseñas.

2.3.2. El departamento de TI no realiza una verificación de las contraseñas que se tiene cumplan con las políticas establecidas por el administrador.

Recomendación:

- El departamento de TI debe tener un control sobre las políticas establecidas para la asignación e ingreso de contraseñas; adicional se debe documentarlas y divulgarlas al personal de la empresa.

3. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS

3.1. Adquisiciones

3.1.1. Los computadores de la empresa tienen instalados programas sin licenciamiento como el sistema operativo y paquete office, al no tener licenciado el software están expuestos a tener fuertes sanciones legales que pueden ser motivos de encarcelamiento del representante legal de la empresa y generar multas para la empresa.

Recomendación:

- El departamento de TI debe gestionar el Licenciamiento del software que se tiene en los equipos de la empresa

3.1.2. Las aplicaciones utilizadas en la empresa son desarrollada por personal externo, sin embargo no tiene un procedimiento para las adquisiciones de software, a fin de comprar software que se ajusten a los requerimientos o necesidades del negocio.

Recomendación:

- El departamento de TI con Gerencia General debe implementar un procedimiento para las adquisiciones de paquetes informáticos, que contemple:
  - Objetivo por el cual se deba comprar la herramienta.
  - Análisis Costo-Beneficio.
  - Justificativo de compra.

- Tiempo de garantía.
- Costo y Tipos de Mantenimiento
- Ayuda en línea o capacitación de la herramienta.

3.2. Desarrollo y Control de Cambios

3.2.1. Durante la revisión realizada en el departamento de TI no existe un ambiente separado de desarrollo y pruebas, en un computador se hace la implementación y pruebas con el usuario, con esto se corre el riesgo de tener errores de procesamiento en la información y fraudes.

Recomendación:

- Se debe tener un ambiente separado para pruebas y desarrollo, el cual debe contemplar el ambiente de pruebas tenga los requerimientos mínimos como el de producción.

3.2.2. El departamento de TI no tiene un procedimiento para la administración de cambios en especial para cambios críticos de la empresa, el encargado de software realiza el cambio sin llevar un registro lo cual puede afectar a otras aplicaciones o interfaces críticas involucrando la integridad y confiabilidad de los datos.

Recomendación:

- El departamento de TI debe tener una política de control de cambios en especial para procedimientos críticos, que incluya:
  - Prioridad de Cambios Críticos.
  - Análisis de la Solicitud del Usuario.
  - Registro de cambios de requerimientos y verificación de estos por parte de QA antes de llevarlo a producción.
  - Firma de la persona responsable del cambio y Usuario Final para constancia de conformidad del cambio realizado.
  - Responsable del Cambio

3.2.3. El departamento de TI no lleva un control de versiones de programas fuentes y ejecutables de los aplicativos, al realizar un cambio se saca una copia de la carpeta donde se modifica el código sin documentarlo y posteriormente se lo envía a producción por lo que no garantiza si reflejen los cambios realizados.

Recomendación:

- El departamento de TI debe implementar un control para los cambios al código fuente que se incluya:

- Definición del número de versiones anteriores de los programas que deben ser almacenadas.
- Definición del responsable encargado de la realización de los cambios.
- Documentación del código.
- Realización de copias de respaldo de las versiones anteriores en dispositivos externos.

3.3. Mantenimiento

3.3.1. El departamento de TI no tiene un registro o bitácora de los parches instalados en las aplicaciones, sistemas operativos o base de datos principales, al no tener conocimiento del parche instalado puede que cause errores en la ejecución de los aplicativos.

Recomendación:

- Se recomienda tener un registro de las actualizaciones de los parches de seguridad que contenga:
  - Descripción del último parche de seguridad instalado en le sistema
  - Fecha de la instalación
  - Responsable de la instalación
  - Aplicaciones que afecten esta instalación
  - Computadores a instalar
  - Ubicación física del Parche

4. ADMINISTRACIÓN DE REDES

4.1. Políticas y procedimientos de mantenimiento y soporte de la red

4.1.1. El departamento de TI no cuenta con políticas o procedimientos formales para la planificación de los mantenimientos y soporte de la red, lo que puede ocasionar un deterioro de equipos y canales de comunicación.

Recomendación:

- El departamento de TI debe establecer un plan de mantenimiento de soporte de la red que tenga:
  - Limpieza de los componentes
  - Ordenamiento de la red
  - Actualización del Software de los dispositivos de la red
  - Reparaciones o cambios de los elementos de comunicación

- Responsable
- Periodicidad

4.2. Monitoreo

4.2.1. El departamento de TI no tiene herramientas destinadas para el control y monitoreo de la red de la empresa tanto para la matriz y sucursal.

Recomendación:

- Se recomienda establecer políticas para el control y monitoreo de la red que incluya:
  - Verificación de detección de intrusos
  - Negación de los servicios
  - Sniffing
  - Responsable

4.3. Antivirus

4.3.1. El departamento de TI no tiene procedimientos formales en caso de que los equipos se infecten de virus, lo que puede afectar a la integridad de la información.

Recomendación:

- Establecer procedimientos a seguir en caso que se encuentre un virus en el sistema, verificando:
  - Escaneo de Disco Duro.
  - Dispositivos de entrada para saber fuente de virus.
  - Determinar la fuente.
  - Comprobar si se eliminó completamente el virus.

4.3.2. Se evidenció que el antivirus instalado no se encuentra licenciado, por lo que se tiene limitaciones en el software por ser una versión gratuita.

Recomendación:

- Se recomienda tener una versión licenciada del antivirus para una protección del equipo y redes de manera óptima.

5. ADMINISTRACION DE BASE DE DATOS

5.1. Perfiles de Usuarios

5.1.1. La administración de la base de datos la realizan 2 personas: el Gerente de TI y el asistente; cualquiera de los dos puede realizar actualizaciones, consultas, inserción y eliminación de la información; adicional pueden realizar modificaciones en la estructura de la base. Al no estar definidas formalmente las funciones del personal de TI no se tiene un control de las actividades realizadas en la BD, pudiendo afectar la integridad y confiabilidad de la información.

Recomendación:

- Definir un manual de funciones y responsabilidades del personal del departamento de TI, en donde se describan todas las actividades que deben desarrollarse para el buen desempeño del personal en la ejecución de sus labores.

- El departamento de TI debe activar los registros de auditoría y designar una persona que sea la encargada de administrar la base de datos y de resguardar la información que en ella se almacena.

5.1.2. Las claves de los usuarios almacenadas en la bese de datos no se encuentran encriptadas y existe el riesgo que personal no autorizado tenga acceso a la información confidencial.

Recomendación:

- Se debe implementar mecanismos de encriptación para las contraseñas almacenadas en la base de datos.

5.2. Cambios a la información y Niveles de aprobación.

5.2.1. No se tiene un control de cambios definidos formalmente, cada vez que necesitan realizar un cambio el gerente de TI o el asistente pueden realizar los cambios en la base de datos según la necesidad que tengan en ese momento, al realizar cambios inadecuados a la base de datos y niveles de aprobación es que afectar el funcionamiento de los diferentes módulos existentes o posibilidad fraude.

Recomendación:

- Se recomienda que el Departamento de TI defina una metodología para una buena administración de cambios que incluya:

- Solicitud del cambio.
- Niveles de Autorización del cambio.
- Responsable del Cambio

5.3. Disponibilidad de Respaldos

5.3.1. No se está realizando correctamente los respaldos en la herramienta Virtual Box debido a que el respaldo solicitado del 22 de Agosto no se encontraba completo en el contenedor, esto lleva el riesgo de no tener disponibilidad de la información al momento de tener una falla en el servidor.

Recomendación:

- El departamento de TI dentro de sus políticas de respaldos se debe incluir una verificación y prueba diaria de los respaldos realizados, adicional se debe tener una verificación de las configuraciones de la herramienta Virtual Box.

6. ADMINISTRACION DE OPERACIONES

6.1. Segregación de Funciones

6.1.1. Durante la revisión realizada en el departamento de TI no se tiene una segregación de funciones adecuada debido a que el mismo encargado es quien diseña, desarrolla y prueba con el usuario. Al no haber responsabilidades puntuales asignadas a cada empleado puede generarse duplicación de tareas, lo que genera una pérdida de productividad.

Recomendación:

- Se recomienda que el departamento de TI debe establecer una definición de funciones para los diferentes roles.

6.1.2. No existe un empleado designado como responsable de la seguridad y manejo de incidentes de la información. La integridad, confiablidad y operatividad de la misma puede ser alterada en forma intencional o accidental por fallas de los equipos, software o acción de un virus informático.

Recomendación:

- Se sugiere tener un empleado a cargo de la seguridad del sistema que tenga funciones de coordinación de las tareas de seguridad y cumplimiento de las políticas que se implementen en la organización.

- El encargado de la seguridad de la información no debe ser parte del departamento de TI para garantizar la independencia necesaria respecto de las áreas usuarias.

6.2. Capacidad de Almacenamiento y Rendimiento

6.2.1. No se tiene un control de almacenamiento y rendimiento a nivel de equipos, aplicativos, redes y base de datos. Se puede presentar lo siguiente

- Desbordamiento de datos.
- Fallas y tiempos de respuesta en los aplicativos.
- Cuellos de botella en la red.
- Pérdidas de comunicaciones en la red.
- Alto Tiempo de respuesta de un equipo.

Recomendación:

- El departamento de TI debe establecer políticas para la medición de la capacidad de los equipos y servidores a nivel de memoria, procesador y espacio en disco.

6.3. Políticas de respaldos

6.3.1. No existe un procedimiento formal para la generación, restauración y prueba de los respaldos, esto puede afectar la integridad y disponibilidad de la información al querer restaurar la base de datos, ya que no se realizan pruebas de que los respaldos se hayan generado correctamente.

Recomendación:

- El departamento de TI debe definir un procedimiento escrito y formal de política de respaldo, que contenga las recomendaciones:
  - Responsable de la generación de las copias de seguridad, restauración y prueba.
  - Los respaldos deben ser probados para verificar que se hayan realizado correctamente.
  - Descripción del procedimiento de generación de respaldo.
  - Los archivos de respaldo deberían tener una contraseña que los proteja ya que contienen información confidencial.