Universidad de Costa Rica

Sistema de Estudios de Postgrado

Programa de Postgrado en Administración de Empresas

Trabajo Final de Graduación para optar al grado de Maestría

Profesional en Auditoría de Tecnologías de Información

Auditoría de Tecnologías de Información en Corporación Arrocera Costa Rica S.A.

Manfred Hernández Villalobos

2007

"A Dios, a mis padres, mi hermano y todas las personas y empresas que han hecho posible la realización de este sueño tan importante para mi vida profesional"

Agradecimientos

Quiero realizar un agradecimiento especial a la Corporación Arrocera Costa Rica S.A. por permitirme realizar mi trabajo final de graduación en tan distinguida empresa, en especial a sus colaboradores Lic. Manuel Arroyo Vargas, Ing. Norberll A. Carmona Rodríguez y Lic. Gerardo Díaz Alvarado.

A PricewaterhouseCoopers, Costa Rica, por creer en mí y suministrarme todas las facilidades y herramientas necesarias para poder concluir este proyecto, en especial a Lic. Oscar Piedra Cordero y MARI Alejandro Campos Sánchez.

Adicionalmente quiero agradecer a mi tutor y amigo MATI Sergio Espinoza Guido, quien ha servido de inspiración y apoyo a lo largo no solo de este proyecto, sino de toda mi carrera profesional hasta la fecha.

En general a toda mi familia y amigos, por su voz de aliento y apoyo incondicional,

Gracias.

Hoja de aprobación

Este Trabajo Final de Graduación fue aceptado por la Comisión del Programa de Postgrado en Administración y Dirección de Empresas, de la Universidad de Costa Rica, como requisito parcial para optar al grado de Magíster con énfasis en Auditoría de Tecnologías de Información.

_____	_____
Msc. Aníbal Barquero Chacón	MATI Sergio Espinoza Guido
Director Programa de Maestría	Profesor Coordinador
_____	_____
MARI Alejandro Campos Sánchez	Lic. Manuel Arroyo Vargas
Lector Guía	Supervisor Laboral

_____

Lic. Manfred Hernández Villalobos
Estudiante

Contenido

Auditoría de Tecnologías de Información en Corporación Arrocera Costa Rica S.A.

Índice de anexos complementarios

Índice de siglas y abreviaturas

ATI	Auditoría de Tecnologías de Información
CACSA	Corporación Arrocera Costa Rica S.A.
CGTI	Controles Generales de Tecnologías de Información
MADE	Maestría en Administración y Dirección de Empresas
MARI	Maestría en Administración de Recursos Informáticos
MATI	Maestría en Auditoría de Tecnología de Información
TI	Tecnologías de Información
UCR	Universidad de Costa Rica

Resumen

Hernández Villalobos, Manfred
Auditoría de Tecnologías de Información en Corporación Arrocera Costa Rica S.A.
Programa de Postgrado en Administración y Dirección de Empresas. –San José, C.R.:
M.Hernández.,2007.
59 h. : il. – 15 refs.

El objetivo general del trabajo es realizar una auditoría sobre los Controles Generales de Tecnologías de Información en la empresa Corporación Arrocera Costa Rica S.A. con el fin de detectar áreas potenciales de mejora, mediante la implementación de una metodología de auditoría basada en los conocimientos adquiridos durante el plan de estudio de la Maestría en Auditoría de Tecnologías de Información.

La Corporación Arrocera Costa Rica S.A., se dedica a la comercialización de arroz a nivel nacional.

Este proyecto de investigación pretende realizar una práctica profesional de auditoría de tecnología de información, mediante la auditoría de los controles generales de tecnología de información.

Dentro de sus principales conclusiones se puede decir que existen varios aspectos de mejora en las actividades de controles generales de tecnología de información en las áreas de operaciones computacionales, acceso a programas y datos, además de cambios y desarrollo de programas.

Con base en todo lo anterior, se recomienda que se establezca un plan de acción de corrección para los aspectos de mejora detectados, con el fin que se puedan establecer prioridades de implementación a corto plazo.

Palabras clave:
Auditoría, Tecnología, Información, Arroz, Corporación, Industria Arrocera, Controles, Evaluación, Riesgo

Director de la investigación:
MATI Sergio Espinoza Guido

Unidad Académica:
Maestría en Auditoría de Tecnologías de Información
Programa de Postgrado en Administración y Dirección de Empresas
Sistema de Estudios de Postgrado

Introducción

La Auditoría de Tecnologías de Información (ATI) como se le conoce contemporáneamente (también conocida como Auditoría de Sistemas), ha tomado gran auge alrededor del mundo como una actividad multidisciplinaria que reúne gran cantidad de conocimientos, que responden a la acelerada evolución de la tecnología informática en los últimos tiempos.

En respuesta al avance tecnológico, muchas empresas han decidido confiar sus operaciones de negocio (tanto relacionales como de toma de decisiones) como herramientas de apoyo vital para el cumplimiento de objetivos y metas, tanto en el sector público como privado, en la medida en que la información es considerada un activo tan o más importante que cualquier otro en una organización.

De tal manera existe un cuerpo de conocimientos, normas, técnicas y buenas prácticas dedicadas a la evaluación y aseguramiento de la calidad, seguridad, razonabilidad, y disponibilidad de la información tratada y almacenada a través del computador y equipos afines, así como de la eficiencia, eficacia y economía con que la administración de una organización están manejando dicha información y todos los recursos físicos y humanos asociados para su adquisición, captura, procesamiento, transmisión, distribución, uso y almacenamiento. Todo lo anterior con el objetivo de emitir una opinión o juicio, para lo cual se aplican técnicas de auditoría de general aceptación y conocimiento técnico específico.

En función de retribuir y poner en práctica los conocimientos adquiridos durante el programa de estudio de esta maestría, se realizará una ATI en la empresa Corporación Arrocera Costa Rica S.A. donde apoyado por un conjunto de conocimientos profundos acerca de la tecnología informática, de técnicas y procedimientos de auditoría y de conocimientos contables suficientes, para evaluar la calidad, fiabilidad y seguridad del entorno informático, así como brindar seguridad razonable acerca de la utilidad de la información almacenada y procesada en ellos, con el fin de emitir un juicio al respecto.

Se pretende enfatizar el trabajo Auditoría de Tecnologías de Información en la Corporación Arrocera Costa Rica S.A., en el departamento de Tecnologías de Información enfocado en la revisión específica de Controles Generales de Tecnología de Información para las actividades de operaciones computarizadas, cambios de los programas, accesos a los programas y datos, además de desarrollo de programas, ya que estás áreas engloban el ambiente de control interno relacionado con las tecnologías de información y su relación directa con las actividades para el logro de los objetivos de negocio.

De conocimiento preliminar la empresa no destina suficientes recursos humanos y capital en el departamento de tecnologías de la información, factor limitante para no ampliar nuestro enfoque de auditoría a niveles más específicos, cómo lo podría ser una revisión específica de vulnerabilidad de red u otra área por el estilo.

Complementariamente, a esta evaluación se pretenderá emitir un juicio u opinión acerca de lo adecuado del control interno informático y expresar una opinión acerca del grado de eficiencia, eficacia y economía con que están siendo usados y administrados todos los recursos de tecnología informática a cargo de la administración, incluido el factor humano.

Para tales efectos se han planteado los siguientes objetivos:

Objetivo Principal

- Realizar una auditoría sobre los Controles Generales de Tecnologías de Información en la empresa Corporación Arrocera Costa Rica S.A. con el fin de detectar áreas potenciales de mejora, mediante la implementación de una metodología de auditoría basada en los conocimientos adquiridos durante el plan de estudio.

Objetivos Específicos

- Obtener un conocimiento preliminar del negocio y sobre la naturaleza de las operaciones de tecnologías de información, ambiente de control del área de tecnología de la información e infraestructura tecnológica de la Corporación Arrocera Costa Rica S.A.

- Realizar un diagnóstico de la situación actual de la Corporación Arrocera Costa Rica S.A. y analizar posibles áreas de riesgo o factores claves de éxito.

- Aplicar un plan de trabajo de auditoría delimitando el periodo a revisión, alcance de las áreas a evaluar y los factores claves de éxito para enfocar los esfuerzos de auditoría.

- Presentar los resultados de la auditoría luego de ejecutar el plan de trabajo de auditoría, categorizando los resultados en criticidad de corrección e impacto en el negocio.

- Generar las conclusiones y recomendaciones luego de la presentación de los resultados de la auditoría.

Capítulo I. Entendimiento de Negocio, Corporación Arrocera Costa Rica S.A. (CACSA)

CACSA es la compañía matriz de un conglomerado agroindustrial cuyo rubro principal es el arroz. A través de sus subsidiarias en Costa Rica, opera en la producción e industrialización de semilla de arroz, en la producción agrícola de arroz en granza y en la industrialización y comercialización de diferentes mezclas de arroz blanco, precocido y subproductos.

Con base en las reuniones preliminares con el Contador de la empresa Sr. Manuel Arroyo[1] e información obtenida del sitio Corporativo en Internet (www.arrozeta.com)[2], se obtuvo el siguiente perfil corporativo por áreas:

1.1 Entendimiento de negocio

1.1.1 Ambiente competitivo

La empresa se dedica a la venta del arroz, después de procesarlo industrialmente, este es vendido a diferentes clientes con distintas marcas entre ellas, Arroz Imperio, Llanero, Águila, las marcas privadas de Megasuper y PriceSmart. Compite en forma directa con las distintas marcas del mercado y entre sus principales competidores se tiene a Coopeliberia con su marca de Arroz Sabanero, también con Pelón de la Bajura y Demasa con su marca de arroz Luisiana.

1.1.2 Ambiente regulatorio

El ambiente de regulación para esta industria es bastante fuerte en el país, desde la imposición del precio hasta los lineamientos que se presentan en cuanto a las importaciones del grano. Esta empresa está regida por las disposiciones de la Oficina del

[1] Entrevista con el Sr. Manuel Arroyo Vargas, Contador de Corporación Arrocera Costa Rica S.A., Lunes 26 de febrero del 2007, Planta Central, Barrio San José, Alajuela, Costa Rica

[2] Corporación Arrocera Costa Rica S.A., Perfil de la empresa, Sitio Web Oficial, http://www.arrozeta.com/, Lunes 26 de enero del 2007, Alajuela, Costa Rica

Arroz bajo la ley No 7014 y su reglamento[3], la cual entre otras se otorga ciertas atribuciones como:

- Fijar las cuotas necesarias de arroz para el consumo nacional y establecer las reservas que considere pertinentes.
- Dirigir, reglamentar y ejecutar la exportación e importación de arroz.
- Intervenir en las relaciones entre los beneficiadores y productores de arroz para que cumplan con los propósitos de la ley.

También todo lo referente a la producción y comercialización del arroz, importación, exportación, selección de variedades y zonas se regula en la ley No 6289[4].

1.1.3 Ambiente macroeconómico

Macro-económicamente la empresa se ve afectada porque el gobierno mantiene una política de regulación del precio. Cabe aclarar que el hecho de ser una actividad regulada tiene un efecto a nivel macroeconómico, puesto que existen muchos intereses políticos entre otros que pueden provocar un manejo a conveniencia.

1.1.4 Metas y objetivos

Mantener un volumen de ventas de 70.000 quintales por mes y participación del 18% en el mercado. Aumentar la participación en la venta de arroz especial (el 90% del arroz es entero).

1.1.5 Diseño organizacional

La Compañía mantiene un organigrama, el cual no aplica en la parte funcional. En el mismo las Compañías operan bajo la figura de la vicepresidencia a la cual reporta la gerencia general. Cada una de las 3 plantas industriales tiene un Gerente que reporta a la Gerente General y Financiera.

[3] Asamblea Legislativa de la Republica de Costa Rica, Ley No. 7014, Ley de Creación de la Oficina del Arroz, http://www.asamblea.go.cr/ley/leyes/7000/7014.doc, 1985, San José, Costa Rica

[4] Asamblea Legislativa de la Republica de Costa Rica, Ley No. 6289, Ley de Creación de la Oficina Nacional de Semillas, http://www.asamblea.go.cr/ley/leyes/6000/6289.doc, 1978, San José, Costa Rica

1.1.6 Gobierno

- Visión: Ser el mejor y más innovador grupo arrocero de la región, sólido como una gran multinacional, ágil como una pequeña empresa.
- Misión: Ser el líder de la región en producción, industrialización y comercialización de arroz, manteniendo la vanguardia a través de la innovación constante y la excelencia en el recurso humano, para el beneficio de clientes, proveedores, accionistas y empleados.

1.1.7 Clientes

Entre los principales clientes de la empresa se encuentran, Megasuper, PriceSmart, que forma un 20%, Cadena Comercial San Carleña, CODESUR, Almacén Luis Bolaños, Almacén San Isidro, entre otros que corresponde a zonas rurales.

1.1.8 Gente

La empresa cuenta con personal altamente capacitado puesto que poseen mucha experiencia en el campo, tanto la gerencia general como la gerencia financiera, han mostrado que es posible alcanzar los objetivos trazados.

1.1.9 Innovación

Se cuenta con los estándares de calidad para la industria, siempre innovando con marcas que satisfagan las necesidades de los consumidores, también innovando en la parte de la investigación para obtener mayor provecho del arroz que se procesa.

1.1.10 Marcas

La compañía posee diferentes marcas, con las cuales entra a distintos sectores de la población, entre ellas las marcas de Arroz Imperio, Arroz Felipe, Llanero, Águila y marcas privadas que le confecciona a Megasuper y PriceSmart.

1.1.11 Cadena de suplidores

La empresa obtiene su materia prima de distintos proveedores, de las 63,500 toneladas métricas se recibe 12,500 toneladas de Haciendas Unidas Mecanizadas S.A., el resto es proveniente de productores financiados por la misma empresa. De la cuota internacional a

la empresa le corresponde aproximadamente un 19%, lo que representa unas 27,000 toneladas métricas, el restante entre de los 27,000 y 12,500 es provisto como se mencionó antes por proveedores nacionales.

1.1.12 Riesgos

- El principal riesgo de la empresa es el hecho que el arroz es un producto muy regulado por el gobierno.
- A nivel de industria y comercialización es la actuación deshonesta de algunos industriales que salen al mercado compitiendo con descuentos hasta de 13%.
- No existe fidelidad en los clientes, ya que los mismos se inclinarán hacia el precio más bajo.
- El Tratado de Libre Comercio es un factor de riesgo a tomar en cuenta, ya que podría generar más opciones de competencia.

1.1.13 Análisis de segmento de mercado

Está dirigido a las distintas áreas del mercado, dependiendo de la calidad del arroz, ya que éste se comercializa en porcentajes de granos enteros, es de esperar que entre más alto sea el porcentaje de grano entero, más se acerque a preferencias de las clases más altas del país, lo mismo que si el arroz es quebrado y alrededor del 80% más será de preferencias para el sector más bajo.

1.1.14 Políticas contables

Estados Financieros preparados con base en las Normas Internacionales de Información Financieras y sus interpretaciones.

1.1.15 Plantas de almacenamiento y empaque

La empresa cuenta con 3 plantas de empaque y almacenamiento de arroz:

- Planta Alajuela
    - Capacidad de almacenaje: 10 silos de 1,500 toneladas c/u
    - Capacidad de producción: 8 1/2 toneladas x hora
    - Personal: 70 personas

- Capacitación: Desarrollo permanente a todo nivel
- Localización: Barrio San José, Alajuela

- Planta Liberia
  - Capacidad de almacenaje: 10 silos de 1,500 toneladas c/u
  - Capacidad de producción: 3 1/2 toneladas x hora
  - Personal: 30 personas
  - Capacitación: Desarrollo permanente a todo nivel
  - Localización: Liberia, Guanacaste
- Planta Palmar Norte
  - Capacidad de almacenaje: 4 silos de 1,500 toneladas c/u
  - Capacidad de producción: 3 1/2 toneladas x hora
  - Personal: 30 personas
  - Capacitación: Desarrollo permanente a todo nivel
  - Localización: Palmar Norte, Puntarenas

1.2 Entendimiento del área de TI

1.2.1 Naturaleza de las operaciones de tecnologías de información

Existe gran dependencia de las tecnologías de información para el logro de los objetivos operacionales de la empresa, específicamente en la parte de administración, que incluye las actividades de control de inventario, ventas, cuentas por cobrar, cuentas por pagar y tesorería.

1.2.2 Ambiente de control del área de tecnología de la información

Hasta hace algunos años, el departamento de tecnologías de información era considerado por la administración, como un departamento de soporte técnico y pocas veces se ha considerado como un área estratégica para el logro de objetivos corporativos. De tal manera, a la fecha no se ha fomentado una cultura adecuada de manejo de las operaciones de tecnologías de información, que incluyen actividades de control interno en la gestión del departamento, operaciones computarizadas, desarrollo y mantenimiento de aplicaciones y acceso a programas y datos.

Con el incremento en ventas y estrategia de ventas de la competencia, se ha visto la necesidad de tener cada día mayor información oportuna para la toma de decisiones, así como la necesidad de agilizar la información para el control de inventarios y gestión de cobros, factor que pretende ser un indicador clave de cambio para la administración, con el fin de cambiar la visión del departamento de tecnologías de información e involucrarlo de una manera más activa.

1.2.3 Estructura del departamento de tecnología de información

El departamento de tecnologías de información, está conformado actualmente sólo por dos personas, el Encargado de TI y una Soportista Técnica, que deben hacerse cargo de todas las actividades de esta área. El organigrama de TI se puede apreciar en la Figura 1. El encargado de TI a su vez depende directamente de la Gerencia Financiera y no de la Gerencia General. No existe un Comité de Informática, ni un plan estratégico vigente, formal y aprobado por la gerencia general, adicionalmente, no existe un presupuesto para las actividades de tecnología de información, los proyectos de inversión y compra de recursos tecnológicos, son solicitados a la Administración con base en las necesidades de negocio.

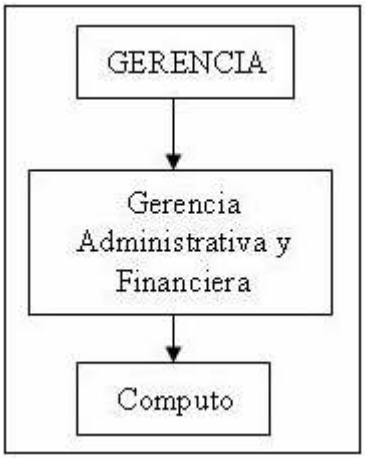

Figura 1. Organigrama de TI
Fuente: Administración CACSA

1.2.4 Infraestructura tecnológica

1.2.4.1 Operaciones computacionales

Topología de red	Estrella expandida
Modelo de procesamiento	Centralizado
Cantidad de estaciones interconectadas a través de la LAN	40 usuarios
Tipo de conexión utilizada	Fibra óptica y wireless
Dispositivos de comunicación utilizados	Switches, routers, firewall y access point
Protocolos de comunicación	TC/IP
Descripción de servidores principales	• Domain Controler (Windows 2000 Server, Active Directory) • Internet/Correo (Linux Red Hot) • Base de datos (SQL Server)
Aplicación principal	Microsoft Navision Axapta v.3
Aplicación manejo correo electrónico	Microsoft Outlook
Aplicación antivirus	Nod32
Aplicación backups	Backup Plus

1.2.4.2 Desarrollo y mantenimiento a sistemas

El mantenimiento (cambios a los programas) y desarrollo de aplicaciones se realizan de manera informal, por medio de una solicitud expresa de una gerencia usuaria o por un proyecto del cual se encarga un comité de proyecto. No existen procedimientos relacionados con esta función.

1.2.4.3 Accesos a programas y datos

Los accesos a los programas y datos, son asignados por medio de una solicitación explícita de una gerencia usuaria. Para estas labores no existe un formalismo o política de seguridad a seguir, la mayoría de la asignación de perfiles se realiza con base en las experiencias del personal de TI.

Capítulo II. Diagnóstico de la situación actual, posibles áreas de riesgo y factores claves de éxito

2.1 Diagnóstico de áreas críticas

Con base en el análisis preliminar obtenido en relación con las visitas de entendimiento de negocio, observación del ambiente de control interno de la empresa, visita a las instalaciones, indagación de fuentes primarias de información y la naturaleza de la organización, se determinó que la empresa es de carácter agrícola-productiva, sus actividades principales se encuentran enfocadas a la comercialización de arroz, por ende todas las actividades de control se enfatizan con las actividades sustantivas y no las adjetivas como lo son las tecnologías de información.

No existe un departamento de Auditoría Interna, ni se han hecho revisiones externas sobre las actividades de tecnologías de información.

En general, la empresa por su naturaleza de negocio, no soporta una infraestructura compleja y robusta de control interno, donde se incluyen las actividades de tecnología de información.

De tal manera se han detectado las siguientes áreas críticas de riesgo con base en los factores claves de éxito, tal y como se puede apreciar a continuación en la Tabla 1.

Área de TI	Área crítica de TI	Factor clave de éxito
Operaciones computacionales	Objetivos, plan estratégico y presupuesto de TI	Directrices administrativas
	Políticas y procedimientos formales de TI	Políticas para la conducción de las funciones de TI
	Administración de problemas y respaldos	Continuidad de las operaciones
	Recuperación en caso de desastre	Continuidad del negocio
Accesos a los programas y datos	Seguridad de datos	Restricción de acceso a los usuarios apropiados
	Seguridad del sistema operativo	Restricción de acceso a personal de TI
	Seguridad de la red	Restricción de acceso a personal de TI
	Seguridad física	Restricción de acceso a personal autorizado
Desarrollo y mantenimiento a sistemas	Especificación, autorización y seguimiento de las solicitudes de cambio	Las modificaciones son realizadas de manera controlada
	Iniciación, análisis y diseño de proyectos	Los desarrollos se realizan en base a las necesidades de negocio
	Construcción/Selección de paquetes	Los desarrollos o adquisiciones se realizan en base a una justificación de negocio
	Implementación de programas	Las implementaciones se realizan en base a lo planificado
	Documentación y entrenamiento	Todos los cambios y desarrollos son comunicados y documentados apropiadamente
	Segregación de funciones	Todas las actividades se realizan respetando los roles definidos

Tabla 1. Factores críticos de éxito por área de TI, área crítica de TI y factor clave de éxito
Fuente: El autor en base a criterios CobiT 4.0

2.2 Identificación de amenazas y vulnerabilidades

2.2.1 Amenazas

Las principales amenazas asociadas con el departamento de TI son las siguientes:

- Evolución acelerada de las tecnologías de información para las cuales no se tenga capacidad de respuesta o adquisición para las necesidades de negocio.
- Fortalecimiento de la competencia en aspectos tecnológicos y comercio electrónico que puedan generar desventaja competitiva.
- Las contrataciones de personal especializado en TI, se han disparado en los últimos años, razón que podría tentar al personal actual para aprovechar oportunidades laborales.
- Licenciamiento de software que podría ocasionar repercusiones legales contra la empresa.

2.2.2 Vulnerabilidades

Las principales debilidades asociadas con el departamento de TI son las siguientes:

- Poco personal a cargo de las labores de TI, lo que ocasiona conflictos en la segregación de funciones.
- Falta de recursos de TI (hardware y software), lo cual limita la capacidad de ofrecer servicios de calidad a nivel interno.
- Visión de la empresa hacia el departamento de TI como un departamento de soporte técnico, no como un departamento estratégico de negocio.
- Poca cultura de seguridad a nivel organizacional que se ve reflejado en la falta de políticas y directrices administrativas.
- No se denota una apropiada alineación de los objetivos de negocio con los objetivos de TI, que ayuden a su cumplimiento y brinden ventajas competitivas.

2.3 Delimitación del alcance de auditoría

Con base en las áreas críticas de riesgo detectadas, entendimiento preliminar de negocio, se estableció el alcance de auditoría, el cual se detalla a continuación:

Empresa:

Corporación Arrocera Costa Rica S.A.

Unidad de Negocio:

Departamento de Tecnologías de Información

Áreas a evaluar:

Controles Generales de Tecnología de Información:

- Operaciones computarizadas
- Cambios de los programas
- Accesos a los programas y datos
- Desarrollo de programas

Periodo de revisión:

Enero a marzo del 2007

Capítulo III. Plan de trabajo de auditoría

3.1 Preparación del programa de trabajo

3.1.1 Operaciones computarizadas

Para cada una de las áreas de riesgo identificadas en el punto 2.1 del Capítulo anterior y las cuales se encuentran reflejadas en la Figura 2, se pretenderá establecer con base en el factor clave de éxito, un objetivo de auditoría del cual se desprenderán procedimientos detallados de auditoría a ser evaluados.

Tal y como se estableció en el punto 2.3 del Capítulo anterior, en la definición del alcance, se determinó el análisis de los Controles Generales de TI (CGTI). Ya que la empresa tiene centralizadas las labores de mantenimiento y desarrollo de aplicaciones, las áreas a evaluar serán las siguientes:

- Operaciones computarizadas
- Accesos a los programas y datos
- Cambios y desarrollo de programas

Objetivo General

El objetivo primordial para las operaciones computadorizadas es asegurar que los sistemas de producción se procesan en forma completa y correcta de acuerdo con los objetivos de control establecidos por la administración y que los problemas de procesamiento son identificados y resueltos en forma completa y correcta para mantener la integridad de la información.

Objetivos Específicos

a) Determinar la existencia de objetivos, plan estratégico y presupuesto de TI
b) Verificar la existencia y aplicación de políticas y procedimientos formales de TI
c) Corroborar que existe un procedimiento para la administración de problemas y respaldos
d) Confirmar la existencia y aplicación de un plan de recuperación en caso de desastre

3.1.2 Accesos a los programas y datos

Objetivo General

El objetivo principal para el acceso a los programas y datos es asegurar que sólo se otorga acceso autorizado a los programas y datos si se autentica la identidad de un usuario, con base en una justificación o necesidad explícita de negocio.

Objetivos Específicos

a) Determinar que existen mecanismos apropiados de seguridad para la asignación de permisos de manipulación de datos
b) Cerciorarse que existan adecuados mecanismos de control de seguridad para el control de acceso al sistema operativo
c) Confirmar que existan adecuados mecanismos de seguridad de acceso a la red de la empresa
d) Verificar que existan adecuados mecanismos de seguridad física y control de activos sobre los recursos informáticos

3.1.3 Cambios y desarrollo de programas

Objetivo General

El objetivo dominante para los cambios y desarrollo de programas es asegurar que los sistemas son desarrollados, configurados, modificados e implantados para cumplir con los objetivos de control sobre aplicaciones de la administración.

Objetivos Específicos

a) Identificar que existan adecuados mecanismos de especificación, autorización y seguimiento de las solicitudes de cambio a los programas
b) Cerciorarse que existan adecuados controles sobres las actividades de iniciación, análisis y diseño de proyectos
c) Determinar que exista una adecuada metodología de construcción y/o selección de paquetes
d) Confirmar la existencia de adecuados planes de implementación de programas

e) Verificar la existencia de adecuados mecanismos de documentación y entrenamiento a usuarios finales luego de la implementación de cambios y programas
f) Constatar que exista una adecuada segregación de funciones en las actividades de cambios y desarrollo de programas.

3.2 Ejecución del programa de trabajo

Luego de definir el programa de trabajo por objetivos generales y específicos, para poder ejecutar el programa, se deben establecer procedimientos específicos para poder validar cada uno de los objetivos.
De tal manera se establecieron los siguientes procedimientos:

3.2.1 Operaciones computarizadas

A1. Determinar la existencia de objetivos, plan estratégico y presupuesto de TI
1. ¿Existen objetivos de TI a corto y largo plazo? 2. ¿Existe un plan estratégico alineado con los objetivos de negocio? 3. ¿Existe un presupuesto formal de TI que se integre con el presupuesto de la empresa?
A2. Verificar la existencia y aplicación de políticas y procedimientos formales de TI
1. ¿Existen políticas y procedimientos documentados, aprobados por la gerencia general y comunicados a todos los usuarios respectivos? 2. ¿Todos los componentes de software poseen su licencia de uso respectiva y las mismas permanecen vigentes? 3. ¿Existe una adecuada segregación de funciones dentro del personal de TI? 4. ¿Existen adecuados recursos informáticos para el cumplimiento de las expectativas de la administración y cumplimiento de objetivos de negocio?

A3. Corroborar que existe un procedimiento para la administración de problemas y respaldos
1. ¿Existen procedimientos formales de respaldo? 2. ¿Se realizan respaldos en forma controlada y con qué periodicidad se realizan? 3. ¿Se mantienen copias en dispositivos magnéticos resguardados adecuadamente y son probados periódicamente? 4. ¿Se realizan copias en dispositivos magnéticos fuera de sitio?
A4. Confirmar la existencia y aplicación de un plan de recuperación en caso de desastre
1. ¿Existe un plan de recuperación en caso de desastre o plan de contingencia? 2. ¿De existir, es éste adecuado y se encuentra actualizado? 3. ¿Existe un procedimiento adecuado de prueba del plan?

3.2.2 Accesos a los programas y datos

B1. Determinar que existen mecanismos apropiados de seguridad para la asignación de permisos de manipulación de datos
1. ¿Existe un adecuado procedimiento para la asignación de permisos que involucre al departamento de recursos humanos? 2. ¿Existe un estándar de creación de usuarios para cada uno de las aplicaciones y usuarios de red? 3. ¿Se revisan los permisos periódicamente para detectar usuarios inactivos o usuarios que han cambio sus roles dentro de la empresa? 4. ¿Existe una adecuada parametrización de seguridad lógica en la aplicación Axapta? (Utilice el formulario de verificación de seguridad lógica, de acuerdo a las mejores prácticas) 5. ¿Existe una adecuada parametrización de seguridad lógica para el manejo de la base de datos SQL Server 2000 utilizada en la empresa? (Utilice un formulario de verificación de seguridad lógica para la base de datos SQL Server 2000, de acuerdo a las mejores prácticas)

B2. Cerciorarse que existan adecuados mecanismos de control de seguridad para el control de acceso al sistema operativo
1. ¿Existe una adecuada parametrización de seguridad lógica para el sistema operativo Windows 2000 Server utilizado por la empresa? (Utilice un formulario de verificación de seguridad lógica para el sistema Windows 2000 Server, de acuerdo a las mejores prácticas)
B3. Confirmar que existan adecuados mecanismos de seguridad de acceso a la red de la empresa
1. ¿Existen adecuados dispositivos y herramientas para el manejo de red? 2. ¿Existe un adecuado diseño de la red (separación lógica de dominios, conexiones con una red externa, etc.) para garantizar que los sistemas significativos están protegidos en forma apropiada del acceso no autorizado (firewalls)? 3. ¿Existe una adecuada configuración de la red donde se incluyan controles de autenticación (controles de contraseñas, asignación de usuarios a los grupos, acceso remoto, etc.)? 4. ¿Existen adecuados mecanismos de monitoreo para los posibles incidentes de seguridad en la red interna y externa, y cómo responde a ellos?
B4. Verificar que existan adecuados mecanismos de seguridad física y control de activos sobre los recursos informáticos
1. ¿Existen adecuados controles de seguridad física para el cuarto de servidores y equipo sensible de red? (Utilice un formulario de verificación de seguridad física, de acuerdo a las mejores prácticas)

3.2.3 Cambios y desarrollo de programas

C1. Identificar que existan adecuados mecanismos de especificación, autorización y seguimiento de las solicitudes de cambio a los programas
1. ¿Existe un proceso controlado para todos los cambios en los sistemas en todos los programas de aplicación, componentes de infraestructura, unidades de administración y localidades?

C2. Cerciorarse que existan adecuados controles sobres las actividades de iniciación, análisis y diseño de proyectos
1. ¿Existe un adecuado procedimiento o metodología para asegurar el desarrollo uniforme de las aplicaciones, en línea con los objetivos de negocio y de control interno?
C3. Determinar que exista una adecuada metodología de construcción y/o selección de paquetes
1. ¿Existe un estándar de programación para las aplicaciones desarrolladas internamente? 2. ¿Existe una metodología de adquisición que establezca los pasos requeridos para la selección, adaptación a medida e implantación de los paquetes de software adquiridos?
C4. Confirmar la existencia de adecuados planes de implementación de programas
1. ¿Existe un procedimiento de control para asegurar que todas las actividades de implementación se realicen de manera adecuada?
C5. Verificar la existencia de adecuados mecanismos de documentación y entrenamiento a usuarios finales luego de la implementación de cambios y programas
1. ¿Existen mecanismos adecuados de control para desarrollar documentación técnica y usuaria, que se comunica oportunamente para todos los cambios y nuevos sistemas? 2. ¿Existen adecuados mecanismos para asegurar que los usuarios y el personal de IT recibe capacitación adecuada en todos los nuevos sistemas y los controles internos relacionados?
C6. Constatar que exista una adecuada segregación de funciones en las actividades de cambios y desarrollo de programas
1. ¿Existe un adecuado procedimiento de asignación de roles y responsabilidades para las tareas de cambio y desarrollo de programas, incluso acceso a datos, ambientes de prueba y producción?

3.3 Recolección de evidencia

Con base en el trabajo de campo, realizado; se procedió a la obtención de la evidencia y valuación de cada uno de los procedimientos, establecidos en el punto 3.2 del presente Capítulo los cuales se detallan a continuación:

Área de TI	Objetivo	Procedimiento	Respuesta			Comentario	Evidencia
			SI	NO	NA		
Operaciones computarizadas	A1	1		X		Se comprobó la inexistencia de objetivos, plan estratégico y presupuesto de TI	
		2		X			
		3		X			
	A2	1		X		Se realizan procedimientos, no obstante no existe documentación formal de los mismos	
		2		X		Existen algunas licencias específicamente con el proveedor Microsoft, que no están actualizadas (Office, Windows XP, Windows 2000 Server y SQL Server 2000)	Verificación de las listas de control de recursos informáticos
		3		X		Existen sólo 2 personas en el departamento de TI, que tienen acceso a realizar todas las actividades debido a la limitación de personal	
		4		X		Existen recursos limitados de TI, específicamente servidores, licencias de software y personal de TI	Se compró que los funcionarios de TI realizan múltiples actividades, el encargado de TI utiliza su computador personal como servidor y que existe software sin licenciamiento
		4		X		A la fecha no se mantiene respaldos fuera de sitio	

Área de TI	Objetivo	Procedimiento	Respuesta			Comentario	Evidencia
			SI	NO	NA		
Operaciones computarizadas	A3	1	X			Aunque no se encuentran formalmente documentados, si se realizan actividades de respaldos	Se comprobó que se realizan procesos de respaldos por medio de la aplicación Backup Plus
		2	X			Los respaldos se realizan automáticamente, diariamente y semanalmente	Se comprobó la configuración de los respaldos con la aplicación Backup Plus
		3	X			La información se respalda en discos duros externos	Se compró la existencia de los discos duros externos y del contenido de los respaldos
		4		X		A la fecha no se mantiene respaldos fuera de sitio	
	A4	1		X		No existe un plan de recuperación en caso de desastre o plan de contingencia	
		2		X			
		3		X			

Área de TI	Objetivo	Procedimiento	Respuesta			Comentario	Evidencia
			SI	NO	NA		
Accesos a los programas y datos	B1	1		X		No existe un procedimiento formal, ni que involucre de lleno al departamento de recursos humanos, las solicitudes son enviadas directamente de cada jefatura	
		2	X			No existe un estándar formal, aunque el encargado de TI utiliza uno a su criterio	Se determinó que el estándar de identificar a los usuario con la primera letra del nombre y luego el apellido es consistente y adecuado
		3		X		Este procedimiento no se realiza debido a razones de saturación de trabajo según el encargado de TI	
		4	X			Se realizó el formulario de validación de seguridad lógica para la aplicación Axapta, con resultados satisfactorios. Este formulario se elaboró de acuerdo a las mejores prácticas obtenidas en los marcos de referencia y control ISO/IEC 27001 y CobiT 4.0	Ver Anexo 1
		5		X		Se realizó el formulario de validación de seguridad lógica para la base de datos SQL Server 2000, aunque en la mayoría de los casos se encontraron resultados satisfactorios, se detectaron excepciones. Este formulario se elaboró de acuerdo a las mejores prácticas obtenidas en el sitio de Internet de Microsoft Corporation[5]	Ver Anexo 2

[5] Microsoft Corporation: Martes 13 de marzo del 2007, Soporte Técnico SQL Server 2000, Mejores Prácticas de Configuración SQL Server 2000, http://support.microsoft.com/ph/2852, Estados Unidos

Área de TI	Objetivo	Procedimiento	Respuesta			Comentario	Evidencia
			SI	NO	NA		
Accesos a los programas y datos	B2	1		X		Se realizó el formulario de validación de seguridad lógica para el sistema operativo Windows 2000 Server, aunque en la mayoría de los casos se encontraron resultados satisfactorios, se detectaron excepciones. Este formulario se elaboró de acuerdo a las mejores prácticas obtenidas en el sitio de Internet de Microsoft Corporation[6]	Ver Anexo 3
	B3	1	X			Se determinó que aunque no existen políticas de seguridad para el manejo de la red, el encargado de TI mantiene configuraciones adecuadas de acuerdo a las mejores prácticas	
		2	X				
		3	X			Se verificó los parámetros de seguridad configurados en la administración de la red	
		4		X		Estos se realizan sólo si existe una sospecha o revisión explicita por parte de la administración	
	B4	1		X		Se realizó el formulario de validación de seguridad física, aunque en la mayoría de los casos se encontraron resultados satisfactorios, se detectaron excepciones. Este formulario se elaboró de acuerdo a las mejores prácticas obtenidas en los marcos de referencia y control ISO/IEC 27001 y CobiT 4.0	Ver Anexo 4

[6] Microsoft Corporation: Martes 13 de marzo del 2007, Soporte Técnico Windows 2000 Server , Mejores Prácticas de Configuración Windows 2000 Server, http://www.microsoft.com/technet/solutionaccelerators/howto/admhow.mspx, Estados Unidos

Área de TI	Objetivo	Procedimiento	Respuesta			Comentario	Evidencia
			SI	NO	NA		
Cambios y desarrollo de programas	C1	1		X		Aunque la empresa no realiza actividades significativas de desarrollo, las actividades relacionadas y cambio menores (reportes o campos), se realizan de manera informal y sólo el encargado de TI, tiene conocimiento de los mismos. Las solicitudes se canalizan por medio de email.	
	C2	1		X			
	C3	1		X			
	C4	1		X			
	C5	1		X		No existen mecanismos de documentación de cambios y desarrollo de aplicaciones.	
		2	X			Cada cambio debe ser aceptado, por la persona que lo haya solicitado, aunque no existe ningún mecanismo para evidenciar esta aceptación.	
	C6	1		X		No existe un adecuado mecanismo para garantizar la segregación de funciones, ya que solo existen 2 funcionarios en el departamento de TI.	

Capítulo IV. Comunicación de resultados

4.1 Preparación de hallazgos de auditoría

Con base en los resultados obtenidos luego de la ejecución del programa de auditoría por medio de la recolección de evidencia, la cual se detalla en el punto 3.3 del Capítulo anterior, se procedió a reunir los puntos significativos de mejora con los cuales se procedió a realizar los siguientes hallazgos de auditoría. Cabe destacar, que los criterios de información utilizados como base de referencia de mejores prácticas fueron el Marco de Referencia Cobit 4.0[7] y el Estándar de Seguridad BS ISO/IEC 27001[8].

4.1.1 Hallazgo 1: Plan estratégico y presupuesto de TI

Facilidad de implementación: Fácil

Impacto: Alto

Tipo de hallazgo: Control y eficiencia

Observación: Durante la revisión de la documentación del plan estratégico y presupuestario para el Área de Tecnología de Información, se pudo comprobar la inexistencia de un plan estratégico de TI a corto, mediano y largo plazo formalmente documentado y aprobado por la gerencia. Así mismo, no se determinó la existencia de un documento formal de presupuesto de TI donde se detallen los gastos e inversiones requeridos para el área de TI según lo planeado estratégicamente. Lo anterior, puede sugerir que el Área de TI no está alineada con los objetivos y estrategias corporativas.

Criterio: Marco de Referencia CobiT 4.0

Impacto: Los objetivos y estrategias en el área de TI impactan directamente la función del departamento de Sistemas de Información, ya que éstos dirigen el accionar de los miembros de este equipo con los objetivos y metas generales de la organización. Los objetivos y estrategias TI bien definidos, documentados, aprobados y comunicados, facilitan el logro de los objetivos conjuntos de la empresa, permiten una mayor comprensión sobre los riesgos

[7] Instituto de Gobierno de TI: Martes 27 de enero del 2007, CobiT 4.0, Sitio Web Oficial, http://www.isaca.org/, Estados Unidos de América

[8] British Standards Information: Martes 27 de enero del 2007, BS ISO/IEC 27001 Tecnología de Información, Sitio Web Oficial, http://www.bsi-global.com/ICT/Security/bs7799-2.xalter, Reino Unido

claves del manejo de la información, mejoramiento continuo del sistema de control interno, optimizan la asignación de recursos y la elaboración del presupuesto, se da un mejor aprovechamiento de las oportunidades competitivas del negocio, además de fortalecer la cultura de autocontrol y brindar una mayor estabilidad ante cambios del entorno.

Recomendación: Se recomienda, la implementación y documentación de objetivos y estrategias de la función de servicios de información formalmente aprobados y comunicados por la administración de la empresa. Además, el documento tendrá un formato estándar para evitar confusiones o malas interpretaciones y asegurar su vigencia y validez, así como la integración con el resto de los objetivos de la organización. Adicionalmente se recomienda desarrollar anualmente un plan de presupuesto, el cual inicialmente deberá ser analizado por el encargado de sistemas, de acuerdo a las necesidades del departamento, luego debe ser revisado y aprobado por la alta Gerencia o el comité de informática de la compañía.

4.1.2 Hallazgo 2: Políticas y procedimientos formales de TI

Facilidad de implementación: Fácil

Impacto: Alto

Tipo de hallazgo: Control y eficiencia

Observación: Se pudo verificar durante nuestra revisión de los controles generales de TI, que no existen políticas y procedimientos formales relacionados con las actividades de TI. Las áreas básicas que carecen de procedimientos y políticas formales son las siguientes:

- Cambios a los programas (Solicitud de cambios, documentación de cambios, niveles de aprobación, segregación de funciones)
- Operaciones computarizadas (Creación y custodia de backups, administración del departamento de TI, proceso de compra y adquisiciones de software y hardware, procesos de capacitación de personal de TI y usuario final)
- Desarrollo de programas (Solicitud de nuevos proyectos, estándares de desarrollo, control de ejecutables, servidores de prueba)
- Acceso a programas y datos (Solicitud de creación de usuarios, monitoreo de la red, asignación y autorización de permisos de usuario de red, aplicación y base de datos, segregación de funciones, acceso al área de servidores, seguridad física de activos de TI, restricciones de terminales de usuario final)

Criterio: Marco de Referencia CobiT 4.0

Impacto: Las políticas son documentos de alto nivel, ellas representan la filosofía corporativa de una organización. Los procedimientos son documentos detallados derivados de una política corporativa que describen las pautas a seguir para el cumplimiento de la misma. La falta de implementación de esta práctica atenta contra la continuidad de las operaciones de la organización, el nivel de eficacia necesario, la curva de aprendizaje de empleados nuevos, la dependencia de funcionarios en el área TI, entre otros.

Recomendación: Se recomienda, la implementación y documentación de políticas y procedimientos de todos y cada uno de los aspectos de la función de servicios de información formalmente aprobados y comunicados por la administración de la empresa, con la finalidad de comunicar y establecer parámetros funcionales sobre cómo realizar cada labor de manera eficiente para la obtención de los objetivos propuestos y el acatamiento de las disposiciones de la gerencia.

4.1.3 Hallazgo 3: Licenciamiento de software

Facilidad de implementación: Fácil

Impacto: Alto

Tipo de hallazgo: Control y cumplimiento

Observación: Se pudo determinar en la evaluación de las aplicaciones disponibles para la administración de la función de servicios de Tecnología de Información, en el uso de paquetes y software con su debido licenciamiento, se comprobó que no existe licenciamiento para algunas de las aplicaciones utilizadas por la empresa, entre ellas, las aplicaciones de la plataforma Microsoft (SQL Server, Windows Server, Windows 2000 y XP y Office). Además, se detectaron software del tipo freeware (obtenido de Internet) para labores corporativas entre ellas la detección de virus (antivirus).

Criterio: Marco de Referencia CobiT 4.0

Impacto: Utilizar software sin el debido registro o licenciamiento podría generar repercusiones legales contra la empresa, fomentar la cultura de utilizar aplicaciones no autorizadas y pérdida de imagen del negocio en relación con la competencia. Además de uso de software freeware, no garantiza que estos utilitarios cumplan su cometido, ya que muchas

de estas versiones están sujetas a pruebas y en algunas veces presentan limitaciones en algunas de sus funciones.

Recomendación: Se recomienda en primera instancia, realizar un estudio de software instalado por equipo, determinar el software necesario, de acuerdo con las necesidades de negocio, determinar la cantidad de usuarios que poseen la herramienta y proceder a realizar las actualizaciones correspondientes con cada proveedor. Luego de realizad este proceso, se recomienda establecer un control de licencias periódicamente, con el fin de evaluar la necesidad de adquirir o dejar de actualizar licencias de uso de software.

4.1.4 Hallazgo 4: Segregación de funciones y estructura jerárquica del departamento de TI

Facilidad de implementación: Fácil

Impacto: Medio

Tipo de hallazgo: Control, cumplimiento y eficiencia

Observación: Durante nuestra revisión sobre la segregación de funciones y la estructura del departamento de TI, se pudo comprobar que no se han asignado roles y actividades formales a los funcionarios de TI. Adicionalmente se pudo comprobar que el departamento de TI depende directamente de la gerencia financiera y no de la gerencia general, situación que podría afectar la orientación de los objetivos de TI para el logro de los objetivos de negocio.

Criterio: Marco de Referencia CobiT 4.0

Impacto: El no contar con roles y actividades específicas a los funcionarios de TI podría ocasionar que no se establezcan responsables de actividades, no exista rastrehabilidad de acciones y accesos no permitidos y no se garantiza que las funciones que realice cada funcionario, no interfieran o comprometan el manejo adecuado de las herramientas y recursos de TI. Por otro lado la dependencia directa del departamento de TI a la gerencia financiera podría ocasionar conflictos de interés, en satisfacer en primera instancia las necesidades del departamento financiero y no las actividades globales de la empresa como resultado de que no exista una adecuada alineación de los objetivos de TI con los objetivos corporativos.

Recomendación: Se recomienda establecer manuales de puestos de los funcionarios de TI, que establezcan responsabilidades, actividades y la adecuada segregación de funciones de acuerdo con el perfil determinado. Adicionalmente, se recomienda analizar la estructura actual de TI,

de tal manera que los objetivos de la empresa puedan estar directamente relacionados con el logro de objetivos de negocio, situación que pudiese solventarse facilitando la comunicación con la administración general, que ayude a enfocar al departamento de TI no sólo como un departamento de soporte técnico, sino como una unidad estratégica y funcional dentro de la empresa.

4.1.5 Hallazgo 5: Procedimientos de respaldos

Facilidad de implementación: Fácil

Impacto: Medio

Tipo de hallazgo: Control

Observación: Durante la revisión de las herramientas y procedimientos sobre el respaldo de la información crítica de la empresa, se pudo comprobar que no existe un almacenamiento externo de los respaldos de información del servidor central, así como la carencia de bitácoras de control manual de los respaldos. Adicionalmente, ninguno de estos procedimientos se encuentra documentado formalmente.

Criterio: Marco de Referencia CobiT 4.0 y Estándar de Seguridad BS ISO/IEC 27001

Impacto: La falta de respaldos externos podría ocasionar pérdidas de datos debido a que la información sensitiva para la empresa se encuentra centralizada en una sola ubicación, causando pérdidas de tiempo, dinero e imagen del negocio mientras se reconstruye la información, además de los retrasos contables y otros posibles efectos indirectos.

Recomendación: Se recomienda analizar la posibilidad de realizar respaldos en un sitio externo, el cual facilite la reestructuración de la información ante una amenaza fuerte de desastre o de pérdida de datos, a su vez que se fortalezcan los controles de resguardo interno de los dispositivos magnéticos por medio de bitácoras manuales que permitan realizar un control cruzado con los registros lógicos.

4.1.6 Hallazgo 6: Planes de recuperación ante desastres, catástrofes y de restauración interna

Facilidad de implementación: Difícil

Impacto: Alto

Tipo de hallazgo: Control, cumplimiento y eficiencia

Observación: Durante la evaluación del uso de un planeamiento de continuidad del negocio, se determinó que no existe un plan de recuperación ante desastres y/o catástrofes y el de restauración interna debidamente documentado y comunicado. A pesar de cumplir con procedimientos que fortalecen la preparación ante una contingencia, éstos no son suficientes y no están bajo un marco de prevención y corrección formal y comunicado.

Criterio: Marco de Referencia CobiT 4.0 y Estándar de Seguridad BS ISO/IEC 27001

Impacto: No sólo la falta de un adecuado plan para contingencias (desastres, catástrofes, restauración interna), sino la falta de pruebas y documentación de resultados crean una incertidumbre ante la contingencia, por lo que la práctica actual expone a la compañía a problemas financieros y de pérdida de imagen. Entre más grande sea la brecha entre la contingencia y la recuperación o restauración, mayor será el impacto en la entidad.

Recomendación: Se recomienda establecer un plan de continuidad de negocio que considere en su proceso de implementación, el planeamiento de continuidad de operaciones que incluya los siguientes aspectos: el personal clave, respaldos de los suministros requeridos, organización y asignación de responsabilidades, clasificación de riesgo de los sistemas computacionales, periodo de tiempo de recuperación crítica, aplicaciones que deben recuperarse en un periodo crítico de tiempo de recuperación, interrelaciones entre los usuarios y el procesamiento de datos, prioridades de procesamiento, redes de telecomunicación, seguros, alternativas de recuperación, hardware alternativo, custodia fuera del sitio, respaldo de seguridad de los medios y de la documentación, procedimientos periódicos de respaldo, frecuencia de rotación, pruebas del plan de recuperación y continuidad y análisis de resultados.

4.1.7 Hallazgo 7: Control de entradas, modificaciones y salidas de usuarios

Facilidad de implementación: Fácil

Impacto: Medio

Tipo de hallazgo: Control y eficiencia

Observación: Luego de la revisión sobre los controles de control de acceso y asignación de permisos a los usuarios, se detectó que no existe un procedimiento formal para asignación de permisos que involucre las notificaciones por medio del departamento de recursos humanos.

Criterio: Marco de Referencia CobiT 4.0 y Estándar de Seguridad BS ISO/IEC 27001

Impacto: La falta de un proceso controlado de asignación, modificación y eliminación de usuarios, podría generar, que se asignen permisos sin una justificación real de negocio, se actualicen los perfiles para usuarios que han cambiado sus actividades dentro de la empresa y que existan usuarios activos que ya no laboren con la empresa.

Recomendación: Se recomienda incluir, como política de seguridad de la empresa, procedimientos formales para la creación, modificación y eliminación de usuarios en los sistemas de información. Es importante dar a conocer que este paso se inicia en recursos humanos quienes deberían de informar inmediatamente a los encargados de sistemas de manera formal el retiro, modificación o la entrada de nuevo personal a la compañía.

4.1.8 Hallazgo 8: Seguridad lógica de SQL Server 2000 y Windows 2000 Server

Facilidad de implementación: Fácil

Impacto: Alto

Tipo de hallazgo: Control, cumplimiento y eficiencia

Observación: Por medio de la aplicación de formulario de validación de acuerdo con las mejores prácticas relacionadas con la seguridad lógica, para evaluar la base de datos SQL Server 2000 y el administrador de red Windows 2000 Server, se pudieron detectar algunos aspectos de mejora:

SQL Server 2000

- No se encontraron habilitadas las funciones de "log" de auditoría
- No se encontró deshabilitado la función para realizar réplicas remotas

- Se detectaron dos usuarios administradores creados por defecto y con contraseñas en blanco (NULL)
- Muchas de las configuraciones de seguridad se mantienen por defecto luego de la primera instalación

Windows 2000 Server

- No se encontraron habilitadas las funciones de "log" de auditoría
- Muchas de las configuraciones de seguridad se mantienen por defecto luego de la primera instalación

Criterio: Marco de Referencia CobiT 4.0 y Estándar de Seguridad BS ISO/IEC 27001

Impacto: Las debilidades detectadas a nivel de la seguridad lógica podrían generar riesgos tecnológicos, que tienen destacada relevancia por el potencial impacto económico que podría representar: que existiesen usuarios o perfiles genéricos, mala segregación de funciones en la asignación de roles del sistema, actividades no permitidas por usuarios finales, penetración de intrusos de consumo de almacenamiento y red, pérdidas o copia de información confidencial, virus informáticos, "hackers", fallos de hardware y software, fraude informático, mal funcionamiento del centro de datos, entre otros.

Recomendación: Se recomienda establecer un plan de acción de medidas correctivas relacionadas con la seguridad lógica básica, para el buen funcionamiento de las operaciones relacionadas con tecnología de información, que tengan su fundamentación con una política de seguridad alineada con los objetivos de negocio, con el fin de evitar que algunas de estas debilidades se materialicen en algún riesgo en el corto plazo.

4.1.9 Hallazgo 9: Seguridad física cuarto de servidores

Facilidad de implementación: Difícil

Impacto: Alto

Tipo de hallazgo: Control, cumplimiento y eficiencia

Observación: Como parte de la revisión de los procedimientos enfocados a la seguridad física se pudo verificar que el acceso al área de informática, no se encuentra totalmente restringido a terceros, no existe rotulación de acceso restringido, los equipos están expuesto a terceros, no existe un extintor de incendio especial para equipo eléctrico en cada área de servidores, no

existen dispositivos ambientales (detector de humo, óptimo aire acondicionado, alarma contra incendio y humo) y no existen bitácoras de control de accesos de terceros.

Criterio: Marco de Referencia CobiT 4.0 y Estándar de Seguridad BS ISO/IEC 27001

Impacto: El no identificar cuáles áreas específicas de la organización son de acceso restringido y el no resguardar de una manera segura las puertas, ventanas o otros portillos con llave, barandas, rejas o con otro mecanismo de seguridad, permite que algún atacante ingrese fácilmente a esta área sensitiva, lo cual podría ocasionar hurtos, daños a los equipos y la alteración o manipulación de información sensitiva para la empresa, generando un posible daño en la continuidad inmediata de las operaciones. Además, no sólo el resguardo físico, si no también el espacio del área y las condiciones ambientales son esenciales para el adecuado funcionamiento de los recursos de TI.

Recomendación: Se recomienda fortalecer los mecanismos de acceso físico, resguardo de equipo y realizar un análisis de optimización de los recursos informáticos, así como fomentar programas de capacitación continua sobre seguridad física que establezca como objetivo principal crear una cultura de concienciación sobre el debido cuidado y uso de las herramientas informáticas.

4.1.10 Hallazgo 10: Procedimientos de cambios y desarrollo de programas

Facilidad de implementación: Fácil

Impacto: Bajo

Tipo de hallazgo: Control y eficiencia

Observación: Se pudo comprobar que no se mantienen procedimientos relacionados con el control y de cambios, metodología de cambios y desarrollo, estándares de programación, metodología de adquisición, documentación, aceptación de usuarios, implementación y segregación de funciones.

Criterio: Marco de Referencia CobiT 4.0

Impacto: La falta de controles relacionados con las actividades de cambios y desarrollo de programas podría generar, modificaciones no autorizadas y recursos de TI mal canalizados en proyectos que no tengan una justificación real de negocio.

Recomendación: Se recomienda establecer un adecuado mecanismo de control por medio de un estándar o metodología que involucre todas las actividades de cambio y desarrollo de

programas, que incluye responsables, canalización de solicitudes, asignación de plazos y recursos de TI, selección de paquetes, uso de estándares y procedimientos de desarrollo, implementación y documentación.

4.2 Elaboración de informe final de auditoría

Luego de finalizada toda la etapa de ejecución de la auditoría se procedió a realizar el informe final de la misma, que incluye todos los aspectos de mejora detectados, así como la asignación de prioridades e impacto de cada uno de los hallazgos, para que la administración de la empresa tenga un criterio de cuáles aspectos son más críticos para la empresa y requieren de un plan de acción inmediato. Por razones de confidencialidad a petición de la empresa, el informe no se anexa en este trabajo.

4.3 Presentación de informe final de auditoría

El informe final de auditoría, fue presentado a la empresa, canalizado por el encargado de TI y el contador de la empresa, los cuales consideraron que los aspectos de mejora presentados, son pertinentes y que evidentemente, son aspectos de consideración inmediata para la optimización de las labores de TI para el cumplimiento de los objetivos de negocio.
Cada uno de los puntos será valorado por la compañía, para determinar cuál será el plan de acción futuro, en donde se espera poder tener una realimentación futura para el seguimiento de los mismos, como parte del compromiso adquirido entre las partes antes de la realización de la auditoría.
Se espera que el seguimiento de los puntos se realice al cabo de seis meses cumplidos luego de entregado el reporte de auditoría.

Capítulo V. Conclusiones y recomendaciones

5.1 Conclusiones

Luego de realizada la auditoría sobre los Controles Generales de Tecnología de Información en la Corporación Arrocera Costa Rica S.A., se desprenden las siguientes conclusiones:

No existe un adecuado alineamiento de los objetivos de TI que ayuden a cumplir con los objetivos del negocio. El departamento de TI, es considerado, como un área de soporte técnico, que cumple solamente con actividades adjetivas de negocio y no sustantivas o estratégicas.

La gran mayoría de las actividades de TI, no cuentan con políticas ni procedimientos formales, que hayan sido aprobadas por la Administración, que soporten tanto las labores diarias como periódicas, indiquen responsables y recursos de TI.

Los funcionarios de TI, tienen conocimiento sobre la situación actual del departamento de TI, pero la filosofía de la Administración está focalizada en otros aspectos estratégicos de negocios y no ha considerado pertinente, brindar mayor apoyo a las actividades de TI.

Aunque no existan actividades formales de TI, no significa que no se realicen procedimientos adecuados de TI. Los funcionarios del departamento de TI, realizan las actividades con los recursos disponibles y deben dar prioridades a las actividades, debido al poco personal, exceso de labores e inadecuada segregación de funciones.

5.2 Recomendaciones

Con base en las conclusiones antes mencionadas, se recomienda:

Considerar la viabilidad de implementación de las recomendaciones para cada uno de los aspectos de mejora mencionados en el Capítulo 4 y en el Informe de Auditoría suministrado a la empresa, con el fin de mejorar las actividades de Controles Generales de Tecnologías de Información.

Priorizar la implementación de las recomendaciones, con base en el impacto (alto, medio o bajo) y la dificultad (fácil o difícil), con el fin concentrar esfuerzos en aquellas áreas críticas de negocio que requieran mayor atención por parte de la empresa.

Establecer un Comité de Informática, o comisión que vele por el seguimiento de las recomendaciones de auditoría y que se encargue de coordinar o mediar en la alineación de los objetivos de TI con los objetivos de negocio.

Crear un programa de concienciación de la importancia de las actividades, recursos y controles sobre las Tecnologías de información, que se implante como parte de la filosofía de la Administración y que venga a ayudar a que todos los colabores y usuarios finales sean un factor primordial para que el departamento de TI opere de la mejor manera posible y contribuya al logro de los objetivos de negocio.

Bibliografía

Entrevistas

Arroyo Vargas, Manuel: Lunes 26 de febrero del 2007, Entrevista con el Contador de Corporación Arrocera Costa Rica S.A. sobre el entendimiento del negocio, Planta Central, Barrio San José, Alajuela, Costa Rica

Carmona Rodríguez, Norbel: Martes 13 de marzo del 2007, Entrevista con el Encargado de TI de Corporación Arrocera Costa Rica S.A. sobre el entendimiento del negocio, Planta Central, Barrio San José, Alajuela, Costa Rica

Carmona Rodríguez, Norbel: Martes 27 de marzo del 2007, Entrevista con el Encargado de TI de Corporación Arrocera Costa Rica S.A. sobre el entendimiento del negocio, Planta Central, Barrio San José, Alajuela, Costa Rica

Normativa

Asamblea Legislativa de la Republica de Costa Rica: 1978, Ley No. 6289, Ley de Creación de la Oficina Nacional de Semillas, http://www.asamblea.go.cr/ley/leyes/6000/6289.doc, San José, Costa Rica

Asamblea Legislativa de la Republica de Costa Rica: 1985, Ley No. 7014, Ley de Creación de la Oficina del Arroz, http://www.asamblea.go.cr/ley/leyes/7000/7014.doc, San José, Costa Rica

Consejo de Normas Internacionales de Contabilidad: 2005, Normas Internacionales de Información Financiera, Comperio de Normativas, PricewaterhouseCoopers, Reino Unido

Consejo Nacional de Supervisión del Sistema Financiero: 2002, Normativa de tecnología de información para las entidades fiscalizadas por la SUGEF, http://www.bccr.fi.cr/documentos/secretaria/archivos/NormativaTecnoInformacionEntFiscal-SUGEF.pdf, San José, Costa Rica

Contraloría General de la República: 1995, Manual sobre normas técnicas de control interno relativas a los sistemas de información computadorizados, http://documentos.cgr.go.cr/content/dav/jaguar/documentos/manuales/docs/m_sistemas/indice.html, San José, Costa Rica

Federación Internacional de Contadores: 2005, Normas Internacionales de Auditoría, Comperio de Normativas, PricewaterhouseCoopers, Reino Unido

Otras fuentes bibliográficas

PricewaterhouseCoopers: 2005, Team Mate Audit Management System, PricewaterhouseCoopers International Limited, Versión 8.0, Reino Unido

Fuentes digitales

British Standards Information: Martes 27 de enero del 2007, BS ISO/IEC 27001 Tecnología de Información, Sitio Web Oficial, http://www.bsi-global.com/ICT/Security/bs7799-2.xalter, Reino Unido

Corporación Arrocera Costa Rica S.A.: Lunes 26 de enero del 2007, Perfil de la Corporación Arrocera Costa Rica S.A., Sitio Web Oficial, http://www.arrozeta.com/, Alajuela, Costa Rica

Instituto de Gobierno de TI: Martes 27 de enero del 2007, CobiT 4.0, Sitio Web Oficial, http://www.isaca.org/, Estados Unidos de América

Microsoft Corporation: Martes 13 de marzo del 2007, Soporte Técnico SQL Server 2000, Mejores Prácticas de Configuración SQL Server 2000, http://support.microsoft.com/ph/2852, Estados Unidos

Microsoft Corporation: Martes 13 de marzo del 2007, Soporte Técnico Windows 2000 Server , Mejores Prácticas de Configuración Windows 2000 Server, http://www.microsoft.com/technet/solutionaccelerators/howto/admhow.mspx, Estados Unidos

Anexos complementarios

Anexo 1

Formulario de verificación de seguridad lógica para la aplicación Axapta

Lista de verificación de Seguridad Lógica Aplicación Axapta

	Administración de usuarios	SI	NO	Comentarios
1	¿Quién es responsable de otorgar acceso a la aplicación y asegurar una adecuada segregación de funciones?	X		El encargado de TI
2	Todos los usuarios y grupos/roles son conocidos y documentados por la persona (s) responsable (s) de mantener la aplicación	X		
3	Todas las cuentas de usuario tienen registrados el nombre completo y descripción de puesto	X		
4	Todas las cuentas de usuario pertenecen a un grupo lógico	X		
5	Cualquier cuenta que no haya sigo logueada por más de dos meses es bloqueada		X	No se considera necesario por la naturaleza de negocio
6	El sistema desactiva una conexión ociosa después de un tiempo determinado (session timeout)		X	
7	Cualquier cuenta que no se ha logueado por más de seis meses debe ser deshabilitada		X	
8	Hay un proceso para notificar a recursos humanos, departamento de sistemas, guardas de seguridad, etc. cuando un funcionario deja la organización o cambia de departamento	X		Aunque no se encuentra documentado
9	Los derechos de acceso de usuarios que cambian de puesto o dejan la organización son cambiados o removidos respectivamente	X		
10	Sólo el administrador del sistema/aplicación o una persona autorizada tiene acceso para crear un usuario, reactivar usuarios bloqueados o alterar los derechos de usuario	X		
11	Existen formularios/emails para autorizar la creación, revocación, o alteración de accesos	X		Vía email
12	Todos los usuarios tienen una cuenta única y propia	X		
13	Los usuarios deben firmar un documento donde indiquen que entienden las condiciones del acceso.		X	No se realiza esta práctica
14	Se lleva y actualiza un registro de usuarios con acceso al sistema.	X		
15	Las cuentas de usuario genéricos han sido removidas o limitadas en la medida de lo posible	X		
16	El sistema no permite sesiones abiertas simultáneamente para un mismo usuario desde diferentes máquinas.	X		
17	Las cuentas default han sido removidas/bloqueadas en la medida de lo posible	X		
	Controles de Password			
1	Las cuentas de usuario se bloquean después de tres intentos fallidos de login	X		Cinco intentos
2	El mínimo número de caracteres de passwords está acorde con los estándares y lineamientos de seguridad de la empresa (idealmente 6-8 caracteres)	X		
3	La edad máxima del password está de acuerdo con los estándares y lineamientos de seguridad de la empresa (idealmente 30 días)	X		
4	La edad mínima del password está de acuerdo con los estándares y lineamientos de seguridad de la empresa (idealmente 3 días)		X	No se considera necesario por la naturaleza del negocio
5	El historial de password está de acuerdo con los estándares y lineamientos de seguridad de la empresa.	X		
6	Se requiere que los usuarios cambien la contraseña que se les asigna al crear su cuenta en el primer logon	X		
7	La contraseña que se le asigna al usuario al crear su cuenta es único y difícil de adivinar	X		

Anexo 2

Formulario de verificación de seguridad lógica para la base de datos SQL Server 2000

Lista de verificación de Seguridad Lógica SQL Server 2000

	Administración de usuarios	SI	NO	Comentarios
1	¿Se encuentran habilitadas las opciones de pistas de auditoría de SQL Server?		X	Se comprobó que no se encuentran parametrizadas
2	¿Se encuentran habilitados todos los jobs e historiales de backups, para las diferentes bases de datos?	X		Se revisó el Job History y se determinó adecuado
3	¿La base de datos se encuentra deshabilitada para que no se puedan realizar replicas remotas?		X	Se encontró habilitado la opción en las propiedades de la base de datos
4	¿Es seguro el acceso a la base de datos?		X	Por medio de una consulta en el SQL agent se determinó que existe 2 usuarios como administradores como valores NULL en la contraseña y otro con valor NULL en el nombre usuario
5	¿Los password de la cuentas en la base de datos debe estar de acuerdo a las políticas de la empresa?	X		Se verificó en las propiedades de SQL Server Enterprise Manager
6	¿Están los comandos ejecutables del sistema en la base de datos restringidos?	X		Se determinó que para el procedimiento almacenado Xp_cmdshell, no se encintrara habilitadas las opciones EXE
7	¿Están solo los usuarios autorizados a accesar la base de datos de manera remota?		X	Se determinó que la casilla que habilita este acceso se encontraba marcada
8	¿Están las cuentas asignadas a bases públicas habilitadas para ejecutar, programar o crear jobs por medio del SQL agent?	X		Se determinó la inexistencia de los siguientes procedimientos almacenados: sp_add_job sp_add_jobstep sp_add_jobserver sp_start_job xp_execresultset xp_printstatements xp_displayparamstmt
9	¿Están los administradores del servidor habilitados para tener acceso a la base de datos?	X		Esta opción se encuentra habilitada, ya que se dejaron las opciones parametrizadas que tiene SQL Server por default
10	¿Está restringido el uso de cuentas de invitados?	X		
11	¿Todos los usuarios, grupos, los roles dentro del servidor y los roles de la base de datos son conocidos y documentados por el grupo responsable del mantenimiento a la base de datos?	X		
12	¿Se encuentra instalada y configurada apropiadamente la última versión de Microsoft Service Packs para SQL Server 2000?	X		Se determinó que se encuentra instalado el Service Pack 4 Server 2000

Anexo 3

Formulario de verificación de seguridad lógica para el sistema operativo Windows 2000 Server

Lista de verificación de Seguridad Lógica Windows 2000 Server

	Administración de usuarios	SI	NO	Comentarios
1	¿Se encuentran habilitadas las opciones de pistas de auditoría de Windows 2000 Server? (A nivel de Domain Controllers)		X	Se comprobó que no se encontraban habilitadas
2	¿Están los log de auditoría protegidos por medio de acceso?		X	
3	¿Está habilitada la opción de pista de auditoría para los intentos fallidos de registro?		X	
4	¿Existe acceso restringido por usuario para el los objetos donde se encuentran las aplicaciones de la empresa?	X		
5	¿Existe acceso restringido por usuario para los datos y directorios donde se encuentra la información crítica de la empresa?	X		Se verificó la configuración del Active Directory
6	¿Solo existen cuentas con permisos de administrador autorizadas?	X		
7	¿Solo existen relaciones de confianza con otros Active Directory autorizadas?	X		
8	¿Existen relaciones de confianza con terceros? (Estas no deben ser permitidas)		X	
9	¿Los password para todas las cuentas de servicio expiran periódicamente?	X		Incluso expira para las cuentas de administrador
10	¿Los nuevos usuarios deben de cambiar su contraseña en el primer login al haber suministrado previamente una contraseña que no es genérica o fácil de recordar?	X		Se otorga un password de primer inicio que es fuerte
11	¿Se encuentran habilitados los servicios de operación, operaciones de backup, cuentas de operación y operaciones de impresión, a los usuarios respectivos, sólo por medio de grupos, donde se asignan los permisos correspondientes?	X		Se comprobó que es estos permisos sólo se asignan a un grupo determinado
12	¿Se ingresan todas las cuentas directamente desde el Domain Controller y no desde las estaciones de trabajo y los servidores?	X		No es posible realizar esta labor desde otra ubicación que no sea el Domain Controller
13	¿Se encuentra habilitada la opción de bloqueo de cuentas luego de un periodo establecido de acuerdo a las políticas de la empresa?	X		30 minutos
14	¿Se encuentran parametrizadas las opciones para que los usuarios utilicen contraseñas fuertes?	X		
15	¿Existe una política de historial de password habilitada?	X		3 contraseñas recordadas
16	¿Se ha habilitado un límite de caracteres para establecer el password de cada usuario?	X		8 caracteres
17	¿Se ha establecido un máximo de tiempo de uso de un mismo password?	X		30 días
18	¿Se ha establecido un mínimo de tiempo de uso de un mismo password?	X		0 días
19	¿El manejo de las cuentas de administrador aplica para también en base a las políticas de seguridad de la empresa?	X		Se comprobó las opciones de la cuenta de administrador

Anexo 4

Formulario de verificación de seguridad física

Lista de verificación de Seguridad Física

	Acceso al centro de cómputo	SI	NO	Comentarios
1	¿El acceso físico al centro de cómputo se encuentra debidamente restringido al personal autorizado? (Llave, tarjeta magnética)	X		Por medio de una llave
2	¿Únicamente el personal que requiere acceso al centro de cómputo dadas las responsabilidades propias de su puesto esta autorizado para acceder a el centro de cómputo?	X		
3	¿Existen políticas y procedimientos en cuanto al acceso físico al centro de cómputo? Las mismas comprenden los siguientes puntos:		X	No existen políticas relacionadas con el acceso físico
	a) requisitos de autorización de entrada de terceras personas		X	
	b) supervisión a terceras personas autorizadas durante su estadía		X	
	c) obligatoriedad de que el centro de cómputo permanezca cerrado en todo momento		X	
	d) procedimiento de entrada de terceras personas supervisadas (firma de bitácora, proceso de autorización, etc.).		X	
	e) procedimiento de salida de la sala (cierre de puertas, regulación de temperatura, etc.).		X	
4	¿Se tiene una bitácora donde se registre el ingreso de terceras personas?		X	No existe una bitácora de control de acceso a terceros
	a) ¿se registra la fecha y hora de entrada?		X	
	b) ¿se registra el motivo del ingreso?		X	
	c) ¿se registra el responsable por supervisar al visitante?		X	
5	¿Se lleva a cabo una revisión periódica de los registros de visitantes, persona responsable de los visitantes para verificar que su ingreso haya sido justificado?		X	
	Centro de Cómputo			
1	El Centro de Cómputo cuenta con los siguientes controles ambientales			
	a) alarma de robo		X	
	b) alarma de incendio		X	
	c) extintor de fuego vigente		X	
	d) paredes, pisos y cielorrasos a prueba de incendios		X	
	e) piso falso a prueba de inundaciones		X	
	f) cielorraso a prueba de inundaciones		X	
	g) no cuenta con ventanas		X	
	h) inexistencia de papeles, cajas u otros materiales inflamables		X	
	i) aire acondicionado (preferiblemente con respaldo) propio para el área	X		
	j) los tableros de cableado no se encuentran saturados	X		
	k) controladores de humedad		X	
	l) termómetros / medidores de humedad		X	
	m) protectores de voltaje UPS	X		
	Otras consideraciones			
1	¿Se han establecido procedimientos de cómo se tendrá que proceder en caso de que ocurran los diferentes escenarios de contingencia dentro del centro de cómputo?		X	
2	¿La seguridad física es tomada en cuenta en el plan de recuperación/contingencia en caso de desastre y abarca una seguridad física similar en las instalaciones aprovisionadas?		X	